

Notas de
**ESTABILIDAD
FINANCIERA**

Número 2 - noviembre 2002



**Debida diligencia
con la clientela bancaria**



BANCO DE ESPAÑA

Notas de
ESTABILIDAD
FINANCIERA

Número 2 - noviembre 2002

Debida diligencia
con la clientela bancaria



BANCO DE ESPAÑA

El contenido de todos los artículos firmados es responsabilidad única de sus autores, sin que necesariamente reflejen criterios del Banco de España, ni de ninguna de sus dependencias, salvo mención explícita en sentido contrario.

El Banco de España difunde todos sus informes y publicaciones periódicas a través de la red INTERNET en la dirección <http://www.bde.es>

© BANCO DE ESPAÑA, Madrid, 2002

ISBN: 84-7793-788-5

Depósito legal: M. 17342-2002

ÍNDICE

	<u>Páginas</u>
PRESENTACIÓN.	7
ARTÍCULOS	
Debida diligencia con la clientela de los bancos, <i>Comité de Supervisión Bancaria de Basilea</i>	11
Las Cuarenta Recomendaciones, <i>Grupo de Acción Financiera sobre el Blanqueo de Capitales</i>	43
Directrices globales para la prevención del blanqueo de capitales en actividades de banca privada, <i>Grupo Wolfsberg</i>	63
El sistema financiero y el blanqueo de capitales, <i>Ignacio Palicio Díaz-Faes</i>	73

Presentación

Aunque a veces se asocie únicamente al blanqueo de capitales y —especialmente, tras los acontecimientos del 11 de septiembre— a la financiación de actividades terroristas, la debida diligencia con los clientes tiene un significado mucho más rico, profundamente arraigado en la mejor tradición bancaria.

En su sentido más amplio, actuar con la debida diligencia equivale a ejecutar algo con suficiente cuidado. A partir de esta definición general, existen dos concepciones, en gran parte complementarias, sobre la utilización de este concepto en la actividad empresarial. La primera tiene reminiscencias jurídicas y es esencialmente defensiva, ya que concibe la debida diligencia como actuar con el cuidado que sea necesario para evitar la posibilidad de llegar a ser considerado culpable por negligencia y de incurrir en las correspondientes responsabilidades. La segunda interpretación, de contenido más económico y más proactiva, la identifica con el conjunto de procesos necesarios para poder adoptar decisiones suficientemente informadas.

En línea con esta última acepción, pero sin olvidar la primera, una mayor aproximación a cómo se aplica a la actividad bancaria la debida diligencia lleva a considerar esta como el proceso de captación y evaluación sistemática de información, con el fin de identificar la verdadera naturaleza y los riesgos de cualquier operación. Aceptando esta definición, dado que el riesgo de crédito es el más antiguo e importante de los que asumen las entidades bancarias, resulta lógico que la debida diligencia haya penetrado en la cultura bancaria, esencialmente de la mano de dicho riesgo.

Como consecuencia de este origen, una vertiente concreta de «conozca a su cliente» (o a su contraparte) —es decir, investigue su verdadera identidad, su historial, la naturaleza de sus negocios, su entorno, su solvencia, su capacidad de gestión y la viabilidad de sus proyectos— se ha convertido desde hace tiempo en el pilar básico de la política crediticia de las entidades. Como consecuencia de ello, esta vertiente del principio «conozca a su cliente» ha fraguado en un conjunto, sólido y muy experimentado, de políticas, procedimientos, autorizaciones, registros y controles, cuyos aspectos fundamentales son normalmente establecidos y vigilados por el consejo de administración. Además, para mantener vivo en toda la organización este aspecto clave de la política crediticia, habitualmente existen programas continuados de formación y actualización. A la vez, su cumplimiento efectivo es permanentemente verificado y evaluado por unidades especiales independientes, como la auditoría interna y el departamento responsable del cumplimiento normativo.

La misma causa, la importancia del riesgo de crédito, explica que también la actuación supervisora, en lo que al terreno organizativo se refiere, se haya centrado fundamentalmente en verificar la calidad del diseño de los procedimientos relacionados con el citado riesgo, y su nivel de implantación y cumplimiento.

A medida que han ido cobrando suficiente relevancia otros riesgos, dependiendo de su naturaleza y magnitud, y de las características de las entidades, estas han ido adoptando las correspondientes medidas de debida diligencia, cuya adecuación y eficacia también han ido pasando a ser evaluadas por el supervisor, al establecer el perfil de riesgo de cada entidad.

Los cuatro documentos que incluye esta publicación plantean la necesidad de fortalecer una modalidad específica de debida diligencia con los clientes bancarios: la que se refiere a la prevención de los riesgos (básicamente, de reputación, operativo y legal) que implica, para las entidades, su participación, incluso involuntaria, en actividades ilegales o poco éticas.

Resulta obvio que, a nivel de cada entidad, los riesgos citados pueden ocasionar pérdidas considerables, que lleguen a cuestionar hasta su propia viabilidad. Sin embargo, estas posibles repercusiones individuales no son las únicas cuestiones relevantes. Están, por ejemplo, las exigencias legales, tanto de carácter general como, en particular, las derivadas, entre otras, de la Ley 19/1993, sobre determinadas medidas de prevención del blanqueo de capitales, y de su desarrollo. Además, dada la importancia básica que tiene la confianza del público en la integridad del sistema bancario, para que este pueda desempeñar su papel central en el sistema económico, el supervisor debe prevenir, con el máximo rigor, la posibilidad de que eventuales actuaciones negligentes, incluso de una entidad aislada, puedan poner en peligro la reputación de todo el sector y, con ello, perturbar la estabilidad del sistema financiero.

Es evidente que toda esta problemática no es nueva. De hecho, esta vertiente de la debida diligencia está presente, desde hace tiempo, tanto en la actividad de las entidades como en su supervisión. Sin embargo, lo que sí es nuevo, y desde luego positivo, es la creciente sensibilización social acerca de si el sistema bancario está adoptando todas las medidas razonables para evitar que los servicios que presta puedan ser indebidamente utilizados, es decir, no solo para la financiación del terrorismo o el blanqueo de capitales, sino también para cualquier otra finalidad ilegal o poco ética.

Ninguna vertiente de la debida diligencia es una ciencia exacta, acabada, cuyo contenido sea de aplicación universal. La que se pretende potenciar con la difusión de estas *Notas de estabilidad financiera* tampoco lo es. Por el contrario, concretar los principios generales que en esta publicación se proponen en función de las características de cada entidad; potenciarlos de acuerdo con las nuevas demandas sociales; plasmarlos

en el diseño, aplicación y control de medidas eficaces; y mantenerlos debidamente vigentes y actualizados requiere de las entidades un ejercicio de rigor y de creatividad tan importante como inaplazable.

Perfeccionar los niveles actuales de debida diligencia bancaria con sus clientes, para evitar la utilización ilícita del sistema, es un esfuerzo costoso. Por ello, exige del consejo de administración de las entidades su previa mentalización en la importancia del tema y una doble implicación. Por un lado, en que todos los niveles de la entidad lleguen a impregnarse de una cultura de riesgo que incluya los asumidos por la posible utilización indebida de la entidad. Por otro, en la definición, implantación y seguimiento de políticas, procedimientos y controles coherentes con dicha cultura y con las características específicas de la entidad.

Dado el ingente volumen de transacciones que realiza una entidad bancaria, incluso de tamaño relativamente pequeño, cualquier intento no selectivo de conocer debidamente la identidad de sus clientes y la naturaleza de sus negocios, detectar las operaciones sospechosas y poner en marcha los correspondientes procesos de evaluación y de notificación, interna y externa, resulta poco factible, incluso con el debido soporte informático, por sus prohibitivos costes. Por ello, en relación con todas estas cuestiones, resulta imprescindible aplicar un enfoque basado en el riesgo, que establezca selectivamente dónde conviene concentrar los mayores esfuerzos.

Es necesario, por tanto, que, a partir de un conocimiento profundo y actualizado de la entidad, de su clientela, del perfil habitual de las operaciones y servicios en todas sus líneas de negocio, de sus zonas geográficas de actuación, etc., cada entidad establezca con precisión y revise periódicamente sus propios criterios cuantitativos y cualitativos, que definan los clientes, áreas y actividades con mayor riesgo.

Sin perjuicio de la debida diligencia general, en cuya implantación el apoyo informático resulta particularmente útil, es en los clientes, áreas y actividades detectados como más arriesgados donde hay que concentrar los mayores recursos. Además, en relación con estos clientes y actividades de especial riesgo, es preciso establecer una clara distribución de responsabilidades a la hora de autorizar su aceptación y mantenimiento.

Aunque sean las entidades las máximas responsables de mejorar la debida diligencia en las relaciones con sus clientes, adaptándolas a las nuevas circunstancias cuando sea necesario, los supervisores no pueden ni deben quedar al margen de este proceso.

Como explícitamente establece el Comité de Supervisión Bancaria de Basilea: «Los supervisores tienen la responsabilidad de controlar que los bancos utilicen procedimientos seguros para conocer a sus clientes y que mantengan estándares éticos y profesionales elevados. Los supervisores deben confirmar la existencia de controles internos adecuados en el banco y la conformidad con las orientaciones de supervisión y regulación

emitidas. El proceso de supervisión incluirá, por un lado, la evaluación de las políticas y procedimientos y, por otro, el examen de archivos de clientes y el muestreo de algunas cuentas (...). Los supervisores deben dejar claro que adoptarán todas las medidas necesarias (que podrían ser severas y públicas si las circunstancias así lo exigen) para actuar en contra de los bancos y altos cargos que no sigan sus propios procedimientos y requisitos de regulación internos.»

El Banco de España, como responsable de la supervisión del sistema bancario y como miembro del Comité de Supervisión Bancaria de Basilea, comparte estos criterios. En consecuencia, y sin interferir en las responsabilidades propias de otros organismos, como la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y su Servicio Ejecutivo, el Banco de España tiene en estudio las formas concretas de potenciar y actualizar la vertiente de su labor supervisora relativa a la debida diligencia de las entidades bancarias con sus clientes.

A esta línea de actuación obedece la publicación del presente número monográfico de *Notas de estabilidad financiera*, que incluye, en primer lugar, el documento «Debida diligencia con la clientela de los bancos», sin duda el más importante resumen de principios básicos en materia de «conozca a su cliente», adaptados a las peculiaridades de la actividad bancaria. Publicado por el Comité de Supervisión Bancaria de Basilea en octubre de 2001, se ofrece la versión en español, traducida en septiembre de 2002 por la Asociación de Supervisores Bancarios de las Américas (ASBA).

En segundo lugar, figuran «Las cuarenta recomendaciones» del Grupo de Acción Financiera sobre el Blanqueo de Capitales (GAFI o FATF, en su acrónimo inglés). Este organismo, adscrito a la OCDE, está integrado por 31 países, entre ellos España, y cuenta con observadores de 21 organizaciones internacionales directamente interesadas en el tema. La actualización de estas recomendaciones se encuentra en estos momentos en la fase de consultas.

En tercer lugar, se reproduce la revisión de mayo de 2002 de los denominados «Principios Wolfsberg». El Grupo Wolfsberg está integrado por 12 de las mayores entidades del mundo con fuerte presencia en actividades de banca privada. Sus Principios, en cuya revisión ha colaborado Transparency International, entre otros expertos, constituyen un desarrollo de la debida diligencia, especialmente aplicable a las actividades de banca privada.

Finalmente, se incluye un artículo de Ignacio Palicio, director adjunto del Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales. En él, el autor repasa los conceptos básicos relacionados con el blanqueo de capitales, los riesgos y responsabilidades que este plantea para las entidades bancarias, los mecanismos básicos de prevención y la regulación española y de la Unión Europea sobre la materia.

*DEBIDA DILIGENCIA CON LA
CLIENTELA DE LOS BANCOS*

Comité de Supervisión
Bancaria de Basilea

Grupo de Trabajo sobre Banca Transterritorial

Copresidentes:

Sr. Charles Freeland, Secretario General Adjunto del Comité de Supervisión Bancaria de Basilea

Sr. Colin Powell, Presidente del Grupo Extraterritorial de Supervisores Bancarios y Presidente de la Comisión de Servicios Bancarios de Jersey

Autoridad Monetaria de las Bermudas	<i>Sr. D. Munro Sutherland</i>
Autoridad Monetaria de las Islas Caimán	<i>Sr. John Bourbon Sra. Anna McLean</i>
Banco de Francia / Comisión Bancaria	<i>Sr. Laurent Ettori</i>
Oficina Federal de Supervisión Bancaria de Alemania	<i>Sr. Jochen Sanio Sr. Peter Kruschel</i>
Comisión de Servicios Financieros de Guernesey	<i>Sr. Peter G. Crook (hasta abril 2001) Sr. Philip Marr (desde abril 2001)</i>
Banco de Italia	<i>Sr. Giuseppe Godano</i>
Agencia de Servicios Financieros de Japón	<i>Sr. Kiyotaka Sasaki (hasta julio 2001) Sr. Hisashi Ono (desde julio 2001)</i>
Comisión de Supervisión del Sector Financiero de Luxemburgo	<i>Sr. Romain Strock</i>
Autoridad Monetaria de Singapur	<i>Sra. Foo-Yap Siew Hong Srta. Teo Lay Har</i>
Comisión Federal de Bancos de Suiza	<i>Sr. Daniel Zuberbühler Srta. Dina Balleyguier</i>
Autoridad de Servicios Financieros del Reino Unido	<i>Sr. Richard Chalmers</i>
Junta de Gobernadores del Sistema de la Reserva Federal de EEUU	<i>Sr. William Ryback</i>
Banco de la Reserva Federal de Nueva York	<i>Srta. Nancy Bercovici</i>
Oficina del Controlador de la Moneda de EEUU	<i>Sr. José Tuya Srta. Tanya Smith</i>
Secretaría	<i>Sr. Andrew Khoo</i>

ÍNDICE

	<u>Páginas</u>
I. Introducción	17
II. Importancia de las normas KYC para supervisores y bancos . . .	19
III. Elementos esenciales de las normas KYC	21
1. Política de aceptación de clientes	22
2. Identificación de clientes	22
2.1. Requisitos generales de identificación	24
2.2. Cuestiones específicas de identificación.	25
2.2.1. Cuentas de fideicomiso, de nominatario y fiduciarias	25
2.2.2. Vehículos corporativos	25
2.2.3. Negocios presentados	26
2.2.4. Cuentas de clientes abiertas por intermediarios profesionales.	27
2.2.5. Personas del medio político	28
2.2.6. Clientes no presentes	29
2.2.7. Banca corresponsal	30
3. Seguimiento continuo de cuentas y transacciones.	31
4. Gestión de riesgos	33
IV. El papel de los supervisores	34
V. Aplicación de las normas KYC en un contexto transterritorial . . .	35
ANEXO 1: Extractos de Metodología de Principios Básicos.	38
ANEXO 2: Extractos de las Recomendaciones FATF.	40

I. INTRODUCCIÓN

1. Los supervisores de todo el mundo otorgan cada vez más importancia a los controles y procedimientos con los que deben contar los bancos para conocer a sus clientes. Ejercer la debida diligencia con respecto a clientes nuevos y antiguos es una parte muy importante de estos controles. Sin esta debida diligencia, los bancos podrían correr riesgos de reputación, operativos, legales y de concentración, lo que podría conllevar un coste financiero importante.

2. Al examinar los resultados de una encuesta interna de banca transterritorial en 1999, el Comité de Basilea observó que existían deficiencias en las políticas de «conozca a su cliente» para bancos de un gran número de países. Visto desde la perspectiva de la supervisión, algunos países tienen políticas KYC (de las siglas en inglés para *know your customer*) inadecuadas y otros no tienen ninguna política de este tipo. Aun en los países con mercados financieros bien desarrollados, la solidez de las políticas KYC varía considerablemente. Por consiguiente, el Comité de Basilea solicitó al Grupo de Trabajo sobre Banca Transterritorial (1) que examinara los procedimientos KYC utilizados actualmente y recomendara normas aplicables a los bancos en todos los países. El resultado de este trabajo fue un documento consultivo publicado en enero de 2001. Después de analizar los comentarios recibidos a raíz de ese primer documento, el Grupo de Trabajo realizó algunas modificaciones y produjo la versión final, que el Comité de Basilea está distribuyendo en todo el mundo con la esperanza de que el marco KYC que en ella se presenta sirva de punto de referencia para que los supervisores establezcan prácticas nacionales y los bancos elaboren sus propios programas. Cabe destacar que las prácticas de supervisión de algunas jurisdicciones satisfacen el propósito de este documento, e incluso lo superan, resultando innecesario en esos casos introducir cambio alguno.

3. La práctica de conocer a su cliente está íntimamente relacionada con la lucha contra el lavado de dinero, competencia del Grupo de Acción Financiera Internacional contra el blanqueo de capitales, GAFI (*FATF* en inglés) (2). El Comité no pretende duplicar los esfuerzos del FATF, sino que su interés nace de una perspectiva más amplia relacionada con la prudencia. Las políticas y procedimientos KYC, cuando son

(1) Grupo conjunto integrado por miembros del Comité de Basilea y del Grupo Extraterritorial de Supervisores Bancarios.

(2) FATF es un organismo intergubernamental que elabora y promueve políticas, tanto nacional como internacionalmente, para combatir el lavado de dinero. Cuenta con 29 países miembros y dos organizaciones regionales. Trabaja en estrecha colaboración con otros organismos internacionales del mismo ámbito, como la Oficina de las Naciones Unidas de Fiscalización de Drogas y de Prevención del Delito, el Consejo de Europa, el Grupo de Asia-Pacífico sobre Lavado de Dinero y el Grupo de Acción Financiera del Caribe. Según la definición de FATF, el lavado de dinero consiste en la transformación de ganancias delictivas para disfrazar sus orígenes ilegales.

eficaces, ayudan a proteger la seguridad y solidez de los bancos y la integridad de los sistemas bancarios. El Comité de Basilea y el Grupo Extraterritorial de Supervisores Bancarios (OGBS, del inglés *Offshore Group of Banking Supervisors*) siguen apoyando firmemente la adopción y puesta en práctica de las recomendaciones de FATF, sobre todo las relacionadas con la banca, y piensan que las normas contenidas en el presente documento están de acuerdo con dichas recomendaciones. El Comité y el OGBS considerarán además la adopción de cualquier norma de mayor rango que FATF pudiera proponer tras haber evaluado las 40 Recomendaciones. En este sentido, el Grupo de Trabajo seguirá de cerca las deliberaciones de FATF y se mantendrá en contacto con él, como lo ha venido haciendo hasta ahora.

4. El Comité de Basilea aborda el tema de KYC desde la perspectiva más general de la prudencia, no solo como una herramienta para combatir el lavado de dinero. Una gestión eficaz de los riesgos bancarios exige procedimientos KYC sólidos y seguros. Las salvaguardas KYC van más allá de la simple apertura de cuentas y mantenimiento de registros, y exigen que los bancos formulen políticas de aceptación de clientes y programas de diferentes niveles para la identificación de los mismos, que incluyan un proceso de debida diligencia más extenso en el caso de cuentas de mayor riesgo y un seguimiento proactivo de cuentas para actividades sospechosas.

5. El interés del Comité de Basilea en normas seguras de KYC nace de su preocupación por la integridad del mercado y se ha incrementado a raíz de las pérdidas sufridas directa o indirectamente por los bancos, debido a su falta de diligencia a la hora de aplicar procedimientos apropiados. Estas pérdidas se hubieran podido evitar, disminuyéndose así el perjuicio para la reputación, si los bancos hubiesen mantenido buenos programas de KYC.

6. Este documento refuerza los principios establecidos en anteriores publicaciones del Comité, brindando una orientación más precisa sobre los elementos básicos de las normas KYC y su aplicación. Para preparar esta orientación, el Grupo de Trabajo recurrió a las prácticas que siguen los países miembros y tomó en cuenta las últimas tendencias de la supervisión. Los elementos básicos presentados en este documento constituyen una guía de las normas mínimas aplicables mundialmente a todos los bancos. Probablemente haya que complementar o reforzar estas normas mínimas con otras medidas, confeccionadas en función de los riesgos de determinadas instituciones y de los sistemas bancarios de cada país. Por ejemplo, las cuentas de mayor riesgo exigen una diligencia más intensa y lo mismo ocurre con los bancos cuyo objetivo es atraer a clientes con grandes cantidades de capital líquido. En algunas de sus secciones específicas, este documento recomienda normas de diligencia más estrictas, aplicables, de ser necesario, a las áreas de mayor riesgo de un banco.

7. La necesidad de contar con normas rigurosas de debida diligencia con los clientes no se limita a los bancos. El Comité de Basilea recomien-

da una orientación similar para las instituciones financieras no bancarias y los intermediarios profesionales de servicios financieros, como los abogados y contables.

II. IMPORTANCIA DE LAS NORMAS K.Y.C. PARA SUPERVISORES Y BANCOS

8. El Grupo de Acción Financiera y otras agrupaciones internacionales han trabajado con ahínco en el ámbito de KYC. Las 40 Recomendaciones de FATF para combatir el lavado de dinero (3) son reconocidas y aplicadas internacionalmente. El propósito de este documento no es duplicar el trabajo ya realizado.

9. Al mismo tiempo, los procedimientos eficaces de KYC son particularmente importantes para la seguridad y solidez de los bancos, porque:

- ayudan a proteger la reputación de los bancos y la integridad de los sistemas bancarios, al reducir la probabilidad de que los bancos se conviertan en un vehículo o en una víctima del crimen financiero y sufran así daños en su reputación;
- constituyen una parte esencial de la gestión de riesgos eficaz (por ejemplo, ofrecen una base sobre la cual identificar, limitar y controlar los riesgos para el activo y el pasivo, incluso para los activos en administración).

10. La inadecuación o falta de normas KYC puede someter a los bancos a riesgos serios con sus clientes y contrapartes, especialmente *riesgos de reputación, operativos, legales y de concentración*. Cabe destacar que todos estos riesgos están relacionados entre sí. Sin embargo, cualquiera de ellos puede resultar en un coste financiero considerable para los bancos (por ejemplo, a raíz de la retirada de fondos por parte de los depositantes, el cese de servicios interbancarios, las demandas interpuestas contra del banco, los gastos de investigación, el embargo y la congelación de haberes, y los préstamos incobrables), así como en la necesidad de consagrar una cantidad considerable de tiempo y energía de gestión para resolver los problemas que surgen.

11. El *riesgo de reputación* amenaza especialmente a los bancos, ya que la clase de negocio que realizan requiere de la confianza de los depositantes, los acreedores y el mercado en general. El riesgo de reputación puede definirse como la posibilidad de que una publicidad negativa relacionada con las prácticas y relaciones de negocios de un banco, ya sea acertada o no, cause una pérdida de confianza en la integridad de la institución. Los bancos son especialmente vulnerables al riesgo de repu-

(3) Ver las recomendaciones FATF números 10 a 19 reproducidas en el anexo 2.

tación, porque pueden convertirse fácilmente en vehículo o víctima de las actividades ilegales de sus clientes. Deben por lo tanto protegerse con una vigilancia continua, a través de un programa KYC eficaz. Los bienes en administración, o los mantenidos en fideicomiso, pueden presentar un peligro especial para la reputación del banco.

12. El *riesgo operativo* es el riesgo de una pérdida directa o indirecta resultante de un fallo en los procesos, personal y sistemas internos o de acontecimientos externos. En el contexto KYC, la mayoría del riesgo operativo tiene que ver con insuficiencias en la aplicación de los programas del banco, procedimientos de control deficientes y el hecho de no practicar la debida diligencia. Si ante los ojos del público el banco es incapaz de manejar su riesgo operativo convenientemente, su negocio se verá perturbado o perjudicado.

13. El *riesgo legal* es la posibilidad de que procesos, sentencias adversas o contratos que resulten ser inaplicables puedan perturbar o perjudicar las operaciones o la situación de un banco. Los bancos pueden ser objeto de acciones procesales por no respetar las normas KYC obligatorias o por no practicar la debida diligencia. Por lo tanto, los bancos pueden ser, por ejemplo, pasibles de multas, responsabilidad penal y sanciones especiales impuestas por los supervisores. En efecto, para un banco, el coste de un juicio puede ser mucho mayor que las costas judiciales. Los bancos no podrán protegerse contra tales riesgos legales sin la debida diligencia en el momento de identificar a sus clientes y entender sus negocios.

14. Desde el punto de vista de la supervisión, la preocupación por el *riesgo de concentración* se manifiesta en el activo del balance general. Comúnmente, los supervisores exigen no solo que los bancos cuenten con sistemas de información para identificar las concentraciones de crédito, sino que la mayoría fija también límites prudenciales para restringir los riesgos de los bancos frente a un prestatario único o a un grupo de prestatarios relacionados. Si el banco no sabe precisamente quiénes son sus clientes ni qué relación tienen con los demás clientes, no podrá medir su riesgo de concentración. Esto es especialmente importante en el caso de contrapartes relacionadas y préstamos ligados.

15. En el lado del pasivo, el riesgo de concentración está estrechamente asociado al riesgo de financiación, especialmente el riesgo de una retirada temprana y repentina de fondos por parte de grandes depositantes, con consecuencias potencialmente dañinas para la liquidez del banco. El riesgo de financiación será probablemente más alto en el caso de bancos pequeños y bancos menos activos en los mercados interbancarios que en el caso de los grandes bancos. Para analizar las concentraciones de depósitos, los bancos deben comprender las características de sus depositantes, incluyendo sus identidades y la medida en que sus acciones pueden estar ligadas a las de otros depositantes. Las personas encargadas de administrar el pasivo en los bancos pequeños deben conocer bien a los grandes depositantes y mantener una estrecha relación

con ellos, pues de lo contrario correrían el riesgo de perder sus fondos en los momentos difíciles.

16. Es frecuente que los clientes tengan varias cuentas con el mismo banco, pero en oficinas ubicadas en distintos países. Para manejar el riesgo de reputación, cumplimiento y legal resultantes, los bancos deben ser capaces de agregar y controlar saldos y actividades importantes en esas cuentas, en base consolidada y a escala mundial, independientemente de si las cuentas están recogidas en el balance, fuera del balance, como activos en administración o de forma fiduciaria.

17. Tanto el Comité de Basilea como el Grupo Extraterritorial de Supervisores Bancarios están plenamente convencidos de que las prácticas eficaces de KYC deben formar parte de los sistemas de gestión de riesgos y control internos de los bancos. Los supervisores nacionales son responsables de asegurar que los bancos cuenten con normas mínimas y controles internos que les permitan conocer a sus clientes. Los códigos de conducta voluntarios (4) emitidos por organizaciones o asociaciones del sector pueden ser muy útiles para secundar la orientación de regulación, ya que ofrecen a los bancos consejos prácticos en materia de operaciones. Sin embargo, dichos códigos no deben ser considerados como un sustituto de una orientación formal para la regulación.

III. ELEMENTOS ESENCIALES DE LAS NORMAS K.Y.C.

18. El Comité de Basilea ha emitido orientaciones sobre KYC en tres documentos diferentes, los cuales reflejan la evolución del pensamiento de supervisión con el tiempo. Estos documentos son: «La Prevención del Uso Delictivo del Sistema Bancario con el Propósito de Lavado de Dinero», emitido en 1988, en el que se estipulan los principios éticos básicos y se insta a los bancos a instalar procedimientos eficaces para identificar a sus clientes, rechazar transacciones sospechosas y cooperar con los organismos encargados de hacer cumplir la legislación. Los «Principios Básicos para la Supervisión Bancaria Eficiente», de 1997, sostienen, dentro de una discusión más general sobre controles internos, que los bancos deben contar con políticas, prácticas y procedimientos adecuados, incluyendo reglas estrictas de «conozca a su cliente». Más concretamente, los supervisores deben alentar la adopción de las recomendaciones pertinentes del FATF. Estas recomendaciones se refieren a la identificación de clientes y al mantenimiento de registros, mayor diligencia por parte de las instituciones financieras para detectar transacciones sospechosas e informar sobre ellas, y medidas para tratar con países cuyas reglas contra el lavado de dinero son insuficientes. La «Metodología de los Principios Básicos», de 1999, explica con más detalle los Principios Básicos, e incluye una lista de criterios esenciales

(4) Un ejemplo de código del sector son las «Directrices Globales Contra el Lavado de Dinero para la Banca Privada» (conocidas también como los Principios Wolfsberg), elaboradas en octubre de 2000 por 12 de los principales bancos con operaciones de banca privada.

y complementarios. (El anexo 1 presenta los extractos pertinentes de los Principios Básicos y la Metodología.)

19. Todos los bancos deberían «contar con políticas, prácticas y procedimientos adecuados que promuevan normas éticas y profesionales estrictas y eviten que el banco sea utilizado, intencional o involuntariamente, por agentes delictivos» (5). Los bancos deben incluir ciertos elementos claves en el diseño de sus programas KYC. Estos elementos esenciales deberían partir de los procedimientos de gestión y control de riesgos del banco e incluir: 1) una política de aceptación de clientes, 2) identificación de clientes, 3) seguimiento continuo de cuentas de alto riesgo, y 4) gestión de riesgos. Los bancos deben establecer la identidad del cliente y, además, controlar la actividad de la cuenta para determinar aquellas transacciones que no se ajusten a las transacciones normales o esperadas para ese cliente o tipo de cuenta. KYC debe ser un elemento básico de los procedimientos de gestión y control de riesgos del banco, y estar respaldado por evaluaciones de cumplimiento y auditorías internas regulares. La intensidad de los programas KYC más allá de estos elementos esenciales dependerá del grado de riesgo.

1. Política de aceptación de clientes

20. Los bancos deben elaborar políticas y procedimientos claros de aceptación de clientes. Estos deben incluir una descripción de los tipos de clientes que podrían presentar un riesgo superior al riesgo promedio. Al preparar dichas políticas, será necesario tomar en cuenta factores tales como los antecedentes del cliente, su país de origen, si ocupa un puesto relevante en el sector público o privado, las cuentas vinculadas, actividad de negocios u otros indicadores de riesgo. Los bancos deben elaborar políticas de aceptación del cliente graduales, es decir, cuanto más alto sea el riesgo del cliente, mayor será el grado de debida diligencia necesario. Por ejemplo, los requisitos de apertura de cuenta más básicos serían los aplicables a los asalariados con pequeños saldos. Es importante que la política de aceptación del cliente no sea demasiado restrictiva y termine negando el acceso del público en general a los servicios del banco, especialmente a los grupos financiera y socialmente desfavorecidos. Por otro lado, en el caso de un particular con un patrimonio considerable, cuya fuente de recursos no está muy clara, se haría indispensable ejercer un alto grado de debida diligencia. Las decisiones de establecer o no relaciones comerciales con clientes de alto riesgo, tales como personas del medio político (véase la sección 2.2.3, más abajo), deben adoptarse únicamente al nivel de dirección más alto.

2. Identificación de clientes

21. La identificación del cliente es un elemento esencial de las normas KYC. A efectos del presente documento, un cliente incluye:

(5) «Metodología de Principios Básicos», Criterio Esencial 1.

- la persona o entidad que mantiene una cuenta con el banco o aquella para la que se mantiene la cuenta (es decir, el usufructuario);
- los beneficiarios de transacciones efectuadas por intermediarios profesionales; y
- toda persona o entidad ligada a una transacción financiera y que pudiera representar un riesgo considerable de reputación o de otro tipo al banco.

22. Los bancos deberían poner en práctica un procedimiento sistemático de identificación de nuevos clientes y establecer una relación bancaria solo después de haber verificado satisfactoriamente la identidad del nuevo cliente.

23. Los bancos deberían «documentar y aplicar políticas de identificación de clientes y de aquellos que actúan en nombre de ellos» (6). Los mejores documentos para verificar la identidad de los clientes son aquellos que son más difíciles de falsificar o de obtener ilícitamente. El caso de clientes no residentes requerirá particular atención, y el banco no deberá, en ningún caso, soslayar los procedimientos de verificación de identidad solo porque el nuevo cliente no pueda presentarse a una entrevista. El banco deberá preguntarse por qué el cliente decidió abrir una cuenta en una jurisdicción extranjera.

24. El proceso de identificación del cliente se realiza naturalmente al comienzo de la relación. Para asegurar que los registros se mantengan al día, el banco deberá efectuar revisiones regulares de los mismos (7). Un buen momento para efectuar una revisión de este tipo es cuando se realiza una transacción importante, cuando varían las normas de documentación de un cliente o cuando se produce un cambio relativamente importante en la forma de operar la cuenta. Sin embargo, en cuanto el banco vea que la información que posee sobre un cliente es insuficiente, deberá adoptar las medidas necesarias para obtener rápidamente toda la información necesaria.

25. Los bancos que ofrecen servicios bancarios privados están especialmente expuestos al riesgo de reputación y deberían, por lo tanto, aplicar mayor debida diligencia a dichas operaciones. Las cuentas bancarias privadas, que por definición comprenden un alto grado de confidencialidad, pueden abrirse a nombre de un particular, negocio comercial, fideicomiso, intermediario o una compañía de inversión personalizada. En cada uno de estos casos, el riesgo de reputación puede surgir si el banco no sigue diligentemente los procedimientos KYC establecidos. Todos los clientes y cuentas nuevos deben ser aprobados por, al menos, una persona que cuente con la suficiente autoridad, que no sea el di-

(6) «Metodología de Principios Básicos», Criterio Esencial 2.

(7) La aplicación de nuevas normas KYC a cuentas existentes está siendo actualmente analizada por FATF.

rector de relaciones de banca privada. En caso de existir salvaguardas especiales para proteger internamente la confidencialidad de los clientes de banca privada y sus negocios, los bancos deben asegurar que es posible efectuar un examen y control, por lo menos equivalentes, de esos clientes (por ejemplo, deben estar dispuestos a ser examinados por parte de agentes de verificación de cumplimiento y auditores).

26. Los bancos deberían elaborar «normas claras sobre qué registros deben mantener con la identificación de clientes y de las transacciones individuales y su período de retención» (8). Este tipo de práctica es indispensable para permitir al banco controlar su relación con el cliente, comprender el negocio del cliente y, si fuese necesario, presentar pruebas en el caso de controversias, acción legal o una investigación financiera que pudieran terminar en un proceso penal. Como punto de partida y seguimiento natural del proceso de identificación, los bancos deberían obtener los documentos de identificación de los clientes y guardar copias de los mismos durante, al menos, cinco años desde el cierre de la cuenta. También deberían conservar todos los registros de transacciones financieras, como mínimo, durante cinco años después de efectuada la transacción.

2.1. Requisitos generales de identificación

27. Los bancos tienen que obtener toda la información necesaria para poder establecer, a su entera satisfacción, la identidad de cada nuevo cliente y la finalidad y naturaleza de la relación de negocios deseada. La cantidad y tipo de información dependerá de la clase de solicitante (personal, empresarial, etc.) y del tamaño previsto de la cuenta. Los supervisores nacionales deberían orientar a los bancos en la elaboración de sus propios procedimientos de identificación. El Grupo de Trabajo se propone desarrollar elementos esenciales de los requisitos de identificación de clientes.

28. Cuando, después de abierta una cuenta, surgen problemas de verificación en la relación bancaria que no pueden ser resueltos, el banco debe cerrar la cuenta y devolver el dinero a la fuente de donde lo recibió (9).

29. Si bien la transferencia del saldo de apertura de una cuenta mantenida en nombre del cliente a otro banco sujeto a las mismas normas KYC podría ofrecer cierta tranquilidad, los bancos deberían considerar la posibilidad de que el anterior gerente de cuentas haya solicitado el cierre de la cuenta a raíz de sus sospechas ante ciertas actividades dudosas. Los clientes tienen, naturalmente, el derecho de cambiar de banco; sin embargo, si un banco sospecha de los motivos del cambio (servicios bancarios negados por otro banco), debería aplicar procedimientos de diligencia más rigurosos al solicitante.

(8) «Metodología de Principios Básicos», Criterio Esencial 2.

(9) Sujeto a cualquier ley nacional referente al trámite de transacciones sospechosas.

30. Los bancos no deberían abrir jamás una cuenta ni hacer negocios con un cliente que insista en el anonimato o que dé un nombre ficticio. Tampoco deberían funcionar las cuentas confidenciales numeradas (10) como cuentas anónimas, sino que deberían estar sujetas a los mismos procedimientos KYC que las demás cuentas de clientes, aun cuando la prueba la efectúe personal seleccionado. Considerando que una cuenta numerada puede ofrecer mayor protección para la identidad del titular, esta debe ser conocida por un número suficiente de funcionarios del banco como para ejercer la debida diligencia. Dichas cuentas en ningún caso serán utilizadas para ocultar la identidad del cliente a la función de cumplimiento del banco o a los supervisores.

2.2. Cuestiones específicas relacionadas con la identificación

31. La identificación del cliente comprende otros puntos más detallados que deben ser igualmente tratados. Muchos de ellos están siendo actualmente considerados por FATF, como parte de una revisión general de sus 40 recomendaciones, y el Grupo de Trabajo subraya la necesidad de estar en la misma línea de ese organismo.

2.2.1. Cuentas de fideicomiso, de nominatario y fiduciarias

32. Las cuentas de fideicomiso, de nominatario y fiduciarias pueden ser utilizadas para burlar los procedimientos de identificación del cliente. Aunque en ciertas circunstancias sería admisible aumentar el grado de seguridad para proteger la confidencialidad de los clientes de banca privada, es imprescindible entender su verdadera relación. En este sentido, los bancos deben determinar si el cliente está adoptando el nombre de otro cliente, si está actuando de testaferro, o si obra en nombre de otra persona en calidad de fiduciario, apoderado u otro intermediario. De ser así, se haría necesario recibir pruebas satisfactorias de la identidad de cualquier intermediario y de las personas que representan dichos intermediarios, así como detalles sobre la clase de fideicomiso u otro tipo de acuerdo establecido. Específicamente, la identificación de un fideicomiso debe incluir a los fiduciarios, fideicomitentes/otorgantes y beneficiarios (11).

2.2.2. Vehículos corporativos

33. Los bancos deben estar alerta para evitar que las personas físicas utilicen a las entidades comerciales corporativas como un mé-

(10) En el caso de una cuenta numerada, el nombre del usufructuario es conocido por el banco, pero se sustituye por un número de cuenta o un código en la documentación ulterior.

(11) Los beneficiarios deben ser identificados lo antes posible. Se entiende que no siempre es posible identificar a los beneficiarios de un fideicomiso desde un principio. Por ejemplo, algunos beneficiarios pueden ser niños nonatos y otros pueden depender de la ocurrencia de acontecimientos específicos. Además, siendo los beneficiarios categorías específicas de particulares (por ejemplo, fondos de jubilación de empleados), se les puede tratar como cuentas comunes, según se indica en los párrafos 38-39.

todo para operar cuentas anónimas. Los vehículos tenedores de bienes personales, tales como las compañías comerciales internacionales, pueden dificultar la identificación de los clientes o usufructuarios. El banco debe conocer la estructura de la compañía, determinar el origen de sus fondos e identificar a los usufructuarios y a aquellos que controlan los fondos.

34. Especial cuidado deben tener los bancos al iniciar transacciones comerciales con sociedades que tienen accionistas representados por apoderados o acciones al portador. Se deberán obtener pruebas satisfactorias de la identidad de los usufructuarios de dichas sociedades. En el caso de entidades que poseen gran parte de su capital en forma de acciones al portador, la vigilancia será todavía mayor. Es posible que el banco ignore completamente que las acciones al portador cambiaron de propietario. Es el banco quien tiene la obligación de contar con procedimientos adecuados para controlar la identidad de los usufructuarios. Esto podría requerir la inmovilización de las acciones por parte del banco, manteniéndolas en custodia, por ejemplo.

2.2.3. *Negocios presentados*

35. Los procedimientos de identificación toman tiempo y es natural querer evitarle inconvenientes al nuevo cliente. En algunos países, se ha convertido en una práctica común el que los bancos se fíen de los procedimientos efectuados por otros bancos o presentadores, cuando se está trasladando el negocio. Al hacer esto, los bancos arriesgan confiar demasiado en la debida diligencia que supuestamente han practicado los presentadores. El hecho de depender de la debida diligencia llevada a cabo por un presentador, por muy prestigioso que sea, no libera al banco receptor de la responsabilidad de conocer a sus clientes y sus negocios. Los bancos no deberían fiarse de presentadores que estén sujetos a normas menos exigentes que las que rigen sus propios procedimientos KYC o que no quieren compartir copias de la documentación de debida diligencia.

36. El Comité de Basilea recomienda que los bancos que utilizan presentadores analicen cuidadosamente si son «idóneos» y ejercen la debida diligencia necesaria, de acuerdo a las normas presentadas en este documento. La responsabilidad final de conocer a los clientes recae siempre en los bancos. Los bancos deberían utilizar los siguientes criterios para determinar si pueden o no confiar en un determinado presentador (12):

- el presentador debe cumplir las prácticas mínimas de debida diligencia con clientes contenidas en este documento;

(12) FATF está actualmente estudiando la idoneidad de los presentadores reconocidos.

- los procedimientos de debida diligencia con los clientes del presentador deben ser tan rigurosos como los que el banco hubiera efectuado para el cliente en cuestión;
- el banco debe quedar satisfecho con la fiabilidad de los sistemas que posee el presentador para verificar la identidad del cliente;
- el banco debe llegar a un acuerdo con el presentador para que le permita verificar la debida diligencia practicada por este último en cualquier momento; y
- el presentador debe entregar inmediatamente todos los datos de identificación pertinentes y demás documentación relacionada con la identidad del cliente al banco, quien deberá examinar cuidadosamente todo lo recibido. Dicha información debe quedar a disposición del supervisor y de la unidad de inteligencia financiera u organismo de ejecución equivalente, toda vez que cuenten con la autorización legal necesaria.

Además, los bancos deberían efectuar exámenes periódicos para asegurar que el presentador en quien confían siga cumpliendo los criterios mencionados.

2.2.4. *Cuentas de clientes abiertas por intermediarios profesionales*

37. Cuando un banco sabe o tiene motivos para creer que una cuenta abierta por un intermediario profesional pertenece a un solo cliente, dicho cliente debe ser identificado.

38. No es raro que los bancos mantengan cuentas «comunes» administradas por intermediarios profesionales, en nombre de entidades tales como fondos de inversión, fondos de pensiones y fondos de dinero. Los bancos también mantienen cuentas comunes gestionadas por abogados o corredores de bolsa que representan fondos mantenidos en depósito o en garantía para varios clientes. Cuando los fondos mantenidos por el intermediario no se mezclan en el banco, sino que hay «subcuentas» que pueden atribuirse a cada usufructuario, todos los usufructuarios de la cuenta mantenida por el intermediario deben ser identificados.

39. Cuando los fondos se mezclan los unos con los otros, el banco debe descubrir quiénes son los usufructuarios. Es posible que en ocasiones el banco no necesite ir más allá del intermediario, por ejemplo, cuando este está sujeto a las mismas leyes y procedimientos de regulación y lavado de dinero, y, en particular, a las mismas normas de debida diligencia con respecto a su base de clientes que el banco. Las pautas nacionales de supervisión deben explicar claramente aquellas circunstancias en las que los bancos no necesitan investigar más allá del intermediario. Los bancos deben aceptar dichas cuentas únicamente cuando sea posi-

ble determinar que el intermediario ha efectuado un proceso adecuado de debida diligencia y posee los sistemas y controles necesarios para asignar los haberes de las cuentas comunes a los correspondientes beneficiarios. Al evaluar el proceso de debida diligencia del intermediario, el banco debería aplicar los criterios del párrafo 36, con respecto al negocio presentado, para determinar si puede confiar o no en un intermediario profesional.

40. En los casos en que el intermediario no está facultado para proporcionar al banco la información requerida sobre los beneficiarios [como es el caso de los abogados (13) obligados por el secreto profesional] o cuando dicho intermediario no está sujeto a normas de debida diligencia equivalentes a las mencionadas en este documento o a una legislación exhaustiva contra el lavado de dinero, el banco no debería permitir que el intermediario abra una cuenta.

2.2.5. *Personas del medio político*

41. Las relaciones de negocios con personas que ocupan cargos públicos importantes y con personas o sociedades claramente relacionadas con ellas pueden exponer al banco a riesgos de reputación o legales considerables. Dichas personas del medio político (PEP, por sus siglas en inglés) son personalidades que cumplen o han cumplido funciones públicas destacadas, incluyendo jefes de Estado o de gobierno, líderes políticos de larga trayectoria, altos cargos del gobierno, del poder judicial o de las fuerzas armadas, importantes ejecutivos de empresas del Estado y miembros influyentes de los partidos políticos. Siempre existe la posibilidad, sobre todo en los países en que la corrupción es generalizada, de que dichas personas abusen de su poder para su propio enriquecimiento ilícito a través del soborno, malversación de fondos, etc.

42. El hecho de aceptar y administrar fondos recibidos de estas personas corruptas dañará seriamente la reputación del banco y puede socavar la confianza del público en las normas éticas de todo un centro financiero, ya que los escándalos de este tipo son objeto de una extensa cobertura en los medios de comunicación y una fuerte reacción política, aun cuando el origen ilegal de los bienes sea difícil de probar. Además, el banco podría verse sometido a costosas solicitudes de información y órdenes de embargo de bienes por parte de las fuerzas del orden o las autoridades judiciales (incluyendo procedimientos de asistencia mutua internacional en asuntos criminales) o enfrentarse a juicios por daños y perjuicios interpuestos por el Estado o las víctimas de un régimen. En ciertas circunstancias, el banco o sus propios dirigentes y empleados pueden estar expuestos a acusaciones de lavado de dinero si sabían o deberían haber sabido que los fondos provenían de la corrupción u otros delitos graves.

(13) FATF está actualmente examinando los procedimientos KYC que rigen las cuentas abiertas por abogados en nombre de sus clientes.

43. Algunos países han modificado recientemente sus leyes y reglamentos, o están en proceso de hacerlo, con el fin de penalizar la corrupción activa de empleados públicos y funcionarios de Estado extranjeros, de acuerdo con el convenio internacional pertinente (14). En estas jurisdicciones, la corrupción extranjera se vuelve un delito predicado para el lavado de dinero, aplicándose por consiguiente todas las leyes y reglamentos pertinentes contra el lavado de dinero (por ejemplo, notificación de transacciones sospechosas, prohibición de notificación del cliente, congelación interna de fondos, etc.). Empero, incluso sin un fundamento legal tan explícito en el derecho penal, resulta claramente indeseable, inmoral e incompatible con la conducción apropiada de las operaciones bancarias, aceptar o mantener una relación comercial si el banco sabe o debería suponer que los fondos provienen de la corrupción o uso indebido de bienes públicos. De ahí la imperiosa necesidad de que el banco identifique totalmente a toda persona sospechosa de ser una PEP, así como a las personas y sociedades relacionadas con ella, antes de establecer cualquier tipo de relación comercial.

44. Los bancos deben recabar suficiente información de un cliente nuevo y verificar la información de dominio público para determinar si el cliente es o no una persona del medio político. Los bancos deben investigar el origen de los fondos antes de aceptar a una PEP. La decisión de abrir una cuenta para una PEP se tomará al más alto nivel de dirección del banco.

2.2.6. *Clientes no presentes*

45. Los bancos reciben cada vez más solicitudes de apertura de cuentas en nombre de clientes que no pueden presentarse para una entrevista personal. La expansión reciente de la banca por correo, telefónica e informática ha incrementado lo que antes era una práctica limitada a clientes no residentes. Estos clientes, a quienes el banco no conoce cara a cara, deben ser sometidos a procedimientos de identificación y normas de seguimiento continuo tan eficaces como los aplicables a los demás clientes. Una de las cuestiones que ha surgido recientemente es la posibilidad de una verificación independiente por parte de terceros acreditados. La identificación de clientes no presentes está siendo analizado por FATF, así como en el contexto de la modificación de la Directiva CEE de 1991.

46. Un ejemplo típico de este tipo de clientes es aquel que desea realizar operaciones bancarias electrónicas por Internet o una tecnología similar. La banca electrónica incorpora actualmente una variada gama de productos y servicios a través de redes de telecomunicación. La naturaleza impersonal y sin límites de la banca electrónica, combinada con la velocidad de la transacción, dificulta inevitablemente la identificación y

(14) Ver el Convenio OCDE de «Lucha contra el Soborno de Funcionarios Públicos Extranjeros en Transacciones Comerciales Internacionales», adoptado por la Conferencia Negociadora el 21 de noviembre de 1997.

verificación del cliente. Por el momento, los supervisores esperan que los bancos evalúen de forma activa los diversos riesgos que representan las tecnologías emergentes y que elaboren procedimientos de identificación del cliente que tengan en cuenta dichos riesgos (15).

47. Si bien tanto los clientes presentes como los no presentes pueden presentar la misma documentación, resulta más difícil asignar al cliente su documentación correspondiente en el segundo caso. El problema de la verificación es todavía más difícil para la banca telefónica y electrónica.

48. Al aceptar a clientes no presentes:

- los bancos deben aplicar procedimientos de identificación del cliente tan eficaces como los utilizados en el caso de clientes que sí pueden presentarse para entrevistas; y
- debe haber medidas específicas y adecuadas para reducir el riesgo más alto.

Los ejemplos de medidas para reducir el riesgo incluyen:

- certificación de la documentación presentada;
- solicitud de documentos adicionales para complementar los requisitos de los clientes presentes;
- contacto independiente del banco con el cliente;
- presentación a través de terceros, por ejemplo, mediante un presentador sujeto a los criterios establecidos en el párrafo 36; o
- solicitar que se lleve a cabo el primer pago a través de una cuenta a nombre del cliente en otro banco cuyas normas de debida diligencia con los clientes sean similares.

2.2.7. Banca corresponsal

49. La banca corresponsal consiste en la provisión de servicios bancarios por un banco (el «banco corresponsal») a otro banco (el «banco representado»). Las cuentas corresponsales, utilizadas en todo el mundo, permiten a los bancos realizar negocios y proveer servicios que no ofrecen directamente. Las cuentas corresponsales que requieren especial atención son aquellas que están relacionadas con la provisión de servicios en jurisdicciones en las que los bancos representados no

(15) El Grupo de Banca Electrónica del Comité de Basilea emitió un documento sobre principios de gestión de riesgos para banca electrónica en mayo de 2001.

tienen presencia física. Si los bancos no aplican el nivel necesario de debida diligencia a dichas cuentas, se exponen a todos los riesgos identificados anteriormente en este documento y podrían inclusive encontrarse en la situación de estar manteniendo o transmitiendo dinero ligado a la corrupción, fraude u otra actividad ilegal.

50. Los bancos deberían recabar suficiente información sobre sus bancos representados para conocer la clase de negocio que dirigen. En este sentido, los factores a considerar son: información sobre la gerencia del banco representado, sus actividades comerciales principales, su ubicación y sus medidas de prevención y detección de lavado de dinero; el propósito de la cuenta; la identidad de otras entidades que utilizarán los servicios de banca corresponsal; y la situación de la regulación y supervisión bancaria en el país del banco representado. Solo los bancos extranjeros efectivamente supervisados por autoridades competentes deben ser considerados para establecer relaciones de corresponsalía. Por su parte, los bancos representados deben contar con políticas de aceptación de clientes y KYC eficaces.

51. En particular, los bancos deberían negarse a establecer o continuar una relación de banca corresponsal con un banco constituido en una jurisdicción en la que no tienen ninguna presencia física y que no esté afiliado a un grupo financiero regulado (es decir, bancos ficticios). Los bancos deben estar especialmente vigilantes cuando mantienen relaciones con bancos representados ubicados en jurisdicciones con normas KYC deficientes o identificadas como «no dispuestas a cooperar» en la lucha contra el lavado de dinero. Los bancos deben confirmar que sus bancos representados cuentan con normas de debida diligencia como las estipuladas en este documento y que emplean los mejores procedimientos en las transacciones efectuadas a través de cuentas de corresponsalía.

52. Un riesgo al que los bancos deben prestar especial atención es el uso de las cuentas de corresponsalía por parte de terceros, para sus propios negocios (por ejemplo, las cuentas de transferencia de pagos). Estos tipos de arreglos dan origen a la mayoría de las consideraciones aplicables a los negocios presentados y deberían ser tratados conforme a los criterios descritos en el párrafo 36.

3. Seguimiento continuo de cuentas y transacciones

53. El seguimiento continuo es un aspecto esencial para los procedimientos KYC eficaces. Los bancos solo podrán controlar y reducir sus riesgos si conocen las actividades habituales y razonables de las cuentas de sus clientes y pueden así identificar las transacciones que se salen del patrón de actividad regular de una cuenta. Sin estos conocimientos, los bancos probablemente no podrán cumplir con su deber de notificar las transacciones sospechosas a las autoridades pertinentes en aquellos casos en los que tienen obligación de hacerlo. La extensión del

seguimiento dependerá del riesgo, por lo que el banco ha de contar con sistemas para detectar patrones de actividad anómalos o sospechosos para todas las cuentas. Esto es posible mediante la fijación de límites para cada clase o categoría especial de cuentas. Las transacciones que sobrepasen estos límites serán objeto de una atención especial. Ciertos tipos de transacciones deberían alertar a los bancos sobre la posibilidad de que el cliente esté realizando actividades poco usuales o sospechosas. Entre ellas se incluyen las transacciones que no tienen ningún sentido económico ni comercial aparente, o las que comprenden grandes cantidades de depósitos en efectivo que no corresponden a las transacciones normales y esperadas del cliente. Un movimiento bancario de gran envergadura que no guarde relación con el tamaño del saldo podría indicar que los fondos están siendo «lavados» a través de la cuenta. Los ejemplos de actividades sospechosas pueden ser muy útiles para los bancos y deberían formar parte de los procedimientos y orientaciones contra el lavado de dinero de una jurisdicción.

54. El seguimiento de las cuentas de alto riesgo deberá ser más intenso. Cada banco debe fijar indicadores clave para dichas cuentas, considerando los antecedentes del cliente, como su país de origen y la procedencia de sus fondos, el tipo de transacciones y otros factores de riesgo. Para las cuentas de mayor riesgo:

- los bancos deben asegurarse de que cuentan con sistemas de información gerencial adecuados que ofrezcan a los directivos y agentes encargados de cumplimiento del banco la información necesaria para identificar, analizar y seguir eficazmente las cuentas de alto riesgo. Los informes necesarios podrían ser informes sobre ausencia de documentación de apertura de cuenta, transacciones anómalas efectuadas a través de una cuenta de cliente y sumas del total de la relación de un cliente con el banco.
- la alta gerencia encargada de las transacciones de banca privada debe conocer las circunstancias personales de los clientes de alto riesgo del banco y estar alerta ante las fuentes de información de terceros. Las transacciones importantes que realizan estos clientes deben ser aprobadas por un director de alto rango.
- los bancos deben elaborar políticas y directivas internas claras, procedimientos y controles, así como vigilar de cerca las relaciones comerciales con PEP y otras personalidades o con personas y sociedades claramente relacionadas o asociadas con ellas (16). Como no todas las PEP son identificables desde un principio y, además, los

(16) Sería poco realista pretender que el banco conozca o investigue todas las conexiones familiares, políticas o comerciales de un cliente extranjero. La necesidad de investigar las sospechas dependerá de la cantidad de fondos o movimientos bancarios, patrón de transacciones, antecedentes económicos, reputación del país, verosimilitud de las explicaciones del cliente, etc. Cabe destacar, sin embargo, que las PEP (o, más bien, sus familiares y amigos) no necesariamente se presentarán a sí mismas como tales, sino más bien como personas de negocios corrientes (aunque adineradas), disimulando el hecho de que el alto puesto que ocupan en una empresa legítima se debe únicamente a la relación privilegiada que mantienen con el titular del cargo público.

clientes pueden adquirir dicho estatus con el correr del tiempo, el banco debería programar exámenes regulares de, al menos, los clientes más importantes.

4. Gestión de riesgos

55. Los procedimientos KYC eficaces comprenden rutinas de vigilancia adecuada de la gestión, sistemas y controles relacionados, distribución de responsabilidades, capacitación y otras políticas afines. El Consejo de Administración del banco debe estar totalmente comprometido con un programa KYC eficaz, estableciendo procedimientos apropiados y asegurando la eficacia de los mismos. Es necesario asignar responsabilidades explícitas dentro del banco para garantizar que las políticas y procedimientos sean gestionados correctamente y estén, como mínimo, a la altura de la práctica local de supervisión. Los canales de notificación de transacciones sospechosas deben estar claramente especificados por escrito y han de estar en conocimiento de todo el personal. Otro requisito son los procedimientos internos destinados a determinar si las obligaciones del banco, a partir de regímenes de notificación de actividades sospechosas reconocidos, exigen que la transacción sea notificada a las autoridades policiales o de supervisión.

56. Las funciones de auditoría interna y cumplimiento de los bancos desempeñan un papel importante en la evaluación y aplicación de las políticas y procedimientos KYC. En términos generales, la función de cumplimiento debe realizar una evaluación independiente de las políticas y procedimientos del banco, incluyendo los requisitos legales y de regulación. Sus responsabilidades deberían incluir el seguimiento continuo del desempeño del personal, mediante verificación por muestreo del cumplimiento y el análisis de informes de anomalías, para alertar a la alta dirección o al Consejo de Administración del banco si considera que la dirección no está abordando los procedimientos KYC de forma responsable.

57. La auditoría interna desempeña una función importante, al evaluar de forma independiente la gestión y los controles del riesgo, cumpliendo con su responsabilidad ante el Comité Auditor del Consejo de Administración o un órgano de vigilancia similar, mediante evaluaciones periódicas de la efectividad del cumplimiento de las políticas y procedimiento KYC, incluyendo la adecuada capacitación de personal. La dirección del banco debe asegurar que las funciones de auditoría estén dotadas de personal experto en dichas políticas y procedimientos. Además, los auditores internos deben ser proactivos en el seguimiento de los resultados de su trabajo y sus críticas.

58. Todos los bancos deberían contar con un programa permanente de capacitación de empleados para que el personal del banco esté bien entrenado en los procedimientos KYC. La programación y el contenido de la capacitación para el personal de las distintas secciones se adaptarán a las necesidades específicas de cada banco. La capacitación tendrá

un enfoque distinto según se trate de personal nuevo, personal operacional, personal de cumplimiento o funcionarios del banco que atienden a nuevos clientes. Para personal nuevo, la capacitación se centrará en la importancia de las políticas KYC y los requisitos básicos en el banco. El personal operacional que trata directamente con el público debe estar formado para verificar la identidad de los nuevos clientes, ejercer permanentemente debida diligencia en el manejo de las cuentas de los clientes y detectar patrones de actividad sospechosa. El programa de capacitación deberá incluir cursos regulares de actualización para asegurar que el personal no pierda de vista sus responsabilidades y se mantenga al tanto de los nuevos acontecimientos. Es de suma importancia que todo el personal comprenda la necesidad de aplicar permanentemente políticas KYC. Una cultura que promueva esta comprensión es la clave de una ejecución de políticas KYC exitosa.

59. En muchos países, los auditores externos también cumplen un papel importante en fiscalizar los controles y procedimientos internos de los bancos, y en confirmar que cumplen con las prácticas de supervisión.

IV. EL PAPEL DE LOS SUPERVISORES

60. A partir de las actuales normas KYC internacionales, los supervisores nacionales deberían elaborar prácticas de supervisión que rijan los programas KYC de los bancos. Los elementos esenciales presentados en este documento deberían servir de orientación para que los supervisores procedan con la tarea de diseñar o mejorar las prácticas nacionales de supervisión.

61. Además de exponer elementos básicos para orientar a los bancos, los supervisores tienen la responsabilidad de controlar que los bancos utilicen procedimientos KYC seguros y mantengan estándares éticos y profesionales elevados. Los supervisores deberían confirmar la existencia de controles internos adecuados en el banco y la conformidad con las orientaciones de supervisión y regulación emitidas. El proceso de supervisión incluirá, por un lado, la evaluación de las políticas y procedimientos y, por otro, el examen de archivos de clientes y el muestreo de algunas cuentas. Los supervisores deben tener siempre el derecho de revisar toda la documentación relacionada con las cuentas mantenidas en su jurisdicción, incluyendo cualquier análisis realizado por el banco para detectar transacciones anómalas o sospechosas.

62. Los supervisores tienen el deber no solo de asegurar que los bancos apliquen normas KYC estrictas para proteger su propia seguridad y solidez, sino para proteger también la integridad del sistema bancario nacional (17). Los supervisores deben dejar claro que adoptarán

(17) Muchos supervisores tienen además el deber de informar sobre cualquier transacción sospechosa, anómala o ilegal detectada, por ejemplo, durante inspecciones en el sitio.

todas las medidas necesarias (que podrían ser severas y públicas, si las circunstancias así lo exigen) para actuar en contra de los bancos y altos cargos que no sigan sus propios procedimientos y requisitos de regulación internos. Además, los supervisores deben asegurar que los bancos tienen conocimiento de las transacciones relacionadas con otras jurisdicciones cuyas normas son consideradas inadecuadas, y que las vigilan de cerca. El FATF y algunas autoridades nacionales han elaborado una lista de países y jurisdicciones que poseen ciertas disposiciones legales y administrativas que no cumplen las normas internacionales de lucha contra el lavado de dinero. Esta información debería formar parte de las políticas y procedimientos KYC de un banco.

V. APLICACIÓN DE LAS NORMAS K.Y.C. EN UN CONTEXTO TRANSTERRITORIAL

63. Los supervisores de todo el mundo deberían esforzarse por seguir las normas internacionales para elaborar y aplicar sus propias normas KYC nacionales, con el fin de evitar un posible arbitraje de regulación y proteger la integridad del sistema bancario local e internacional. La aplicación y valoración de dichas normas ponen a prueba la voluntad de los supervisores para cooperar entre ellos de forma práctica, así como la habilidad de los bancos para controlar los riesgos de su grupo. Esta es una tarea difícil, tanto para los bancos como para los supervisores.

64. Los supervisores esperan que los bancos sigan un nivel mínimo aceptado de políticas y procedimientos KYC en sus operaciones locales y extranjeras. La supervisión de la banca internacional es eficaz únicamente si se la lleva a cabo en base consolidada. Por otro lado, el riesgo de reputación, así como los demás riesgos a los que está expuesta la banca, no conocen fronteras. Los bancos matriz deben comunicar sus políticas y procedimientos a sus sucursales y filiales en el extranjero, incluidas las entidades no bancarias, como las sociedades fiduciarias, e implantar un sistema de pruebas de verificación del cumplimiento de las normas KYC, tanto en el país de origen como en el de acogida, para que sus programas funcionen eficazmente en todo el mundo. Dichas pruebas de cumplimiento serán además verificadas por los auditores externos y los supervisores, siendo por lo tanto importante que la documentación KYC esté convenientemente archivada y disponible para su inspección. En lo que respecta a verificaciones de cumplimiento, los supervisores y auditores externos deberían, en la mayoría de casos, examinar los sistemas y controles y estudiar el seguimiento de las cuentas y transacciones de los clientes como parte de un proceso de muestreo.

65. Por pequeño que sea el establecimiento en el extranjero, debe tener un alto cargo encargado de asegurar que el personal conozca y cumpla los procedimientos KYC acordes con las normas tanto del país de origen como del de acogida. Si bien esta persona será el primer responsable de esta tarea, debe estar apoyado por auditores internos y agentes de cumplimiento de la oficina local y central, según proceda.

66. Cuando las normas KYC mínimas del país de origen y del país de acogida difieren, las sucursales y filiales de la jurisdicción de acogida aplicarán las normas más estrictas. En general, no debería haber ningún impedimento para que el banco pueda adoptar normas más estrictas que las requeridas localmente. Sin embargo, si las leyes y reglamentos locales (especialmente, las disposiciones de confidencialidad) prohibieran la aplicación de las normas KYC del país de origen, aunque estas sean más estrictas, los supervisores del país de acogida deberán intentar por todos los medios hacer que se enmienden dichas leyes y reglamentos. Hasta que esto ocurra, las sucursales y filiales en el extranjero tendrán que cumplir las normas del país de acogida, informando a su oficina central o banco matriz y a su supervisor nacional de la diferencia en cuestión.

67. Las jurisdicciones con este tipo de impedimentos normalmente atraen a elementos criminales y, por ende, los bancos deben tomar en cuenta el alto riesgo de reputación que representa tener actividades en ellas. Los bancos matriz deberían contar con un procedimiento para examinar la vulnerabilidad de las unidades individuales de operación y aplicar medidas de salvaguardia suplementarias donde sea necesario. En casos extremos, los supervisores deberían pensar en aplicar controles adicionales sobre los bancos que operan en esas jurisdicciones y, en última instancia, sugerir su retirada.

68. Durante las inspecciones *in situ*, los supervisores o auditores del país de origen no deberían tener ningún impedimento para verificar el cumplimiento de las políticas y procedimientos KYC. Esta verificación requerirá una revisión de los archivos de clientes y algún muestreo aleatorio de cuentas. Los supervisores del país de origen deben tener acceso a la información sobre las cuentas de clientes del muestreo, en la medida en que sea necesario para realizar una evaluación de la aplicación de las normas KYC y una valoración de las prácticas de gestión de riesgo, y no deben verse constreñidos por leyes locales de secreto bancario. No deberían existir impedimentos cuando el supervisor del país de origen requiera informes consolidados sobre las concentraciones de depósitos o prestatarios, o la notificación de fondos en administración. Además, con el fin de controlar las concentraciones de depósitos o el riesgo de financiación producido por la retirada de depósitos, los supervisores del país de origen pueden aplicar pruebas de importancia relativa y establecer algunos límites, de manera que, si el depósito de un cliente sobrepasa cierto porcentaje del balance general, el banco tenga que informar al supervisor del país de origen. Sin embargo, son necesarias salvaguardas para asegurar que la información sobre cuentas individuales se utiliza únicamente para fines lícitos de supervisión y pueda ser protegida por el receptor en forma satisfactoria. En este contexto, podría ser útil una declaración de cooperación mutua (18) para facilitar el intercambio de información entre los dos supervisores.

(18) Véase el documento *Essential elements of a statement of cooperation between banking supervisors*, de mayo de 2001, producido por el Comité de Basilea.

69. En ciertos casos, puede surgir un conflicto serio entre las políticas KYC impuestas por la autoridad de origen al banco matriz y lo que está permitido en una oficina transterritorial. Las leyes locales podrían, por ejemplo, impedir las inspecciones de los agentes de cumplimiento, auditores internos o supervisores nacionales del banco matriz, o permitir a los clientes del banco utilizar nombres ficticios o ocultarse detrás de agentes o intermediarios que no están autorizados a revelar la identidad de sus clientes. En estos casos, el supervisor del país de origen debe comunicarse con el supervisor de acogida para confirmar si existen realmente impedimentos legales y si son aplicables fuera del territorio nacional. Si los impedimentos resultan ser insuperables, y no hay arreglo alternativo posible, el supervisor de origen debe informar al supervisor de acogida de que el banco podría decidir cerrar la operación en cuestión, por voluntad propia o por orden del supervisor de origen. En última instancia, cualquier arreglo que sirva de sostén para inspecciones *in situ* de este tipo debería ofrecer un mecanismo que permita una valoración satisfactoria para el supervisor de origen. Las declaraciones de cooperación o los memoranda de entendimiento que expliquen la mecánica de los arreglos podrían ser útiles a tal efecto. El acceso de los supervisores de origen a la información debe ser lo menos limitado posible, permitiendo a dichos supervisores, como mínimo, examinar libremente las políticas y procedimientos generales del banco con respecto a la debida diligencia con clientes y al tratamiento de las sospechas.

ANEXO 1

EXTRACTOS DE METODOLOGÍA DE PRINCIPIOS BÁSICOS

Principio 15: Los supervisores bancarios deben determinar si los bancos cuentan con políticas, prácticas y procedimientos adecuados, incluyendo reglas estrictas de «conozca a su cliente», que promueven normas éticas y profesionales estrictas en el sector financiero y evitan que el banco sea utilizado, de forma intencional o no, por elementos criminales.

Criterios esenciales

1. El supervisor determina si los bancos cuentan con políticas, prácticas y procedimientos adecuados que promueven normas éticas y profesionales estrictas y evitan que el banco sea utilizado, de forma intencional o no, por elementos criminales. Esto incluye la prevención y detección de actividad criminal o fraude y la notificación de esas actividades sospechosas a las autoridades competentes.
2. El supervisor determina si los bancos han documentado y aplicado políticas de identificación de los clientes y de las personas que actúan en nombre de ellos, como parte de su programa contra el lavado de dinero. Existen reglas claras sobre qué registros mantener sobre la identificación de clientes y sobre transacciones individuales y su período de retención.
3. El supervisor determina si los bancos cuentan con procedimientos formales para reconocer transacciones potencialmente sospechosas. Estos podrían incluir autorización adicional para depósitos o retiradas de grandes cantidades de efectivo (o similares) y procedimientos especiales para transacciones anómalas.
4. El supervisor determina si los bancos nombran a un funcionario de nivel superior con la responsabilidad explícita de asegurar que las políticas y procedimientos del banco estén, como mínimo, de acuerdo con las estipulaciones legales y reguladoras locales de lucha contra el lavado de dinero.
5. El supervisor determina si los bancos cuentan con procedimientos claros a través de los cuales el personal pueda informar a la autoridad responsable del cumplimiento de la política contra el lavado de dinero de las transacciones sospechosas, y si estos procedimientos han sido comunicados a todo el personal.
6. El supervisor determina si los bancos han establecido líneas de comunicación con la gerencia y con una función de seguridad (custodia) interna para la notificación de problemas.

7. Además de notificar a las autoridades criminales apropiadas, los bancos informan al supervisor de las actividades sospechosas e incidentes de fraude importantes para la seguridad, solidez o reputación del banco.
8. Las leyes, reglamentos y políticas del banco garantizan que el miembro del personal que informe, de buena fe, al oficial responsable, a la persona encargada de la seguridad interna o directamente a la autoridad pertinente sobre transacciones sospechosas, no estará sujeto a responsabilidad alguna.
9. El supervisor verifica periódicamente la suficiencia de los controles contra el lavado de dinero del banco y su sistema de prevención, identificación y notificación del fraude. El supervisor tiene suficientes potestades (reguladoras o de procesamiento penal) para actuar contra un banco que no cumpla sus obligaciones de lucha contra el lavado de dinero.
10. El supervisor puede compartir, ya sea de forma directa o indirecta, información relacionada con actividades criminales sospechadas o reales con las autoridades locales y extranjeras de supervisión del sector financiero.
11. El supervisor determina si los bancos cuentan con una declaración de política sobre ética y conducta profesional, y si esta ha sido debidamente comunicada al personal.

Criterios adicionales

1. Las leyes o reglamentos incorporan prácticas seguras internacionales, tales como la conformidad con las Cuarenta Recomendaciones del Grupo de Acción Financiera Internacional (FATF), emitidas en 1990 (revisadas en 1996).
2. El supervisor determina que el personal del banco está bien entrenado en la detección y prevención del lavado de dinero.
3. El supervisor tiene la obligación legal de informar a las autoridades criminales competentes de cualquier transacción sospechosa.
4. El supervisor puede compartir, directa o indirectamente, información relacionada con actividades delictivas, presuntas o reales, con las autoridades judiciales competentes.
5. Si no es la responsabilidad de otro organismo, el supervisor contará con personal interno especializado en fraude financiero y obligaciones contra el lavado de dinero.

ANEXO 2

EXTRACTOS DE LAS RECOMENDACIONES F.A.T.F.

C. Papel del sistema financiero en la lucha contra el lavado de dinero

Normas para la identificación del cliente y el mantenimiento de registros

10. Las instituciones financieras no deberían mantener cuentas anónimas ni cuentas bajo nombres obviamente ficticios: deberían estar obligadas (por ley, por reglamento, por acuerdos entre las autoridades de supervisión y las instituciones financieras o por acuerdos de autorregulación entre instituciones financieras) a identificar (mediante un documento identificador oficial o algún otro documento fiable) y registrar la identidad de sus clientes, ya sean estos ocasionales o habituales, en el momento de establecer relaciones de negocios o llevar a cabo transacciones (en concreto, al abrir cuentas o libretas de ahorro, realizar operaciones fiduciarias, alquilar cajas de seguridad, efectuar grandes transacciones en efectivo). A fin de cumplir los requisitos de identificación de personas jurídicas, las instituciones financieras deberían, cuando sea necesario, adoptar medidas:
 - (i) Para verificar la existencia y estructura jurídica del cliente, obteniendo para ello, ya sea de un registro público o del cliente o de ambos, una prueba de su constitución, con información acerca del nombre del cliente, forma jurídica, dirección, directores y disposiciones sobre la facultad de vincular legalmente a la entidad.
 - (ii) Para verificar que toda persona que diga actuar en nombre del cliente esté debidamente autorizada y para identificar a esa persona.
11. Las instituciones financieras deberían adoptar medidas razonables para obtener información acerca de la verdadera identidad de las personas en nombre de quienes se abre una cuenta o se lleva a cabo una transacción, en el caso de tener dudas sobre si estos clientes actúan en nombre propio, como, por ejemplo, en el caso de sociedades domiciliarias (es decir, instituciones, empresas, fundaciones, fideicomisos, etc., que no realizan actividades comerciales, ni productoras, ni ninguna otra forma de operación comercial en el país donde se encuentra ubicado su domicilio social).
12. Las instituciones financieras deberían guardar, durante al menos cinco años, todos los registros necesarios de las transacciones locales e internacionales realizadas, para poder responder rápidamente

a las solicitudes de información de las autoridades competentes. Los registros deben ser suficientes como para permitir la reconstrucción de las transacciones individuales (incluyendo, en su caso, las cantidades y tipos de moneda utilizados), con el fin de ofrecer pruebas acusatorias de conducta criminal, si fuese necesario. Las instituciones financieras deberían guardar los registros de identificación de clientes (por ejemplo, copias o registros de documentos oficiales de identidad, tales como pasaportes, tarjetas de identificación, licencias de conducir o documentos similares), los archivos de cuentas y la correspondencia comercial durante, al menos, cinco años después de cerrada la cuenta. Estos documentos deberían estar a disposición de las autoridades locales competentes en el contexto de procesos e investigaciones penales pertinentes.

13. Los países deberían centrarse de modo especial en las amenazas de lavado de dinero inherentes a las tecnologías nuevas o en desarrollo, que pueden favorecer el anonimato, y adoptar medidas, si fuese necesario, para evitar su uso en planes de lavado de dinero.

Aumento de la diligencia en las instituciones financieras

14. Las instituciones financieras deberían prestar especial atención a todas las transacciones complejas o extraordinariamente grandes y a todos los patrones de transacciones poco comunes, que no tienen ningún objetivo económico aparente ni propósito legítimo visible. Es necesario examinar, en la medida de lo posible, los antecedentes y finalidad de dichas transacciones, dejando las averiguaciones realizadas por escrito para asistir a los supervisores, auditores y autoridades del orden público.
15. Si las instituciones financieras sospechan que determinados fondos proceden de actividades criminales, deberían estar obligadas a notificar inmediatamente sus sospechas a las autoridades competentes.
16. Las instituciones financieras, sus directores, agentes y empleados deberían estar protegidos mediante disposiciones legales de toda responsabilidad penal o civil derivada de la violación de cualquier restricción a la revelación de información, impuesta por contrato o por disposición legislativa, reguladora o administrativa, al notificar de buena fe sus sospechas a las autoridades competentes, incluso en el caso de no conocer exactamente el tipo de actividad criminal en cuestión, e independientemente de si se produjo o no tal actividad ilegal.
17. Las instituciones financieras, sus directores, agentes y empleados no deberían alertar a sus clientes o, cuando proceda, no debería permitírseles alertar a sus clientes, cuando se entrega a las autoridades información que les concierne.

18. Las instituciones financieras deberían seguir las instrucciones de las autoridades competentes al notificar sus sospechas.
19. Las instituciones financieras deberían elaborar programas para combatir el lavado de dinero. Estos programas deberían incluir, como mínimo:
 - (i) la elaboración de políticas, procedimientos y controles internos, incluyendo la designación de agentes de cumplimiento a nivel de dirección, y sistemas adecuados de preselección para asegurar normas estrictas de contratación de empleados;
 - (ii) un programa permanente de capacitación de personal;
 - (iii) una función de auditoría para probar el sistema.

*LAS CUARENTA
RECOMENDACIONES*

Grupo de Acción Financiera
sobre el Blanqueo de Capitales

INTRODUCCIÓN

El Grupo de Acción Financiera Internacional sobre el Blanqueo de Capitales (GAFI) es un organismo intergubernamental cuyo propósito es elaborar y promover medidas para combatir el blanqueo de capitales, proceso consistente en ocultar el origen ilegal de productos de naturaleza criminal. Estas medidas intentan impedir que dichos productos se utilicen en actividades delictivas futuras y que afecten a las actividades económicas lícitas.

El GAFI está actualmente integrado por 29 países (1) y dos organismos internacionales (2). Entre sus miembros se encuentran los principales centros financieros de Europa, América del Norte y del Sur, y Asia. Es un organismo multidisciplinario (condición fundamental para luchar contra el blanqueo de capitales), que reúne a expertos encargados de adoptar medidas sobre cuestiones jurídicas, financieras y operativas.

La necesidad de abarcar todos los aspectos relevantes de la lucha contra el blanqueo de capitales se refleja en el conjunto de las Cuarenta Recomendaciones que el GAFI ha decidido aplicar y cuya adopción se promueve en todos los países. Las Recomendaciones se redactaron inicialmente en 1990. En 1996, las Cuarenta Recomendaciones se revisaron para reflejar la experiencia de los últimos seis años y los cambios experimentados en materia de blanqueo de capitales (3).

Las Cuarenta Recomendaciones constituyen el marco básico de lucha contra el blanqueo de capitales y han sido concebidas para una aplicación universal. Abarcan el sistema jurídico penal y policial, el sistema financiero y su reglamentación, y la cooperación internacional.

El GAFI reconoció, desde el principio, que los países tienen sistemas jurídicos y financieros diferentes, de modo que todos ellos no pueden adoptar las mismas medidas. Por lo tanto, las Recomendaciones constituyen los principios de acción en materia de blanqueo de capitales que los países deben aplicar, de acuerdo con sus circunstancias particulares y su marco constitucional, dejando a los países cierta flexibilidad en su

(1) La referencia hecha a «países» en este documento debe entenderse como aplicada también a «territorios» o «jurisdicciones». Los veintinueve países y gobiernos miembros del GAFI son: Alemania, Argentina, Australia, Austria, Bélgica, Brasil, Canadá, Dinamarca, España, Estados Unidos, Finlandia, Francia, Grecia, Hong Kong, China, Irlanda, Islandia, Italia, Japón, Luxemburgo, Méjico, Noruega, Nueva Zelanda, Reino de los Países Bajos, Portugal, Reino Unido, Singapur, Suecia, Suiza y Turquía.

(2) Los dos organismos internacionales son la Comisión Europea y el Consejo de Cooperación del Golfo.

(3) Entre 1990 y 1995, el GAFI elaboró también varias Notas Interpretativas, que tienen por objeto aclarar la aplicación de determinadas Recomendaciones. Algunas de estas Notas Interpretativas han sido actualizadas en el marco de la Revisión de las Recomendaciones para indicar los cambios introducidos en las Recomendaciones. El 2 de julio de 1999, el GAFI adoptó una nueva Nota Interpretativa relativa a la Recomendación 15.

aplicación, en lugar de obligar a cumplir todos los detalles. Las medidas no son especialmente complicadas o difíciles, siempre que exista voluntad política de actuar. Tampoco comprometen la libertad de llevar a cabo operaciones lícitas, ni amenazan el desarrollo económico.

Los países del GAFI se han comprometido claramente a aceptar la disciplina de estar sujetos a una vigilancia multilateral y a evaluaciones mutuas. La aplicación de las cuarenta Recomendaciones por parte de los países miembros se supervisa a través de un doble enfoque: un ejercicio anual de autoevaluación y un proceso más detallado de evaluación mutua, según el cual cada país miembro está sujeto a un examen sobre el terreno. Además, el GAFI realiza exámenes horizontales de las medidas adoptadas para aplicar determinadas Recomendaciones.

Estas medidas son esenciales para el establecimiento de un marco eficaz contra el blanqueo de capitales.

LAS CUARENTA RECOMENDACIONES

A. MARCO GENERAL DE LAS RECOMENDACIONES

1. Cada país debería tomar medidas inmediatas para ratificar y aplicar sin restricciones la Convención de las Naciones Unidas contra el tráfico ilícito de estupefacientes y sustancias sicotrópicas (Convención de Viena).
2. Las leyes de confidencialidad de las instituciones financieras deberían ser concebidas de modo que no dificulten la aplicación de las Recomendaciones.
3. Un programa eficaz de lucha contra el blanqueo de capitales debería incluir una mejora de la cooperación multilateral y de la asistencia jurídica mutua en las investigaciones y los procesos en casos de blanqueo de capitales, así como en procedimientos de extradición, cuando sea posible.

B. PAPEL DE LOS SISTEMAS JURÍDICOS NACIONALES EN LA LUCHA CONTRA EL BLANQUEO DE CAPITALES

Ámbito de aplicación del delito de blanqueo de capitales

4. Cada país debería tomar las medidas necesarias, entre ellas las legislativas, para poder tipificar como delito el blanqueo de capitales, tal y como se prevé en la Convención de Viena. Cada país debería ampliar el delito de blanqueo de capitales procedente del tráfico de estupefacientes al blanqueo de capitales procedentes de delitos graves. Cada país debería determinar qué delitos graves deben ser considerados como delitos subyacentes al blanqueo de capitales.
5. De acuerdo con lo previsto en la Convención de Viena, el delito de blanqueo de capitales debería aplicarse, al menos, a las actividades intencionales de blanqueo, entendiendo que el elemento intencional podrá inferirse de circunstancias de hecho objetivas.
6. En la medida de lo posible, las empresas mismas, y no solo sus empleados, deberían estar sujetas a responsabilidad penal.

Medidas provisionales y decomiso

7. Los países deberían adoptar, en caso necesario, medidas similares a las previstas en la Convención de Viena, entre ellas las legislativas,

para que sus autoridades competentes puedan decomisar los bienes blanqueados, el producto de los mismos, los instrumentos utilizados, o que se pensaba utilizar, en la comisión de cualquier delito de blanqueo de capitales, o bienes de valor equivalente, sin perjuicio de los derechos de terceros de buena fe.

Estas medidas deberían permitir: 1) identificar, localizar y evaluar los bienes objeto de decomiso; 2) adoptar medidas provisionales, tales como el congelamiento y el embargo, para impedir cualquier comercialización, transferencia o disposición de dichos bienes, y 3) adoptar las medidas de investigación pertinentes.

Además del decomiso y de las sanciones penales, los países deberían contemplar también sanciones económicas y civiles, y/o procedimientos judiciales, incluyendo los de tipo civil, con objeto de anular los contratos concluidos entre las partes, cuando estas sabían o deberían haber sabido que el contrato dañaría la capacidad del Estado para conseguir reclamaciones económicas a través, por ejemplo, del decomiso o la imposición de multas y otras sanciones.

C. PAPEL DEL SISTEMA FINANCIERO EN LA LUCHA CONTRA EL BLANQUEO DE CAPITALS

8. Las Recomendaciones 10 a 29 deberían aplicarse no solamente a los bancos, sino también a las instituciones financieras no bancarias. Aun en el caso de las instituciones financieras no bancarias que no están supervisadas en todos los países (por ejemplo, las oficinas de cambio), los gobiernos deberían asegurar que dichas instituciones estén sujetas a las mismas leyes y reglamentos contra el blanqueo de capitales que las demás instituciones financieras y que esas leyes y reglamentos se aplican eficazmente.
9. Las autoridades nacionales competentes deberían considerar aplicar las Recomendaciones 10 a 21 y 23 al ejercicio de actividades financieras por empresas o profesiones que no son instituciones financieras, cuando tal ejercicio está autorizado o no prohibido. Las actividades financieras comprenden, entre otras, las enumeradas en el anejo adjunto. Corresponde a cada país decidir si determinadas situaciones estarán excluidas de la aplicación de medidas contra el blanqueo de capitales (por ejemplo, cuando una actividad financiera se lleve a cabo ocasionalmente o de forma limitada).

Reglas de identificación del cliente y de conservación de documentos

10. Las instituciones financieras no deberían mantener cuentas anónimas o con nombres manifiestamente ficticios: deberían estar obligadas (por leyes, reglamentos, acuerdos con las autoridades de supervisión o acuerdos de autorregulación entre las instituciones financieras) a identificar, sobre la base de un documento oficial o de otro documento de identificación fiable, a sus clientes ocasionales o habituales, y a registrar esa identificación cuando entablen relaciones de negocios o efectúen transacciones (en particular, la apertura de cuentas o libretas de ahorro, la realización de transacciones fiduciarias, el alquiler de cajas fuertes o la realización de transacciones de grandes cantidades de dinero en efectivo).

Con el fin de cumplir con los requisitos de identificación relativos a las personas jurídicas, las instituciones financieras, cuando sea necesario, deberían tomar las siguientes medidas:

- a) Comprobar la existencia y estructura jurídicas del cliente, obteniendo del mismo o de un registro público, o de ambos, alguna prueba de su constitución como sociedad, incluida la información relativa al nombre del cliente, su forma jurídica, su dirección, los directores y las disposiciones que regulan los poderes para obligar a la entidad.
 - b) Comprobar que las personas que pretenden actuar en nombre del cliente están debidamente autorizadas, e identificar a dichas personas.
11. Las instituciones financieras deberían tomar medidas razonables para obtener información acerca de la verdadera identidad de las personas en cuyo nombre se abre una cuenta o se realiza una transacción, siempre que existan dudas de que esos clientes podrían no estar actuando en nombre propio; por ejemplo, en el caso de las empresas domiciliarias (es decir, instituciones, sociedades, fundaciones, fideicomisos, etc., que no se dedican a operaciones comerciales o industriales, o a cualquier otra forma de actividad comercial en el país donde está situado su domicilio social).
 12. Las instituciones financieras deberían conservar, al menos durante cinco años, todos los documentos necesarios sobre las transacciones realizadas, tanto nacionales como internacionales, que les permitan cumplir rápidamente con las solicitudes de información de las autoridades competentes. Esos documentos deberían permitir reconstruir las diferentes transacciones (incluidas las cantidades y los tipos de moneda utilizados, en su caso), con el fin de proporcionar, si fuera necesario, las pruebas en caso de procesos por conductas delictivas.

Las instituciones financieras deberían conservar, al menos durante cinco años, registro de la identificación de sus clientes (por ejemplo, copia o registro de documentos oficiales de identificación, como pasaportes, tarjetas de identidad, permisos de conducir o documentos similares), los expedientes de clientes y la correspondencia comercial, al menos durante cinco años después de haberse cerrado la cuenta.

Estos documentos deberían estar a disposición de las autoridades nacionales competentes, en el contexto de sus procedimientos y de sus investigaciones penales pertinentes.

13. Los países deberían prestar especial atención a las amenazas de blanqueo de capitales inherentes a las nuevas tecnologías o tecnologías en desarrollo, que pudieran favorecer el anonimato y tomar medidas, en caso necesario, para impedir su uso en los sistemas de blanqueo de capitales.

Mayor diligencia de las instituciones financieras

14. Las instituciones financieras deberían prestar especial atención a todas las operaciones complejas, a las inusualmente grandes, y a todas las modalidades no habituales de transacciones, que no tengan una causa económica o lícita aparente. En la medida de lo posible, deberían examinarse los antecedentes y fines de dichas transacciones; los resultados de ese examen deberían plasmarse por escrito y estar a disposición de los supervisores, de los auditores de cuentas y de las autoridades de prevención y represión.
15. Si las instituciones financieras sospechan que los fondos provienen de una actividad delictiva, deberían estar obligadas a informar rápidamente de sus sospechas a las autoridades competentes.
16. Las instituciones financieras, sus directores y empleados deberían estar protegidos por disposiciones legislativas de toda responsabilidad civil o penal, por violación de las normas de confidencialidad, impuestas por contrato o por disposiciones legislativas reglamentarias o administrativas, cuando comuniquen de buena fe sus sospechas a las autoridades competentes, aun cuando no sepan precisamente cuál es la actividad delictiva en cuestión, y aunque dicha actividad no hubiese ocurrido realmente.
17. Las instituciones financieras y sus empleados no deberían advertir a sus clientes o no debería autorizarse que les avisasen, cuando hayan puesto en conocimiento de las autoridades competentes informaciones relacionadas con ellos.
18. Las instituciones financieras que comuniquen sus sospechas deberían seguir las instrucciones de las autoridades competentes.

19. Las instituciones financieras deberían elaborar programas contra el blanqueo de capitales, incluyendo, como mínimo, lo siguiente:
 - a) Procedimientos y controles internos, comprendiendo el nombramiento de las personas responsables a nivel de dirección y los procedimientos adecuados de selección de empleados para asegurar que esta se realiza de acuerdo con criterios exigentes.
 - b) Un programa continuo de formación de los empleados.
 - c) Un sistema de control interno para verificar la eficacia del sistema.

Medidas para hacer frente al problema de los países cuyas disposiciones contra el blanqueo de dinero son insuficientes o inexistentes

20. Las instituciones financieras deberían asegurarse de que los principios mencionados anteriormente se aplican también a sus sucursales y filiales situadas en el extranjero, especialmente en los países donde estas Recomendaciones no se aplican o se hace de modo insuficiente, en la medida en que lo permitan las leyes y los reglamentos locales. Cuando dicho ordenamiento se oponga a la aplicación de esos principios, las instituciones financieras deberían informar a las autoridades competentes del país donde esté situada la institución matriz de que no puede aplicar estas Recomendaciones.
21. Las instituciones financieras deberían prestar especial atención a las relaciones de negocios y a las transacciones con personas físicas y jurídicas, incluidas las empresas e instituciones financieras residentes en países que no aplican estas Recomendaciones, o que lo hacen de forma insuficiente. Cuando estas transacciones no tengan una causa lícita o económica aparente, deberá examinarse su trasfondo y fines, en la medida de lo posible; los resultados de este examen deberían plasmarse por escrito y estar disponibles para ayudar a los supervisores, a los auditores y a las autoridades de prevención y represión.

Otras medidas para evitar el blanqueo de capitales

22. Los países deberían considerar la adopción de medidas viables para detectar o vigilar el transporte transfronterizo de dinero en efectivo e instrumentos negociables al portador, siempre que el uso de esa información se limite estrictamente y no se restrinja de ninguna manera la libertad de los movimientos de capital.
23. Los países deberían estudiar la viabilidad y utilidad de un sistema en el que los bancos y otras instituciones financieras e intermediarios declararían todas las transacciones de moneda nacionales

e internacionales por encima de un determinado umbral, a un organismo central nacional que disponga de una base de datos informatizada a la que tengan acceso las autoridades competentes en materia de blanqueo de capitales, y cuya utilización esté estrictamente limitada.

24. Los países deberían promover de forma general el desarrollo de técnicas modernas y seguras de gestión de fondos, incluyendo un mayor uso de cheques, tarjetas de pago, abono automatizado de sueldos y anotación en cuenta de operaciones de valores, con objeto de estimular la sustitución de los pagos en efectivo.
25. Los países deberían prestar atención a las posibilidades de uso abusivo de las sociedades ficticias por los autores de operaciones de blanqueo y deberían considerar si hay que adoptar otras medidas para prevenir el uso ilícito de dichas entidades.

Creación y papel de las autoridades reguladoras y de otras autoridades administrativas

26. Las autoridades competentes supervisoras de bancos o de otras instituciones o intermediarios financieros, u otras autoridades competentes, deberían asegurarse de que las instituciones supervisadas tengan programas adecuados para evitar el blanqueo de capitales. Esas autoridades deberían cooperar y aportar sus conocimientos específicos, bien de forma espontánea o bien previa solicitud, a otras autoridades nacionales judiciales o de detección y represión en las investigaciones y procesos relativos a blanqueo de capitales.
27. Deberían designarse las autoridades competentes para asegurar la aplicación eficaz de todas las Recomendaciones, a través de regulación y supervisión administrativa, a otras profesiones que manejen dinero en efectivo, en los términos definidos en cada país.
28. Las autoridades competentes deberían establecer directrices para ayudar a las instituciones financieras a detectar los modos de comportamiento sospechosos de sus clientes. Dichas directrices deberán evolucionar con el tiempo y no tendrán carácter exhaustivo. Además, dichas directrices se utilizarán, principalmente, para formar al personal de las instituciones financieras.
29. Las autoridades competentes que regulan o supervisan las instituciones financieras deberían tomar las medidas legales o reglamentarias necesarias para evitar que delincuentes o sus cómplices tomen el control o adquieran participaciones significativas en las instituciones financieras.

D. FORTALECIMIENTO DE LA COOPERACIÓN INTERNACIONAL

Cooperación administrativa

Intercambio de información de carácter general

30. Las administraciones nacionales deberían considerar registrar, al menos de forma conjunta, los flujos internacionales de dinero en efectivo en cualquier tipo de moneda, de modo que, combinando esos datos con los de otras fuentes extranjeras y con las informaciones que poseen los bancos centrales, puedan hacerse estimaciones de los flujos de dinero en efectivo entre las partes. Dicha información debería ponerse a disposición del Fondo Monetario Internacional y del Banco de Pagos Internacionales para facilitar los estudios internacionales.
31. Las autoridades internacionales competentes, tal vez Interpol y la Organización Aduanera Mundial, deberían estar facultadas para recopilar y divulgar, a las autoridades competentes, información acerca de la evolución reciente en materia y técnicas de blanqueo de capitales. Los bancos centrales y los reguladores bancarios podrían hacer lo mismo dentro del sector que les compete. Las autoridades nacionales de distintos sectores, con la participación de las asociaciones profesionales, podrían divulgar esa información entre las instituciones financieras en cada país.

Intercambio de información relativa a transacciones sospechosas

32. Cada país debería esforzarse por mejorar el intercambio internacional, espontáneo o «previa solicitud», entre las autoridades competentes, de la información relativa a las transacciones, personas o empresas involucradas en transacciones sospechosas. Deberían establecerse estrictas garantías para asegurar que ese intercambio de información respete las disposiciones nacionales e internacionales sobre derecho a la intimidad y protección de datos.

Otras formas de cooperación

Base y medios para la cooperación en materia de decomiso, asistencia mutua y extradición

33. Los países deberían tratar de asegurar, sobre una base bilateral o multilateral, que los diferentes criterios tomados en consideración en las definiciones nacionales respecto al conocimiento del acto cometido, es decir, los criterios diferentes sobre el elemento intencional de la infracción, no afecten a la capacidad o disposición de los países para prestarse asistencia legal mutua.
34. La cooperación internacional debería estar apoyada en una red de convenios y acuerdos bilaterales y multilaterales basados en concep-

tos jurídicos comunes, con el objeto de ofrecer medidas prácticas que se apliquen a la asistencia mutua con la mayor amplitud posible.

35. Debería alentarse a los países a ratificar y aplicar los convenios internacionales pertinentes sobre blanqueo de capitales, tales como la Convención del Consejo de Europa de 1990, sobre blanqueo de capitales, investigación, incautación y decomiso del producto de delitos.

Pautas para mejorar la asistencia mutua en cuestiones de blanqueo de capitales

36. Debería alentarse la cooperación en materia de investigaciones entre las autoridades competentes de los diversos países. En este sentido, una técnica válida y eficaz consiste en la entrega vigilada de bienes que se sabe o sospecha que son producto de un delito. Se alienta a los países a apoyar esta técnica, cuando sea posible.
37. Debería haber procedimientos para la asistencia mutua en cuestiones penales relativas al uso de medidas coercitivas, incluyendo la presentación de documentos por parte de las instituciones financieras y otras personas, el registro de personas y locales, el embargo y la obtención de pruebas para usarlas en las investigaciones y los enjuiciamientos de blanqueo de capitales, y en procedimientos conexos ante las jurisdicciones extranjeras.
38. Deberían poder adoptarse medidas rápidas como respuesta a la solicitud de otros países de identificación, congelación, incautación y decomiso del producto u otros bienes de valor equivalente a dicho producto, basándose en el blanqueo de capitales o los delitos subyacentes de esa actividad. Asimismo, debería haber acuerdos para coordinar los procedimientos de incautación y decomiso de forma que se puedan compartir los bienes decomisados.
39. Para evitar conflictos de competencia, debería estudiarse la posibilidad de elaborar y aplicar mecanismos para determinar cuál sería, en interés de la justicia, la jurisdicción más adecuada para juzgar a los acusados en las causas que estén sujetas a enjuiciamiento en más de un país. Asimismo, deberían existir medidas para coordinar los procedimientos de incautación y decomiso, pudiendo incluir el reparto de los bienes decomisados.
40. Los países deberían disponer de procedimientos para extraditar, cuando sea posible, a los acusados de delitos de blanqueo de capitales o delitos conexos. Sin perjuicio de su ordenamiento jurídico, cada país debería tipificar el blanqueo de capitales como delito extraditable. Siempre que su ordenamiento jurídico lo permita, los países podrían considerar la simplificación de las extradiciones al permitir la transmisión directa de las solicitudes de extradición entre los ministerios afectados, extraditando a las personas en base solamente a órdenes de detención o sentencias, extraditando a sus nacionales y/o aplicando la extradición simplificada de personas que consientan en renunciar a los procedimientos oficiales de extradición.

ANEJO A LA RECOMENDACIÓN 9

Lista de las actividades financieras realizadas por empresas o profesiones que no son instituciones financieras

1. Recepción de depósitos y otros fondos reembolsables del público.
2. Préstamos (4).
3. Arrendamiento financiero.
4. Servicios de transferencia de dinero.
5. Emisión y gestión de medios de pago (por ejemplo, tarjetas de crédito y débito, cheques, cheques de viaje, cartas de crédito...).
6. Concesión de garantías y suscripción de compromisos.
7. Negociación por cuenta de clientes (al contado, a plazo, *swaps*, futuros, opciones...) en:
 - a) instrumentos del mercado monetario (cheques, efectos, certificados de depósito, etc.);
 - b) mercados de cambios;
 - c) instrumentos sobre divisas, tipos de interés, o índices;
 - d) valores negociables;
 - e) futuros de materias primas.
8. Participaciones en emisiones de valores y prestaciones de los servicios financieros correspondientes.
9. Gestión individual y colectiva de patrimonios.
10. Custodia y administración de dinero o de valores negociables, en nombre de clientes.
11. Seguros de vida y otros seguros relacionados con inversiones.
12. Cambio de moneda.

(4) Comprenden, en especial:
 — crédito al consumo;
 — crédito hipotecario;
 — *factoring* con o sin recurso;
 — financiación de transacciones comerciales (incluido el *forfaiting*).

NOTAS INTERPRETATIVAS (5) DE LAS CUARENTA RECOMENDACIONES

Recomendación 4

Los países deberían considerar la introducción de un delito de blanqueo de capitales basado en todas las infracciones graves y/o en aquellas que producen una cantidad importante de dinero.

Recomendación 8

Las Recomendaciones del GAFI deberían aplicarse en particular a los seguros de vida y a otras formas de inversión ofrecidas por las compañías de seguros, mientras que la Recomendación 29 se aplica a todo el sector de seguros.

Recomendaciones 8 y 9 (oficinas de cambio)

Introducción

Las oficinas de cambio constituyen un eslabón importante en la cadena del blanqueo de capitales, debido a la dificultad de seguir la pista del origen del dinero una vez que ha sido cambiado. Diversos ejercicios de tipologías llevados a cabo por el GAFI han mostrado un incremento de la utilización de las oficinas de cambio en las operaciones de blanqueo de capitales. Por consiguiente, sería importante adoptar medidas eficaces en este campo. Esta Nota Interpretativa aclara la aplicación de las Recomendaciones del GAFI relativas al sector financiero a las oficinas de cambio y, cuando así es conveniente, define las opciones en esta materia.

Definición de las oficinas de cambio

A efectos de esta Nota, las oficinas de cambio se definen como instituciones que llevan a cabo operaciones de cambio de moneda al por menor (en metálico, por cheque o tarjeta de crédito). Las operaciones de cambio que se realizan únicamente como elementos accesorios de la actividad principal de un negocio están cubiertas ya por la Recomen-

(5) Durante el período de 1990 a 1995, el GAFI elaboró diversas Notas Interpretativas destinadas a clarificar la aplicación de algunas Recomendaciones. Algunas de estas Notas Interpretativas han sido actualizadas en la Revisión de las Cuarenta Recomendaciones para reflejar los cambios introducidos en las mismas. El 2 de julio de 1999, el GAFI adoptó una nueva Nota Interpretativa relativa a la Recomendación 15.

ción 9. Por consiguiente, tales operaciones están excluidas del ámbito de aplicación de esta Nota.

Medidas necesarias aplicables a las oficinas de cambio

Para luchar contra la utilización de las oficinas de cambio para el blanqueo de capitales, las autoridades competentes deberían tomar medidas destinadas a conocer la existencia de todas las personas físicas o jurídicas que, como actividad profesional, realizan operaciones de cambio de moneda.

Los miembros del GAFI deberían disponer, como mínimo, de un sistema eficaz por el cual las oficinas de cambio serían conocidas o declaradas a las autoridades competentes (ya sean de regulación o de prevención y represión). Podría lograrse este propósito solicitando a las oficinas de cambio que presentaran en el organismo designado una simple declaración que contuviera la información adecuada sobre la propia institución y sus directivos. El organismo en cuestión podría, bien dar acuse de recibo, o bien una autorización tácita, considerándose otorgada por la ausencia de expresión de objeciones.

Los miembros del GAFI podrían también considerar la posibilidad de introducir un procedimiento de autorización formal. Las personas que desearan establecer oficinas de cambio tendrían que presentar una solicitud a la autoridad designada, capacitada para conceder las autorizaciones caso por caso. La solicitud de autorización debería contener las informaciones establecidas por la autoridad, pero debería, como mínimo, contener información detallada sobre la institución solicitante y sus directivos. La autorización sería concedida siempre que la oficina de cambio satisficiera las condiciones específicas relativas a sus directivos y accionistas, e incluyendo los criterios de «competencia y honorabilidad».

Otra opción que se podría considerar consistiría en una combinación de los procedimientos de declaración y de autorización. Las oficinas de cambio tendrían que notificar su existencia a una autoridad designada, pero no necesitarían una autorización para empezar a operar. La autoridad competente tendría libertad para aplicar los criterios de «competencia y honorabilidad» a los gestores de las oficinas de cambio una vez que la oficina hubiera iniciado su actividad y, si así fuere conveniente, prohibir a la oficina de cambio que prosiguiera sus actividades.

En el caso de que las oficinas tuvieran la obligación de realizar una declaración de actividad o una solicitud de inscripción, la autoridad designada (que podría ser un organismo público o un organismo autorregulador) podría estar autorizada para publicar la lista de oficinas de cambio registradas. Al menos, debería llevar un archivo (informático) de oficinas de cambio. Esa autoridad estaría también facultada para emprender acciones contra las oficinas de cambio que realizaran operaciones sin haber hecho una declaración de actividad o sin haber sido registradas.

Como se prevé en las Recomendaciones 8 y 9 del GAFI, las oficinas de cambio deberían estar sometidas a las mismas disposiciones contra el blanqueo de capitales que cualquier otra institución financiera. Por tanto, las Recomendaciones del GAFI en materia financiera deberían ser aplicables a las oficinas de cambio. Las obligaciones relativas a la identificación, la comunicación de transacciones sospechosas, la diligencia debida y la conservación de documentos tienen una especial importancia.

Para garantizar la aplicación efectiva de las obligaciones en materia de lucha contra el blanqueo de capitales por parte de las oficinas de cambio, deberían establecerse y mantenerse mecanismos de vigilancia de este cumplimiento. En caso de existir una autoridad de registro para oficinas de cambio o un organismo que recibiera las declaraciones de actividad de las oficinas de cambio, este último podría encargarse de esta función. Pero la vigilancia podría realizarse también por otras autoridades designadas (realizándose por estas directamente o a través de la intervención de terceras partes, tales como sociedades de auditoría). Se deberían tomar las medidas pertinentes contra las oficinas de cambio que no respetaran las obligaciones en materia de lucha contra el blanqueo de capitales.

El sector de las oficinas de cambio tiende a estructurarse (contrariamente a los bancos) sin organismos representativos nacionales que pudieran actuar como intermediarios en las relaciones con las autoridades. Por este motivo, es importante que los miembros del GAFI establezcan medidas eficaces para asegurarse de que las oficinas de cambio sean conscientes de sus responsabilidades contra el blanqueo de capitales y asegurar la transmisión a esas entidades de informaciones tales como directrices sobre tipos de transacciones sospechosas. En este sentido, sería útil fomentar el desarrollo de asociaciones profesionales.

Recomendaciones 11 y 15 a 18

Cuando fuese necesario para conocer la identidad real del cliente y para evitar que las entidades jurídicas puedan ser utilizadas de forma abusiva por personas físicas como un medio para operar en realidad con cuentas anónimas, y si la información no pudiera obtenerse de otro modo a través de registros públicos o de otras fuentes fiables, las instituciones financieras deberían solicitar del cliente información (y actualizar esa información) sobre sus principales propietarios o beneficiarios. Si el cliente no tuviera tal información, la institución financiera debería solicitar al cliente información sobre quien detente el control real del negocio.

Si no se pudiera obtener la información adecuada, las instituciones financieras deberían prestar una atención particular a las relaciones comerciales y a las transacciones con el cliente.

Si, fundándose en la información facilitada por el cliente u obtenida por otras fuentes, la institución financiera tuviera motivos para creer que la cuenta del cliente está siendo utilizada en operaciones de blanqueo

de capitales, la institución financiera debería cumplir la legislación, reglamentos, directivas o acuerdos que sean aplicables en relación con la notificación de transacciones sospechosas o el cese de los negocios con tales clientes.

Recomendación 11

Los bancos u otras instituciones financieras deberían conocer la identidad de sus propios clientes, aunque estos fueran representados por abogados, para descubrir y prevenir transacciones sospechosas, así como para poder responder rápidamente a los requerimientos de información o incautación de las autoridades competentes. Por consiguiente, la Recomendación 14 se aplica también al caso en que un apoderado actuase como intermediario en materia de servicios financieros.

Recomendación 14

- a) En la interpretación de esta recomendación se deben examinar con una atención especial no solo las transacciones entre instituciones financieras y sus clientes, sino también las transacciones y/o envíos, especialmente de dinero e instrumentos equivalentes, entre las instituciones financieras o incluso las transacciones efectuadas dentro de los grupos financieros. Como los términos de la Recomendación 14 sugieren que «todas» las transacciones están comprendidas, debe interpretarse que se aplica a las transacciones interbancarias.
- b) Debe entenderse que la palabra «transacciones» se refiere a contratos de seguros, al pago de primas y a las prestaciones.

Recomendación 15 (6)

En aplicación de la Recomendación 15, las instituciones financieras deberían comunicar las operaciones sospechosas aun cuando consideren que dichas operaciones guardan también relación con cuestiones fiscales. Los países deben tener en cuenta que los blanqueadores de capitales pueden alegar, entre otras razones, que sus operaciones se refieren a cuestiones fiscales, con el fin de disuadir a las instituciones financieras de la obligación de comunicar toda operación sospechosa.

Recomendación 22

- a) Con objeto de facilitar la detección y vigilancia de transacciones en metálico, sin obstaculizar en forma alguna la libertad de movimiento de capitales, los miembros podrían considerar la posibilidad de que todas las transferencias transfronterizas por encima de un umbral

(6) El GAFI adoptó esta Nota Interpretativa el 2 de julio de 1999.

determinado estuvieran sujetas a verificación, vigilancia administrativa, declaración o a la obligación de conservar la documentación.

- b) Si un país descubriera un envío internacional inhabitual de dinero, instrumentos monetarios, metales o piedras preciosas, etc., debería considerar si notificarlo, en su caso, a los servicios de aduanas u otras autoridades competentes de los países de origen y/o de destino del envío, y debería cooperar para determinar el origen, el destino y el propósito de tal envío y para tomar las medidas adecuadas.

Recomendación 26

Respecto a esta recomendación, cabe observar que sería útil para detectar eficazmente el blanqueo de capitales que las autoridades competentes pusieran a disposición de las autoridades de investigación las informaciones estadísticas disponibles, especialmente si estas informaciones contuviesen indicadores específicos de actividades de blanqueo de capitales. Por ejemplo, si las estadísticas de las autoridades competentes mostraran un desequilibrio entre el desarrollo de las actividades de los servicios financieros en una determinada zona geográfica de un país y el desarrollo de la economía local, este desequilibrio podría indicar la existencia de una actividad de blanqueo de capitales en la región. Otro ejemplo sería un cambio manifiesto en los flujos de billetes nacionales sin causa económica lícita aparente. No obstante, estos datos estadísticos deben ser analizados con prudencia, ya que no existe necesariamente una relación directa entre los flujos financieros y la actividad económica (v. g., los flujos financieros en un centro financiero internacional donde una parte importante de los servicios de gestión de inversiones se presta a clientes extranjeros o que posee un importante mercado interbancario no relacionado con la actividad económica local).

Recomendación 29

La Recomendación 29 no puede ser interpretada en el sentido de que requiera la introducción de un sistema de revisión periódica de las autorizaciones concedidas para el control de participaciones significativas en instituciones financieras únicamente para fines de lucha contra el blanqueo de capitales, sino que esta Recomendación subraya, desde el punto de vista del GAFI, la conveniencia de revisar que los accionistas que controlan el capital de las instituciones financieras son adecuados (en particular, de los bancos y de otras instituciones). Por consiguiente, en caso de que existan criterios de aptitud (o de honorabilidad) de los accionistas, las autoridades de vigilancia deberían prestar atención a su adaptación a los objetivos de la lucha contra el blanqueo de capitales.

Recomendación 33

Sin perjuicio de los principios de su ordenamiento interno, los países deberían esforzarse por asegurar que las diferencias en las definiciones nacionales del delito de blanqueo de capitales (es decir, los diferentes criterios

relativos al elemento intencional de la infracción, las diferencias en los delitos subyacentes que den lugar al blanqueo de capitales, las diferencias con respecto a la acusación de la perpetración de la infracción subyacente del delito de blanqueo de capitales) no afecten la capacidad o disposición de los países de prestarse asistencia legal mutua.

Recomendación 36 (entrega vigilada)

La entrega vigilada de fondos que se sabe o sospecha son el producto de un delito es una técnica válida y eficaz de aplicación de las leyes para obtener información y pruebas sobre las operaciones internacionales de blanqueo de capitales. En ciertos países, las técnicas de entrega vigilada pueden incluir también la vigilancia de dinero. Puede ser de gran utilidad para emprender ciertas investigaciones penales y también puede ayudar a obtener más información general sobre las actividades de blanqueo de capitales. Debiera alentarse firmemente el uso de estas técnicas. Por lo tanto, deberían tomarse medidas apropiadas para que no haya obstáculos en los sistemas jurídicos que impidan el uso de las técnicas de entrega vigilada para la realización de tales operaciones, con sujeción a los requisitos legales, entre ellos la autorización judicial. El GAFI acoge con agrado y apoya las gestiones de la Organización Aduanera Mundial y de Interpol para alentar a sus miembros a que tomen todas las medidas apropiadas para promover el uso de estas técnicas.

Recomendación 38

- a) Cada gobierno considerará, cuando sea posible, el establecimiento de un fondo para los activos decomisados en su respectivo territorio, en el que se deposite una parte o la totalidad de los bienes decomisados para los fines de salud, educación, represivos u otros pertinentes.
- b) Cada gobierno debería considerar, cuando sea posible, la adopción de las medidas que sean necesarias para permitir que los bienes decomisados puedan repartirse con otros países; en particular, cuando el decomiso sea el resultado, directo o indirecto, de las acciones operativas coordinadas.

Aplazamiento de la detención e incautación

Los países deberían considerar la adopción de medidas a nivel nacional, incluidas las legislativas, para que las autoridades competentes que investigan las causas de blanqueo de capitales puedan aplazar o suspender la detención de los sospechosos y/o la incautación del dinero, o puedan no llevar a cabo tal detención e incautación, con el fin de identificar a los implicados en dichas actividades o de recopilar pruebas. Sin dichas medidas no es posible aplicar determinados procedimientos, tales como las entregas vigiladas y las operaciones encubiertas.

*DIRECTRICES GLOBALES PARA
LA PREVENCIÓN DEL BLANQUEO
DE CAPITALES EN ACTIVIDADES
DE BANCA PRIVADA*

Grupo de bancos Wolfsberg

PRINCIPIOS WOLFSBERG (1)

(Primera revisión, mayo de 2002)

Los siguientes grandes bancos privados internacionales:

- ABN AMRO Bank N.V.
- Bank of Tokyo-Mitsubishi Ltd.
- Barclays Bank
- Citigroup
- Crédit Suisse Group
- Deutsche Bank AG
- Goldman Sachs
- HSBC
- J. P. Morgan Private Bank
- Santander Central Hispano
- Société Générale
- UBS AG

han acordado estos principios como importantes directrices globales para una adecuada conducta empresarial en actividades de banca privada internacional.

Agradecimiento

Estos bancos colaboraron con un equipo de Transparency International (2), que invitó a participar a dos expertos internacionales: Stanley Morris (3) y el profesor Mark Pieth (4). Transparency International y los citados expertos consideran estos principios como un paso importante en la lucha contra el blanqueo de capitales, la corrupción y otros graves delitos conexos.

(1) Wolfsberg es una localidad suiza donde tuvo lugar una importante sesión de trabajo para la formulación de estas directrices.

(2) Transparency International (TI) es una organización no gubernamental con sede en Berlín, dedicada a incrementar el control y el freno gubernamentales de la corrupción nacional e internacional. TI está presente en más de 70 países. TI estuvo representada por su fundador y presidente del consejo, Peter Eigen, y por el presidente de la sección estadounidense, Fritz Heimann.

(3) Stanley E. Morris es consultor internacional en materia de blanqueo de capitales. Ha sido jefe de FinCEN y miembro del GAFI.

(4) Mark Pieth es profesor de leyes en Basilea, Suiza. Es jefe del Grupo de Trabajo de la OCDE sobre sobornos y corrupción, y ha sido miembro del GAFI.

PRINCIPIOS WOLFSBERG ANTI-BLANQUEO DE CAPITALS

Preámbulo

Las directrices siguientes se consideran apropiadas para las actividades de banca privada. Las directrices para otros segmentos del mercado pueden ser diferentes. Se reconoce que la responsabilidad del establecimiento de políticas y procedimientos que cumplan estas directrices incumbe a la dirección.

1. ACEPTACIÓN DE CLIENTES: DIRECTRICES GENERALES

1.1. Generalidades

Formará parte de la política del banco el impedir la utilización de sus operaciones en todo el mundo para propósitos delictivos. El banco procurará aceptar solo aquellos clientes cuya fuente de riqueza y de fondos se pueda verificar razonablemente como legítima. La responsabilidad primaria de ello le incumbe al responsable de banca privada que proponga la aceptación del cliente. La mera cumplimentación de los procedimientos internos de selección no exime al responsable de banca privada de esta responsabilidad básica.

1.2. Identificación

El banco tomará las medidas razonables para verificar la identidad de sus clientes y propietarios beneficiarios, y solo aceptará clientes cuando haya completado este proceso.

1.2.1. *Cliente*

- Personas físicas: la identidad se verificará a satisfacción del banco, basándose en documentos oficiales de identidad o en otras pruebas que se consideren apropiadas según las circunstancias.
- Sociedades, asociaciones personales y fundaciones: el banco recibirá prueba documental de su debida constitución y existencia.
- Fideicomisos: el banco recibirá pruebas apropiadas de su constitución y existencia, junto con la identidad de los fideicomisarios.
- Los documentos de identificación deben estar en vigor en la fecha de apertura.

1.2.2. *Propietario beneficiario*

La propiedad beneficiaria debe verificarse para todas las cuentas. Se debe aplicar la debida diligencia a todos los principales propietarios beneficiarios identificados, de conformidad con los principios siguientes:

- **Personas físicas:** cuando la cuenta figure a nombre de una persona física, el responsable de banca privada debe verificar si el cliente está actuando por su propia cuenta. Si existen dudas, el banco verificará en calidad de qué actúa y por cuenta de quién.
- **Personas jurídicas:** si el cliente es una sociedad, por ejemplo, una sociedad de inversión privada, el responsable de banca privada deberá comprender la estructura de la sociedad lo suficiente como para determinar la identidad del proveedor de los fondos, del o de los principales propietarios de las acciones y de quienes tengan control sobre los fondos; *v. g.*, los directivos y quienes cuenten con capacidad para dar instrucciones a los directivos de la sociedad. Respecto a otros accionistas, el responsable de banca privada enjuiciará razonablemente la necesidad de otras medidas de debida diligencia. Este principio es aplicable con independencia de que las acciones de la sociedad sean nominativas o al portador.
- **Fideicomisos:** si el cliente es un fideicomisario, el responsable de banca privada habrá de comprender la estructura del fideicomiso lo suficiente como para determinar la identidad del proveedor de los fondos (*v. g.*, fideicomitente), de quienes tienen control sobre los fondos (*v. g.*, fideicomisarios) y de cualesquiera personas o entidades que tengan facultad para cambiar a los fideicomisarios. El responsable de banca privada enjuiciará razonablemente la necesidad de otras medidas de debida diligencia.
- **Asociaciones no constituidas como sociedades:** los principios precedentes son aplicables a las entidades no societarias.
- **El banco no permitirá la utilización de sus cuentas internas de no clientes (a veces denominadas cuentas de «concentración»)** para impedir que se asocie la identidad de un cliente con el movimiento de fondos por cuenta suya; es decir, el banco no permitirá el uso de dichas cuentas internas de forma que pueda impedir el seguimiento adecuado por el banco de la actividad de las cuentas del cliente.

1.2.3. *Cuentas mantenidas a nombre de gestores de dinero o mediadores similares*

El responsable de banca privada aplicará la debida diligencia al mediador y verificará si este aplica la debida diligencia a sus clientes, o está sometido a una obligación regulatoria de aplicar dicha debida diligencia, que sea satisfactoria para el banco.

1.2.4. *Poderes / Firmantes autorizados*

Si el titular de un poder u otro firmante autorizado es designado por un cliente, en general basta con aplicar la debida diligencia al cliente.

1.2.5. *Prácticas para clientes ocasionales y relaciones de banca electrónica*

Antes de la apertura de la cuenta, el banco determinará si los clientes ocasionales o las relaciones iniciadas por vía electrónica requieren un grado más elevado de debida diligencia. El banco adoptará medidas específicamente dirigidas a establecer satisfactoriamente la identidad de los clientes no presenciales.

1.3. **Debida diligencia**

Es esencial recopilar y registrar información que cubra las categorías siguientes:

- Propósito y razones de la apertura de la cuenta.
- Actividad prevista de la cuenta.
- Fuente de riqueza (descripción de la actividad económica que ha generado el patrimonio).
- Patrimonio estimado.
- Fuente de los fondos (descripción del origen y de la forma de transferir los fondos que se acepten para abrir la cuenta).
- Referencias u otras fuentes para corroborar la información sobre la reputación, cuando estén disponibles.

Salvo que otras medidas basten razonablemente para aplicar la debida diligencia a un cliente (*v. g.*, referencias favorables y fidedignas), se debe conocer a un cliente antes de la apertura de la cuenta.

1.4. **Cuentas numeradas o con nombre figurado**

Las cuentas numeradas o con nombre figurado solo serán aceptadas si el banco ha establecido la identidad del cliente y la del propietario beneficiario. Estas cuentas deben ser objeto de un grado de escrutinio igual al aplicable a otras cuentas de clientes, por parte de las adecuadas instancias de control del banco.

1.5. **Jurisdicciones extraterritoriales (*offshore*)**

Los riesgos asumidos con entidades constituidas en jurisdicciones extraterritoriales serán objeto de los procedimientos de debida diligencia recogidos en estas directrices.

1.6. Responsabilidad de control

Se exigirá que todos los clientes nuevos y todas las cuentas nuevas sean aprobados por, al menos, una persona distinta del responsable de banca privada.

2. ACEPTACIÓN DEL CLIENTE: SITUACIONES QUE REQUIEREN DILIGENCIA/ATENCIÓN ADICIONALES

2.1. General

En sus políticas internas, el banco debe definir categorías de personas, cuyas características exijan diligencia especial. Un caso típico es cuando, probablemente, dichas características plantean para el banco un riesgo superior al medio.

2.2. Indicadores

Las características de los siguientes tipos de personas son indicativas de que deben ser definidas como merecedoras de especial diligencia:

- Personas que residen y/o tienen fondos originados en países identificados por fuentes creíbles como poseedores de niveles inadecuados de prevención del blanqueo de capitales o que representan alto riesgo por delincuencia o corrupción.
- Personas implicadas en actividades empresariales o sectores reconocidos como susceptibles de ser utilizados para el blanqueo de capitales.
- Personas del medio político, que incluyen a quienes tengan o hayan tenido cargos de confianza pública, como son funcionarios gubernamentales, altos ejecutivos de empresas públicas, políticos, altos responsables de partidos políticos, etc., así como sus familias y colaboradores cercanos.

2.3. Aprobación por altos directivos

Las políticas internas de los bancos deben indicar si, para una o más de estas categorías, deben ser los altos directivos quienes aprueben entrar en nuevas relaciones.

Las relaciones con personas del medio político solo deben comenzar tras la aprobación de los altos gestores.

3. ACTUALIZACIÓN DE ARCHIVOS DE CLIENTES

- 3.1. El responsable de banca privada tiene la responsabilidad de actualizar el archivo de cada cliente con criterios definidos y/o cuando se

produzcan cambios importantes. El supervisor de las actividades de banca privada o un controlador independiente revisarán una parte relevante de los archivos de clientes de forma periódica, para asegurar su consistencia e integridad. La frecuencia de las revisiones dependerá del volumen, la complejidad y el riesgo que representa la relación.

- 3.2. Con respecto a los clientes clasificados en cualquiera de las categorías mencionadas en 2, las políticas internas de los bancos deben indicar si los altos directivos deben implicarse en estas revisiones.
- 3.3. De igual forma, en relación con los clientes clasificados como se indica en 3.2, las políticas internas de los bancos establecerán la información gerencial que debe ser proporcionada a los directivos y/o a otras instancias de control. Dichas políticas deben también fijar la frecuencia de estos flujos de información.
- 3.4. Las revisiones relativas a personas del medio político deben requerir la implicación de altos directivos.

4. PRÁCTICAS EN LA IDENTIFICACIÓN DE ACTIVIDADES INUSUALES O SOSPECHOSAS

4.1. Definición de actividades inusuales o sospechosas

El banco tendrá una política escrita de identificación y seguimiento de actividades inusuales o sospechosas. Esta política incluirá una definición de lo que se considera sospechoso o inusual y ofrecerá ejemplos de ello.

Las actividades inusuales o sospechosas pueden incluir:

- Operaciones con la cuenta u otras actividades que no sean congruentes con el expediente de debida diligencia.
- Operaciones en efectivo por encima de una determinada cantidad.
- Transacciones de paso/de entrada y salida.

4.2. Identificación de actividades inusuales o sospechosas

Las actividades inusuales o sospechosas se pueden identificar mediante:

- Seguimiento de las transacciones.
- Contactos con el cliente (reuniones, conversaciones, visitas a su país, etcétera).
- Información de terceros (*v. g.*, periódicos, Reuters, Internet).
- Conocimiento interno o del responsable de banca privada del entorno del cliente (*v. g.*, situación política en su país).

4.3. Seguimiento de actividades inusuales o sospechosas

El responsable de banca privada, la dirección y/o el departamento de control llevará a cabo un análisis de los antecedentes de cualquier actividad inusual o sospechosa. Si no existe una explicación verosímil, se tomará una decisión, en la que participe el departamento de control, sobre:

- Mantener la relación de negocio con un mayor seguimiento.
- Cancelar la relación de negocio.
- Poner la relación de negocio en conocimiento de las autoridades.

La comunicación a las autoridades se hará por el departamento de control y normalmente se debe informar de ello a la alta dirección (*v. g.*, un responsable de cumplimiento normativo de alto nivel, el consejero delegado, el auditor jefe, el asesor jurídico jefe). Según lo exijan las leyes y regulaciones locales, los activos pueden ser bloqueados y las transacciones pueden estar sometidas a la aprobación del departamento de control.

5. SEGUIMIENTO

5.1. Programa de seguimiento

Debe estar implantado un programa adecuado de seguimiento. La responsabilidad primaria de la actividad de seguimiento de las cuentas le corresponde al responsable de banca privada. El responsable de banca privada estará al tanto de las transacciones significativas y de los aumentos de actividad en la cuenta, y estará especialmente al corriente de actividades inusuales o sospechosas (véase 4.1). El banco decidirá en qué medida el desempeño de estas responsabilidades necesita estar respaldado por el uso de sistemas automatizados u otros medios.

5.2. Seguimiento continuado

En relación con los clientes clasificados en cualquiera de las categorías de personas mencionadas en 2, las políticas internas de los bancos indicarán cómo debe llevarse a cabo el seguimiento de sus cuentas.

6. RESPONSABILIDADES DE CONTROL

Habrà implantada una política escrita de control, que establezca los procedimientos estándar de control que deban realizar las diversas «instancias de control» (responsable de banca privada, unidad independiente

de operaciones, cumplimiento normativo, auditoría interna). La política de control cubrirá temas como calendario, grado de control, áreas que se deben controlar, responsabilidades y seguimiento, etc.

Un departamento de auditoría independiente (que puede ser interno al banco) verificará los programas incluidos en la política de control.

7. INFORMES

Habrán establecidos informes de gestión periódicos sobre cuestiones relacionadas con el blanqueo de capitales (v. g., número de informes remitidos a las autoridades, herramientas de seguimiento, cambios en la legislación y regulación aplicables, número y contenido de las sesiones de formación impartidas a los empleados).

8. EDUCACIÓN, FORMACIÓN E INFORMACIÓN

El banco establecerá un programa de formación sobre identificación y prevención del blanqueo de capitales para los empleados que tengan contacto directo con clientes y para el personal de cumplimiento normativo. La formación periódica (v. g., anualmente) incluirá asimismo cómo identificar y hacer el seguimiento de actividades inusuales o sospechosas. Además, se informará a los empleados sobre cualesquiera cambios importantes en la legislación y regulación contra el blanqueo de capitales.

A todos los empleados nuevos se les proporcionarán directrices sobre procedimientos contra el blanqueo de capitales.

9. REQUISITOS DE CONSERVACIÓN DE ARCHIVOS

El banco establecerá requisitos de conservación de los archivos de todos los documentos relacionados con la prevención del blanqueo de capitales. Los documentos deben conservarse durante cinco años como mínimo.

10. EXCEPCIONES Y DESVIACIONES

El banco establecerá un procedimiento para las excepciones y desviaciones que requieran la evaluación del riesgo y la aprobación por una unidad independiente.

11. ORGANIZACIÓN CONTRA EL BLANQUEO DE CAPITALES

El banco establecerá un departamento independiente y suficientemente dotado de personal que sea responsable de la prevención del blanqueo de capitales (v.g., cumplimiento normativo, unidad de control independiente, asesoría jurídica).

*EL SISTEMA FINANCIERO
Y EL BLANQUEO DE CAPITALS*

Ignacio Palicio Díaz-Faes

1. INTRODUCCIÓN

La amplitud, diversificación y sofisticación crecientes del sistema financiero lo convierten en un instrumento cada vez más imprescindible en el proceso de blanqueo de capitales, entendido este como la realización de cualquier tipo de operación que tenga como finalidad la ocultación o encubrimiento de la naturaleza, origen, localización, disposición o propiedad de los bienes procedentes de actividades delictivas.

La definición de blanqueo de capitales incluye, en consecuencia, tanto la adquisición, utilización, conversión o transmisión de bienes procedentes de determinadas actividades delictivas, como la participación en las actividades anteriores para ocultar o encubrir su origen o ayudar a la persona que haya participado en las mismas a eludir las consecuencias jurídicas de sus actos; también incluye, por último, la ocultación o encubrimiento de la verdadera naturaleza, origen, localización, disposición y movimientos de los bienes mencionados, así como de la propiedad o de los derechos sobre esos bienes.

En la definición anterior ya empiezan a intuirse varias posibilidades de participación en el proceso del blanqueo de capitales, lo que permite comenzar a identificar distintas fases en este proceso. La identificación de estas fases es importante desde un punto de vista metodológico y permite fijar prioridades tanto para la prevención como para la represión del blanqueo de capitales. Ello no significa que, para que exista blanqueo de capitales, tengan que completarse todas y cada una de ellas o que tengan que producirse en un orden determinado; es más, dependiendo del tipo de delito subyacente en el blanqueo de capitales (tráfico de drogas, terrorismo o delincuencia organizada en el caso de nuestra legislación), cada una de las fases cobra un protagonismo diferente y se convierte en clave para su prevención.

La primera fase, conocida como de *colocación*, tiene como finalidad la introducción en el sistema económico de los fondos obtenidos ilegalmente. Se caracteriza por la utilización masiva de medios de pago muy líquidos (efectivo, medios de pago al portador...) y es una fase decisiva para la prevención y el control de los fondos procedentes del tráfico de drogas.

En la fase de *encubrimiento*, el objetivo es la desvinculación de su origen de los fondos procedentes de una actividad delictiva, mediante la utilización de diversas y a veces complejas operaciones que pretenden

NOTA: Este artículo es responsabilidad del autor.

dificultar su control, ocultar su origen y dificultar la identificación de la titularidad última de los mismos. En esta fase son decisivas la facilidad y la rapidez operativas, así como la posibilidad de realizar operaciones financieras complejas y sofisticadas que permitan la movilización masiva y segura de fondos.

Por último, en la fase de *integración*, los fondos blanqueados vuelven al sector de la economía del que provenían, o a otro diferente, como fondos aparentemente legítimos. Es la fase más difícil para su identificación en la práctica, puesto que, desde cierto punto de vista, puede considerarse que el proceso de blanqueo ya ha terminado en la fase anterior; además, en alguno de los delitos subyacentes al blanqueo de capitales se manejan fondos que ya están integrados, por proceder de actividades lícitas, y que son destinados a la realización de actividades delictivas.

2. INICIATIVAS INTERNACIONALES A FAVOR DE LA COLABORACIÓN DEL SISTEMA FINANCIERO EN LA PREVENCIÓN DEL BLANQUEO DE CAPITALES. PROPUESTAS DEL COMITÉ DE SUPERVISIÓN BANCARIA

El hecho de que el sistema financiero sea uno de los sectores más sensibles para su utilización en operaciones de blanqueo de capitales, y la circunstancia de que el proceso de blanqueo tiende por naturaleza a desarrollarse en un contexto internacional, provocaron, a finales de la década de los ochenta, un movimiento internacional a favor de la colaboración activa del sistema financiero en la prevención del blanqueo de capitales. La primera iniciativa fue la Declaración de Basilea, en diciembre de 1988, en la que los países que formaban parte del Comité de Supervisión Bancaria (CSB) establecieron las reglas deontológicas aplicables por el sector financiero en esta materia. En el mismo mes y año, la Conferencia Diplomática de Viena aprobó el Convenio de las Naciones Unidas contra el tráfico ilícito de estupefacientes, en el que los países signatarios se comprometían a considerar el blanqueo de dinero procedente de la droga como una infracción penal. Por último, en el año 1989 se decidió la creación del Grupo de Acción Financiera sobre el Blanqueo de Capitales (GAFI), dirigido a promover la cooperación y acción contra el blanqueo de dinero en el ámbito internacional.

Los principios recogidos en las iniciativas descritas sirvieron, en los años siguientes, como punto de referencia para el desarrollo y la implantación de las legislaciones nacionales sobre la materia. Las legislaciones europea y española, que serán objeto de un análisis más detallado en un apartado posterior, quedaron desarrolladas en sus aspectos básicos entre los años 1991 y 1995. A continuación se comentan los principales documentos elaborados en el seno del Comité de Supervisión Bancaria, que afectan a la prevención del blanqueo de capitales por las entidades financieras y a la reducción de los riesgos a los que están expuestas en el desarrollo de su actividad.

2.1. La Declaración de Basilea de 1988

La Declaración de Basilea de 1988 está considerada como la primera codificación de las reglas aplicables por las entidades financieras en la prevención del blanqueo de capitales. El preámbulo de siete puntos comenzaba diciendo que «los bancos y otras instituciones financieras pueden ser utilizados inadvertidamente para la transferencia o depósito de fondos de origen delictivo. Los delincuentes y sus cómplices se sirven del sistema financiero para efectuar pagos y hacer transferencias entre cuentas, con la finalidad de ocultar tanto el origen de los fondos como la identidad de sus verdaderos propietarios». La Declaración iba dirigida a los supervisores bancarios, a los que alertaba de que no podían permanecer indiferentes ante la utilización del sistema financiero por parte de los delincuentes, puesto que la confianza del público en los bancos y, consiguientemente, la estabilidad de los mismos podían verse afectadas por una publicidad desfavorable derivada de la asociación involuntaria de los bancos con los delincuentes.

Tras el preámbulo, la Declaración incluía cuatro principios que recogían las políticas y procedimientos básicos, que los gestores bancarios debían implantar para eliminar el blanqueo de capitales a través del sistema financiero. Estos principios hacían referencia a la identificación de los clientes, al cumplimiento de las leyes y regulaciones relacionadas con la materia, a la colaboración con las autoridades responsables de la lucha contra el blanqueo de capitales y a la formación del personal de los bancos en estas políticas y procedimientos.

2.2. Los Principios Básicos

Los «Principios Básicos para una Supervisión Bancaria Eficaz», publicados en el año 1997, dentro del tercer bloque, el referido al tratamiento de los riesgos bancarios, incluyen el Principio 15. Este principio afirma que los supervisores bancarios deben establecer que los bancos tengan políticas y procedimientos adecuados, incluyendo reglas estrictas de conocimiento del cliente, que promuevan altos estándares éticos y profesionales en el sector financiero, para prevenir que los bancos sean utilizados por los delincuentes. Asimismo, establece los requisitos para un adecuado control interno (independencia de los órganos de cumplimiento normativo, papel de la auditoría interna y externa, etc.) e incide, de nuevo, en el daño que puede sufrir la reputación de los bancos, como resultado de su asociación, aunque sea de forma involuntaria, con actividades delictivas. Por último, este principio se refiere a la importancia que tiene para el supervisor que las entidades no se vean involucradas en este tipo de actividades, ya que, cuando la implicación y la importancia del asunto son graves, pueden afectar a la solvencia y solidez de las entidades, pueden ser indicio de unos débiles controles internos que requieran la atención del supervisor, y pueden generar un riesgo sistémico que se transmita de una entidad a todo el sistema.

2.3. Documento sobre la «Debida diligencia de los bancos con sus clientes»

En octubre de 2001, el Comité de Supervisión Bancaria hizo público un documento, «Debida diligencia de los bancos con sus clientes», que tiene una importancia extraordinaria en esta materia, tanto por la claridad de sus propuestas como por el esfuerzo sintetizador realizado para centrar los riesgos que afectan a las entidades, además de proponer las medidas y procedimientos imprescindibles para reducirlos.

El documento destaca la importancia de una adecuada política de «Conozca a su cliente», en línea con las recomendaciones del GAFI, para el que esta política supone la piedra angular de la prevención del blanqueo de capitales. Para los supervisores es importante, porque la solidez de los procedimientos de conocimiento del cliente ayudan a proteger la reputación de los bancos, la integridad de los sistemas bancarios, y constituyen parte esencial de una gestión de riesgos sólida. La insuficiencia o la carencia de normas de «Conozca a su cliente» pueden someter a los bancos a riesgos serios, especialmente a los riesgos reputacional, operativo, legal y de concentración.

En el diseño de sus programas de «Conozca a su cliente», los bancos deberían incluir los siguientes elementos clave:

- Política de aceptación de clientes

Deben desarrollarse políticas y procedimientos claros de aceptación de clientes, incluyendo una descripción de los tipos de cliente que previsiblemente van a representar un riesgo superior al medio para una entidad. Al preparar dichas políticas, deben tenerse en cuenta factores tales como los antecedentes, el país de origen, la posición pública o destacada, las cuentas vinculadas, las actividades empresariales y otros indicadores de riesgo de los clientes. Las entidades deben desarrollar políticas y procedimientos escalonados de aceptación de clientes, que requieran requisitos más exhaustivos para los clientes de alto riesgo.

- Identificación del cliente

Es un elemento esencial de las normas de conocimiento del cliente. Debe establecerse un procedimiento sistemático de identificación de los clientes nuevos, y no deben establecerse relaciones bancarias mientras no se haya verificado satisfactoriamente la identidad del cliente nuevo. Es preciso prestar especial atención a las cuentas de fideicomisos, personas interpuestas, fiduciarias, a los vehículos societarios (establecer impedimentos para que las sociedades sean utilizadas por personas físicas como método para manejar cuentas anónimas, y prestar atención a las sociedades con accionistas interpuestos o con acciones al portador),

a las cuentas de clientes abiertas por profesionales (cuando existan subcuentas que puedan ser atribuidas a cada propietario beneficiario, es preciso tener identificados a todos ellos), a los clientes no conocidos en persona, y a los corresponsales bancarios.

- Seguimiento continuo de cuentas y transacciones

Las entidades solo pueden controlar y reducir de forma efectiva su riesgo si identifican la actividad normal y razonable de las cuentas de sus clientes, de modo que tengan un medio para descubrir transacciones que queden fuera del esquema habitual de actividad de una cuenta. El alcance de este seguimiento ha de ser sensible al riesgo. Para todos los tipos de cuentas, actividades o grupos de clientes, las entidades deberían tener implantadas pautas para identificar actividades inusuales o sospechosas.

- Gestión de riesgos

Unos procedimientos eficaces de «Conozca a su cliente» comprenden sistemas y controles internos adecuados, segregación de funciones, y unas políticas de formación adaptadas a las peculiaridades del negocio y a los distintos cometidos del personal. Como elemento esencial en la gestión de estos riesgos, destaca la implicación de la alta dirección de las entidades en el establecimiento y control posterior de los procedimientos necesarios.

En este documento, el Comité de Supervisión Bancaria insta a los supervisores nacionales a establecer prácticas supervisoras sobre los programas de «Conozca a su cliente» de las entidades, y afirma que el proceso de supervisión debería incluir, no solo una revisión de las políticas y procedimientos, sino también una revisión de los archivos de clientes y el muestreo de algunas cuentas.

2.4. Nuevo Acuerdo de Capital

El Nuevo Acuerdo de Capital del Comité de Supervisión Bancaria de Basilea tiene como uno de sus ejes fundamentales la adecuada medición de los riesgos a los que están expuestas las entidades en el desarrollo de su actividad, y la revisión y evaluación continuadas por parte del supervisor de los procesos internos de control de esos riesgos. Para ello, se exige a las entidades que cuenten con un marco conceptual que incluya un proceso de valoración de cada uno de los riesgos significativos a los que se enfrentan. Entre estos riesgos, clasificados en la correspondiente categoría, las entidades y los supervisores deben incluir los que se derivan de la posible utilización de las entidades en operaciones de blanqueo de capitales.

3. LA NORMATIVA ESPAÑOLA SOBRE PREVENCIÓN DEL BLANQUEO DE CAPITALES

Las iniciativas internacionales adoptadas a finales de la década de los ochenta tuvieron, en los años siguientes, un reflejo en la legislación de los países más desarrollados. La Directiva 91/308, de 10 de junio, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales, define, en el ámbito europeo, los principios básicos sobre la materia, para su trasposición a las legislaciones nacionales. La inclusión en la legislación española de las iniciativas comentadas se produjo con la publicación de la Ley 19/1993 y su Reglamento, y con la introducción del delito de blanqueo de capitales procedente del tráfico de drogas en la reforma del Código Penal de 1988. En el nuevo Código Penal de 1995 se amplió este tipo penal a las ganancias procedentes de otros delitos. La última iniciativa en el ámbito europeo ha sido la aprobación de la Directiva 2001/97, de 4 de diciembre, que modifica la Directiva 91/308 y que está pendiente de trasposición a la legislación española.

Los aspectos más destacables de las directivas comunitarias y de nuestra legislación se resumen en los apartados siguientes.

3.1. Ámbito objetivo

El concepto de blanqueo de capitales ya se ha comentado con detalle en la introducción de este artículo. Únicamente queda hacer referencia a que el concepto incluido en la legislación comunitaria y en la española es el mismo utilizado en la Convención de Viena de 1988.

Por lo que se refiere a las actividades delictivas a las que afecta el blanqueo de capitales, la legislación española considera como delitos subyacentes, el narcotráfico, el terrorismo y la delincuencia organizada. La Directiva de 2001 amplía el ámbito de los delitos subyacentes al delito fiscal.

3.2. Ámbito subjetivo

La Directiva 91/308 impone el deber de colaboración solamente a las entidades financieras, entendiendo como tales las entidades de crédito y ahorro, las empresas de servicios de inversión y las empresas de seguros. No obstante, uno de sus preceptos permite extender la aplicación de la normativa a otras empresas que desarrollen actividades particularmente susceptibles de ser utilizadas en el blanqueo de capitales. La normativa española extendió su ámbito de aplicación a las sociedades emisoras de tarjetas de crédito, las personas físicas o jurídicas que ejerzan la actividad de cambio de moneda, los casinos de juego, las actividades de promoción inmobiliaria o compra de inmuebles, las actividades relacionadas con el comercio de joyas, piedras y metales preciosos, las

actividades relacionadas con el comercio de objetos de arte y antigüedades, y las actividades de inversión filatélica y numismática.

La Directiva 2001/97 prevé incluir entre los sujetos obligados a cumplir la normativa de prevención del blanqueo de capitales, a los auditores, contables externos y asesores fiscales. También extiende la obligación a los notarios y otros profesionales independientes del derecho, cuando participen en la concepción o realización de transacciones por cuenta de su cliente, relativas a la compraventa de inmuebles o entidades comerciales. De igual forma, afecta a la gestión de fondos, valores u otros activos; a la apertura o gestión de cuentas bancarias, cuentas de ahorro o cuentas de valores; a la organización de las aportaciones necesarias para la creación, funcionamiento o gestión de empresas; y a la creación, funcionamiento o gestión de sociedades fiduciarias y de empresas o estructuras análogas.

3.3. Deberes de los sujetos obligados

El objeto esencial de la normativa lo constituyen una serie de deberes que deben cumplir los sujetos obligados.

- Deber de identificación

Exigir, mediante un documento acreditativo, la identificación de sus clientes en el momento de entablar relaciones de negocios, así como de cuantas personas pretendan efectuar cualquier tipo de operación. Cuando existan indicios o certeza de que los clientes no actúan por cuenta propia, los sujetos obligados deben recabar la información precisa para conocer la identidad de las personas por cuenta de las que actúan.

- Deber de atención y examen especial

Examinar con especial atención cualquier operación, con independencia de su cuantía, que, por su naturaleza, pueda estar particularmente vinculada al blanqueo de capitales procedentes de actividades delictivas.

- Deber de conservación de documentos

Conservar durante un período mínimo de cinco años los documentos que acrediten adecuadamente la realización de operaciones y la identidad de los sujetos que las hayan realizado o que hayan entablado relaciones de negocio con la entidad.

- Deber de información y comunicación

Comunicar al órgano responsable de la prevención del blanqueo de capitales (en el caso español, el Servicio Ejecutivo de la Co-

misión de Prevención del Blanqueo de Capitales; en adelante, el Servicio Ejecutivo) cualquier hecho u operación respecto a los que exista indicio o certeza de que están relacionados con el blanqueo de capitales, y facilitar la información que sea requerida.

- Deber de abstención

Abstenerse de ejecutar cualquier operación, cuando sepan o sospechen que pueda estar relacionada con el blanqueo de capitales, sin haber informado previamente al órgano responsable de la prevención.

- Deber de confidencialidad

No revelar ni al cliente ni a terceros que se han transmitido informaciones al órgano responsable de la prevención del blanqueo de capitales, o que se está examinando alguna operación por si pudiera estar vinculada con el blanqueo de capitales.

- Deber de organizarse adecuadamente

Establecer procedimientos y órganos adecuados de control interno y de comunicación, para prevenir e impedir la realización de operaciones relacionadas con el blanqueo de capitales.

- Deber de formación

Adoptar las medidas oportunas para que los empleados de la entidad tengan conocimiento de las exigencias legales, y elaborar planes de formación para capacitar a sus empleados en la detección de operaciones relacionadas con el blanqueo de capitales.

4. MEDIDAS NECESARIAS PARA UN ADECUADO CONTROL DE LOS RIESGOS DERIVADOS DEL BLANQUEO DE CAPITALES POR PARTE DE LAS ENTIDADES FINANCIERAS

Las normas y documentos comentados en los apartados anteriores ya ponen de manifiesto algunos de los aspectos que deben tener en cuenta las entidades financieras, en el diseño y puesta en práctica de sus políticas de prevención del blanqueo de capitales. En este apartado se van a sistematizar las medidas que pueden considerarse imprescindibles para un control adecuado de los riesgos en los que incurren las entidades en este ámbito. Para ello, se incorporará a las recomendaciones mencionadas, por una parte, la experiencia acumulada en el Servicio Ejecutivo al analizar la organización de los sujetos obligados, y, por otra, la problemática derivada de alguna de las líneas de negocio de las entidades que

han tenido un mayor desarrollo recientemente. Estas medidas pueden agruparse en dos grandes capítulos: el primero de ellos se refiere a la potenciación del buen gobierno de las entidades; el segundo, al fortalecimiento de las políticas de «Conozca a su cliente», con especial mención a las áreas de mayor riesgo.

4.1. Potenciación del buen gobierno

La potenciación del buen gobierno de las entidades en lo referente a la prevención del blanqueo de capitales debe tener como premisa básica una estricta separación de funciones entre las áreas de control, en las que debe encuadrarse el área responsable de la prevención, y las áreas comerciales responsables del desarrollo del negocio.

Para que esta separación de funciones sea efectiva, es preciso que la estructura organizativa interna sea apropiada. El órgano interno responsable de la prevención del blanqueo de capitales debe tener dentro de la organización un nivel jerárquico adecuado, que permita que tanto sus decisiones sobre clientes y operativas sospechosos como sus iniciativas acerca de las políticas y procedimientos de prevención tengan el efecto necesario en toda la organización. Por otra parte, en ese órgano debe existir una representación de las principales áreas de control y de negocio de la entidad, que permita tener en cuenta todos los enfoques posibles a la hora de tomar decisiones referidas tanto al análisis de operaciones sospechosas como al desarrollo de procedimientos internos de prevención. La presidencia del órgano interno debe recaer en una persona con nivel suficiente, pero encuadrada en las áreas de control.

El segundo aspecto básico hace referencia a que la implicación de la alta dirección de las entidades en la definición e implantación de los procedimientos es totalmente necesaria para conseguir una organización eficaz en la prevención del blanqueo de capitales.

El apoyo de la alta dirección de las entidades, y una estructura organizativa como la comentada, son elementos imprescindibles para conseguir una organización eficaz en la prevención del blanqueo de capitales, que debe asegurar la generalización de los procedimientos y la definición clara de responsabilidades exigibles a las diferentes áreas. Esta generalización de procedimientos debe alcanzar también a todo el grupo consolidable, debiendo programarse, de forma sistemática y exhaustiva, las revisiones de las sociedades filiales que desarrollen su actividad en sectores o territorios con elevado riesgo de blanqueo.

Por último, señalar la importancia de la implicación de la auditoría interna y externa, que deben incluir en sus planes de revisión periódica la verificación del cumplimiento de la normativa y el diseño de pruebas que permitan emitir opinión sobre la aplicación de los procedimientos internos, por parte de las unidades auditadas.

4.2. Fortalecimiento del conocimiento de los clientes

El fortalecimiento de las políticas de «Conozca a su cliente» exige no solo la identificación de los titulares de las cuentas y otros activos, sino también un conocimiento previo y un seguimiento continuo de su actividad que permita establecer su coherencia con la operativa bancaria que desarrolla. Estas políticas deben incluir criterios para la aceptación de clientes y para su rechazo, cuando las actividades desarrolladas por ellos estén en desacuerdo con las directrices fijadas por la alta dirección.

El grado de desarrollo del negocio bancario, y la extensión y sofisticación del mismo, permiten afirmar la necesidad ineludible, al menos para las entidades que alcancen un determinado tamaño, de desarrollar aplicaciones informáticas que faciliten el conocimiento de los clientes y permitan el seguimiento adecuado de su operativa. El desarrollo de estas herramientas, que pueden tener también una gran utilidad desde la óptica del negocio, tiene que tener, como uno de sus objetivos fundamentales, la prevención del blanqueo de capitales. Para ello, deben basarse en una visión global del cliente y sus operaciones, deben definir los distintos perfiles de los clientes, y deben permitir el análisis de alarmas, a través de factores como la evolución de la calificación de los clientes, las pautas de comportamiento, las operativas asociadas a blanqueo de capitales, etc. Estas herramientas, que se orientan al fortalecimiento de la capacidad de análisis de forma centralizada por el órgano interno responsable, deben permitir también el análisis de la operativa sensible por parte de la propia red de oficinas.

La preocupación por este aspecto fundamental para una prevención eficaz del blanqueo de capitales debe llevar a las entidades a extremar las medidas para conocer a sus clientes, incluso cuando se están utilizando personas interpuestas, vehículos societarios o cuentas que puedan recoger fondos de varios titulares.

4.3. Atención especial a las áreas de mayor riesgo de blanqueo de capitales

Los procedimientos para el conocimiento de los clientes deben aplicarse con especial intensidad en algunas áreas de especial riesgo, como la banca privada, la banca no presencial —principalmente, por Internet—, y la banca de corresponsales. En ellas, es preciso definir procedimientos específicos, que permitan compatibilizar la operatividad necesaria con el conocimiento de los clientes, sean entidades financieras o no.

Banca privada

Las entidades que ofrecen servicios de banca privada están especialmente expuestas al riesgo reputacional y, en consecuencia, deberían

prestar una atención especial a las operaciones realizadas, de forma que sea posible compaginar la confidencialidad necesaria con el nivel de conocimiento exigible sobre el origen y destino de los fondos que se transfieran a través de estas cuentas.

Las características de la banca privada (perfil de los clientes, naturaleza de las operaciones y tipo de productos utilizados) la convierten en un negocio de alto riesgo de blanqueo de capitales. El riesgo se incrementa cuando las operaciones se efectúan a través de países o territorios con normas estrictas sobre secreto bancario o secreto profesional y leyes laxas sobre prevención del blanqueo de capitales. Por esta razón, la normativa interna de las entidades que realizan este tipo de negocio debe ser más exigente, y más rigurosos los procedimientos para conocer a los clientes y analizar sus operaciones.

Respecto al conocimiento del cliente, es necesario que los expedientes de todos los clientes contengan la información y documentación necesarias para poder determinar si las operaciones que realizan se corresponden con la actividad real que desarrollan. A los efectos de prevención del blanqueo de capitales, los expedientes de los clientes de banca privada deben contener, como mínimo, los siguientes documentos: formulario de apertura de cuenta, formulario de conocimiento del cliente, fotocopia de un documento oficial de identificación y toda la documentación que acredite la veracidad de la información recogida en los formularios de apertura de cuenta y de conocimiento del cliente.

Para poder determinar si existe coherencia entre la actividad conocida de los clientes y las operaciones que realizan y, por tanto, detectar las operaciones sospechosas que se pudieran plantear, es necesario efectuar un análisis específico de prevención de blanqueo de capitales de las operaciones.

Banca no presencial

El modelo de prevención de blanqueo de capitales implantado en la banca, tanto española como extranjera, está concebido, básicamente, para unidades y negocios de banca tradicional (minorista, corporativa o privada), en los que la gestión comercial se basa en el esquema organizativo formado por la red de oficinas, empleados, clientes, cuentas y operaciones.

En consecuencia, la prevención de blanqueo de capitales se apoya habitualmente en la red de oficinas y en la actividad que desarrollan los empleados bancarios para la identificación de los clientes y para el conocimiento de sus actividades y del origen de sus fondos.

En algunas entidades, el modelo se completa mediante el control de las operaciones que son susceptibles de ser utilizadas para el blanqueo

de capitales, a través de aplicaciones informáticas que permiten conocer las operaciones de riesgo en las oficinas, para proceder a su análisis y poder calificarlas como normales o sospechosas.

En la actualidad, el desarrollo de las nuevas tecnologías está impulsando otras formas de hacer banca. Ya sea como canal alternativo de distribución, ya sea como sistema independiente, la práctica totalidad de las entidades financieras están ofreciendo productos y servicios que implican transacciones *on line*, sin contacto directo con el cliente. Para algunas de estas manifestaciones de banca no presencial, los procedimientos de prevención del blanqueo de capitales aplicados para la banca tradicional no son efectivos.

En la banca no presencial se elimina todo lo que se interpone entre las partes, con el resultado de suprimir muchos de los registros clásicos que generaba la actividad de los bancos y de otras instituciones financieras, que permiten el seguimiento de las operaciones y de sus intervinientes.

Como manifestación más representativa de la banca no presencial hay que considerar a la banca a través de Internet, donde, al menos en el concepto manejado de banca tradicional, no existe red de oficinas, ni empleados en contacto con los clientes, ni clientes físicos; solamente existen cuentas y operaciones bancarias.

En la banca virtual no hay espacios físicos (oficinas) donde se mantenga contacto con el cliente, se realice su identificación material y se instrumenten cara a cara las operaciones. No existen empleados que activen las alertas sobre la base de su experiencia directa con los clientes. Tampoco hay clientes físicos sobre los que desarrollar una actividad de conocimiento. No se puede garantizar que la persona que realiza una operación *on line* sea la que dice ser, con un grado de seguridad similar a como ocurre con la identificación cuando la persona que realiza la operación está presente.

La banca no presencial exige otros procedimientos para cumplir con el principio básico de la prevención de blanqueo de capitales, que es el «Conozca a su cliente», entendido en su sentido más amplio: conocimiento de la actividad que se realiza, del origen y destino de los fondos que utiliza, y de la coherencia entre su actividad y las operaciones que efectúa.

Los organismos internacionales con responsabilidad en la prevención del blanqueo de capitales están alertando sobre los riesgos potenciales derivados de la banca virtual, expresando su preocupación por aspectos fundamentales, como el conocimiento del cliente y la localización de operaciones sospechosas. Esta situación se traduce en advertencias e iniciativas regulatorias para el control de los riesgos de blanqueo derivados de cualquier modalidad de banca virtual.

Como ejemplo en el ámbito de los supervisores, puede citarse el «Manual sobre Banca en Internet», de la Office of the Comptroller of the Currency de los Estados Unidos, en el que se instruye a sus inspectores para que determinen si los controles de los bancos identifican potenciales actividades de lavado de dinero asociadas con negocios en la banca en Internet. En concreto, sobre la localización de las operaciones sospechosas, el Manual dice que los bancos deberán establecer un sistema de control que identifique las actividades inusuales o sospechosas en Internet, y que deben analizar las transacciones buscando anomalías.

Tanto para minimizar los riesgos de blanqueo como para adaptarse a las exigencias de la reciente Directiva en un futuro próximo, las entidades deberán adoptar, en las operaciones a distancia, medidas específicas y adecuadas para compensar el mayor riesgo de blanqueo. Estas medidas deberán permitir el establecimiento de la identidad del cliente, exigiendo determinados documentos justificativos adicionales; fijando procedimientos complementarios encaminados a comprobar los documentos facilitados; imponiendo la confirmación de la identificación expedida por otra institución sujeta a la Directiva; o exigiendo que el primer pago se efectúe a través de una cuenta abierta a nombre del cliente en una entidad de crédito, en la que, por estar sujeta a la Directiva, haya tenido lugar la correspondiente identificación.

Banca de corresponsales

Las últimas iniciativas internacionales sobre la materia otorgan una gran importancia al control de la banca de corresponsales, quizás por haberse demostrado en algunos casos concretos que el mero hecho de que el cliente fuera otra entidad financiera, había provocado una relajación de los controles exigibles al resto de clientes.

Es de destacar, dentro de estas iniciativas, la nueva legislación anti-blanqueo aprobada en los Estados Unidos tras los atentados del 11 de septiembre, que incluye medidas que tienen efectos extraterritoriales, ya que afectan a los bancos que mantienen cuentas de corresponsalía con bancos norteamericanos. Entre otras medidas, destaca la preocupación por la posibilidad de que personas relacionadas con actos delictivos se beneficien de esas cuentas de corresponsalía. Para evitarlo, se establecen requisitos rigurosos sobre la información que es preciso facilitar a las autoridades norteamericanas. Además, se permite la ejecución de órdenes de embargo contra dichas cuentas, en el caso de que, de acuerdo con las leyes federales, proceda la confiscación de fondos que estén depositados en la entidad extranjera que mantiene la cuenta de corresponsalía.

Esta preocupación tiene su origen en los mayores riesgos derivados de la internacionalización de la actividad bancaria, que, para facilitar la rapidez en las transacciones, precisa del establecimiento de unas rela-

ciones de corresponsalía que posibiliten la fluidez de los flujos financieros internacionales.

Por ello, con la finalidad de limitar los riesgos de blanqueo y, al igual que para otros clientes de sectores de alto riesgo, en la banca de corresponsales es necesario establecer procedimientos internos que posibiliten:

- Determinar la legitimidad de las personas, sistemas, claves o códigos que autoricen transacciones financieras en nombre del corresponsal.
- No establecer relaciones de corresponsalía con bancos pantalla, entendiendo por tales los que no tienen presencia física en ningún país ni pertenecen a grupos financieros conocidos con sede en países con suficiente supervisión financiera.
- Rechazar el establecimiento de relaciones con bancos que mantengan relaciones de corresponsalía con bancos pantalla.
- No ofrecer servicios que permitan que los clientes del banco corresponsal puedan hacer uso directo y en su propio nombre de la cuenta corresponsal. Las operaciones que se canalicen a través de las cuentas de los corresponsales deberán tener información suficiente acerca de sus ordenantes, evitando la utilización de cláusulas genéricas.
- Mantener un conocimiento continuo y actualizado de la actividad de los corresponsales, estableciendo, en función de los países en los que radique su sede social, criterios más o menos exigentes sobre la documentación mínima necesaria que debe estar disponible.

5. CONCLUSIONES

En las páginas anteriores se han ido desgranando los retos a los que se enfrentan las entidades financieras, si quieren mantener controlados los riesgos consecuencia de su posible implicación en operaciones relacionadas con el blanqueo de capitales. También se han descrito las medidas cuyo establecimiento se considera necesario para evitar la utilización de las entidades financieras, por parte de las organizaciones delictivas. Los riesgos derivados del blanqueo de capitales, como los demás riesgos en los que incurren las entidades en el desarrollo de su actividad, nunca pueden desaparecer, si bien las medidas propuestas pueden ayudar en gran medida a minimizarlos.

La vigilancia y el control de los riesgos relacionados con el blanqueo de capitales que asumen las entidades financieras están compartidos, en nuestro ordenamiento, por los supervisores sectoriales (el Banco de

España, para las entidades de crédito) y por los organismos encargados específicamente de estas cuestiones (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias). La eficacia en la prevención del blanqueo de capitales depende, ante todo, de los procedimientos establecidos por las propias entidades, pero también puede verse incrementada con el desarrollo de iniciativas regulatorias en el ámbito de la supervisión financiera y con el aumento de la colaboración entre los organismos encargados de la vigilancia y el control de estos riesgos.

Por lo que se refiere a las posibilidades regulatorias, y dentro del marco definido por el Nuevo Acuerdo de Capital del Comité de Basilea, ya existen actualmente suficientes parámetros para la medida de los riesgos relacionados con el blanqueo de capitales, encuadrados en las correspondientes categorías de riesgos. Esos parámetros —definidos por el propio Comité de Basilea, por el GAFI, por otros organismos internacionales y, en nuestro caso, por la legislación comunitaria y española— pueden permitir la definición de modelos para la estimación y medición de estos riesgos. A partir de ellos, sería posible el establecimiento de requerimientos de capital específicos para su cobertura.

En el contexto de la relación entre los organismos responsables de la supervisión y los responsables de la prevención del blanqueo de capitales, existen posibilidades de colaboración que pueden aumentar la eficacia en el marco de las respectivas responsabilidades. En nuestro modelo, es responsabilidad del Servicio Ejecutivo la verificación del cumplimiento de las obligaciones legales por parte de los sujetos obligados. Esta labor debe verse apoyada por los supervisores sectoriales, integrando la revisión de ciertas medidas de prevención dentro de la labor ordinaria de inspección —como el propio Comité de Basilea sugiere— y debe tener su continuación en el intercambio de información sobre las labores de verificación. Por último, la colaboración debería extenderse a la elaboración conjunta de guías o documentos orientativos sobre operativa sospechosa en cada tipo de sujeto, con el objetivo de incentivar la actividad de prevención y detección de operaciones por parte de las entidades.

PUBLICACIONES DEL BANCO DE ESPAÑA

PUBLICACIONES PERIÓDICAS

INFORME ANUAL (ediciones en español e inglés)
CUENTAS FINANCIERAS DE LA ECONOMÍA ESPAÑOLA (edición bilingüe: español e inglés) (anual)
BALANZA DE PAGOS DE ESPAÑA (ediciones en español e inglés) (anual)
CENTRAL DE ANOTACIONES EN CUENTA (anual)
BOLETÍN ECONÓMICO (mensual)
ECONOMIC BULLETIN (trimestral)
BOLETÍN ESTADÍSTICO (mensual)
BOLETÍN DE ANOTACIONES EN CUENTA (diario)
CENTRAL DE BALANCES. RESULTADOS ANUALES DE LAS EMPRESAS NO FINANCIERAS (monografía anual)
CIRCULARES A ENTIDADES DE CRÉDITO
CIRCULARES DEL BANCO DE ESPAÑA. RECOPILOCIÓN (cuatrimestral)
REGISTROS DE ENTIDADES (anual)
ESTABILIDAD FINANCIERA (semestral)
MEMORIA DEL SERVICIO DE RECLAMACIONES (anual)
MEMORIA DE LA SUPERVISIÓN BANCARIA EN ESPAÑA (anual)

ESTUDIOS ECONÓMICOS (SERIE AZUL)

62. ENRIQUE ALBEROLA ILLA: España en la Unión Monetaria. Una aproximación a sus costes y beneficios (1998).
63. GABRIEL QUIRÓS (coordinador): Mercado español de deuda pública. Tomos I y II (1998).
64. FERNANDO C. BALLABRIGA, LUIS JULIÁN ÁLVAREZ GONZÁLEZ Y JAVIER JAREÑO MORAGO: Un modelo macroeconómico BVAR para la economía española: metodología y resultados (1998). (Publicada una edición en inglés con el mismo número.)
65. ÁNGEL ESTRADA Y ANA BUISÁN: El gasto de las familias en España (1999).
66. ROBERTO BLANCO ESCOLAR: El mercado español de renta variable. Análisis de la liquidez e influencia del mercado de derivados (1999).
67. JUAN AYUSO, IGNACIO FUENTES, JUAN PEÑALOSA Y FERNANDO RESTOY: El mercado monetario español en la Unión Monetaria (1999).
68. ISABEL ARGIMÓN, ÁNGEL LUIS GÓMEZ, PABLO HERNÁNDEZ DE COS Y FRANCISCO MARTÍ: El sector de las Administraciones Públicas en España (1999).
69. JAVIER ANDRÉS, IGNACIO HERNANDO AND J. DAVID LÓPEZ-SALIDO: Assessing the benefits of price stability: The international experience (2000).
70. OLYMPIA BOVER Y MARIO IZQUIERDO: Ajustes de calidad en los precios: métodos hedónicos y consecuencias para la Contabilidad Nacional (2001). (Publicada una edición en inglés con el mismo número.)
71. MARIO IZQUIERDO Y M^a DE LOS LLANOS MATEA: Una aproximación a los sesgos de medición de las variables macroeconómicas españolas derivados de los cambios en la calidad de los productos (2001). (Publicada una edición en inglés con el mismo número.)

Nota: La relación completa de cada serie figura en el Catálogo de Publicaciones.

72. MARIO IZQUIERDO, OMAR LICANDRO Y ALBERTO MAYDEU: Mejoras de calidad e índices de precios del automóvil en España (2001). (Publicada una versión inglesa con el mismo número.)
73. OLYMPIA BOVER Y PILAR VELLILLA: Precios hedónicos de la vivienda sin características: el caso de las promociones de viviendas nuevas (2001). (Publicada una versión inglesa con el mismo número.)
74. MARIO IZQUIERDO Y M^a DE LOS LLANOS MATEA: Precios hedónicos para ordenadores personales en España durante la década de los años noventa (2001). (Publicada una versión inglesa con el mismo número.)

ESTUDIOS DE HISTORIA ECONÓMICA (SERIE ROJA)

32. SEBASTIÁN COLL Y JOSÉ IGNACIO FORTEA: Guía de fuentes cuantitativas para la historia económica de España. Vol. I: Recursos y sectores productivos (1995).
33. FERNANDO SERRANO MANGAS: Vellón y metales preciosos en la Corte del Rey de España (1618-1668) (1996).
34. ALBERTO SABIO ALCUTÉN: Los mercados informales de crédito y tierra en una comunidad rural aragonesa (1850-1930) (1996).
35. M^a GUADALUPE CARRASCO GONZÁLEZ: Los instrumentos del comercio colonial en el Cádiz del siglo XVII (1650-1700) (1996).
36. CARLOS ÁLVAREZ NOGAL: Los banqueros de Felipe IV y los metales preciosos americanos (1621-1665) (1997).
37. EVA PARDOS MARTÍNEZ: La incidencia de la protección arancelaria en los mercados españoles (1870-1913) (1998).
38. ELENA MARÍA GARCÍA GUERRA: Las acuñaciones de moneda de vellón durante el reinado de Felipe III (1999).
39. MIGUEL ÁNGEL BRINGAS GUTIÉRREZ: La productividad de los factores en la agricultura española (1752-1935) (2000).
40. ANA CRESPO SOLANA: El comercio marítimo entre Amsterdam y Cádiz (1713-1778) (2000).
41. LLUIS CASTAÑEDA PEIRÓN: El Banco de España (1874-1900): la red de sucursales y los nuevos servicios financieros (2001).
42. SEBASTIÁN COLL Y JOSÉ IGNACIO FORTEA: Guía de fuentes cuantitativas para la historia económica de España. Vol. II: Finanzas y renta nacional (2002).
43. ELENA MARTÍNEZ RUIZ: El sector exterior durante la autarquía. Una reconstrucción de las balanzas de pagos de España, 1940-1958 (2002).

DOCUMENTOS DE TRABAJO

- 0020 JORDI GALÍ, MARK GERTLER AND J. DAVID LÓPEZ-SALIDO: European inflation dynamics.
- 0101 SILVIO RENDÓN: Job Creation under Liquidity Constraints: The Spanish Case.
- 0102 RAVI BALAKRISHNAN: The interaction of firing costs and on-the-job search: an application of a search theoretic model to the Spanish labour market.
- 0103 FRANCISCO DE CASTRO, JOSÉ MANUEL GONZÁLEZ-PÁRAMO AND PABLO HERNÁNDEZ DE COS: Evaluating the dynamics of fiscal policy in Spain: patterns of interdependence and consistency of public expenditure and revenues.
- 0104 CARSTEN KRABBE NIELSEN: Three Exchange Rate Regimes and a Monetary Union: Determinacy, Currency Crises, and Welfare.
- 0105 JUAN AYUSO AND RAFAEL REPULLO: Why Did the Banks Overbid? An Empirical Model of the Fixed Rate Tenders of the European Central Bank.
- 0106 FRANCISCO J. RUGE-MURCIA: Inflation targeting under asymmetric preferences.
- 0107 JOSÉ VIÑALS: Monetary policy issues in a low inflation environment.
- 0108 AGUSTÍN MARAVALL AND ANA DEL RÍO: Time aggregation and the Hodrick-Prescott filter.

- 0109 JORDI GALÍ AND J. DAVID LÓPEZ-SALIDO: A new Phillips curve for Spain.
- 0110 ÁNGEL ESTRADA AND DAVID LÓPEZ-SALIDO: Accounting for Spanish productivity growth using sectoral data: New evidence.
- 0111 FRANCISCO ALONSO, ROBERTO BLANCO AND ANA DEL RÍO: Estimating inflation expectations using French government inflation-indexed bonds.
- 0112 GIANLUCA CAPORELLO, AGUSTÍN MARAVALL AND FERNANDO J. SÁNCHEZ: Program TSW. Reference manual.
- 0113 SOLEDAD NÚÑEZ RAMOS Y MIGUEL PÉREZ GARCÍA-MIRASIERRA: El grado de concentración en las ramas productivas de la economía española.
- 0114 KLAUS DESMET AND IGNACIO ORTUÑO ORTÍN: Rational underdevelopment.
- 0115 MATTEO CICCARELLI AND ALESSANDRO REBUCCI: The transmission mechanism of European monetary policy: Is there heterogeneity? Is it changing over time?
- 0116 ÁNGEL ESTRADA AND J. DAVID LÓPEZ SALIDO: Sectoral and Aggregate Technology Growth in Spain.
- 0117 IGNACIO HERNANDO AND JORGE MARTÍNEZ PAGÉS: Is there a bank lending channel of monetary policy in Spain?
- 0118 MICHAEL EHRMANN, LEONARDO GAMBACORTA, JORGE MARTÍNEZ PAGÉS, PATRICK SEVESTRE AND ANDREAS WORMS: Financial systems and the role of banks in monetary policy transmission in the euro area.
- 0119 J. B. CHATELAIN, A. GENERALE, I. HERNANDO, U. VON KALCKREUTH AND P. VERMEULEN: Firm investment and monetary policy transmission in the euro area.
- 0120 ROBERTO BLANCO: The euro-area government securities markets. Recent developments and implications for market functioning.
- 0121 JAVIER ANDRÉS, J. DAVID LÓPEZ-SALIDO AND JAVIER VALLÉS: Money in an estimated business cycle model of the euro area.
- 0201 SOLEDAD NÚÑEZ RAMOS: La contribución de las ramas productoras de bienes y servicios TIC al crecimiento de la economía española.
- 0202 LUIS JULIÁN ÁLVAREZ GONZÁLEZ Y JAVIER JAREÑO MORAGO: Implicaciones para la inflación de la conversión de precios a euros.
- 0203 IGNACIO HERNANDO AND SOLEDAD NÚÑEZ: The contribution of ict to economic activity: a growth accounting exercise with Spanish firm-level data.
- 0204 JORDI GALÍ, MARK GERTLER AND J. DAVID LÓPEZ-SALIDO: Markups, gaps, and the welfare costs of business fluctuations.
- 0205 ÁNGEL ESTRADA AND J. DAVID LÓPEZ-SALIDO: Understanding Spanish dual inflation.
- 0206 ÁNGEL ESTRADA, PILAR GARCÍA-PEREA Y MARIO IZQUIERDO: Los flujos de trabajadores en España. El impacto del empleo temporal.
- 0207 AGUSTÍN MARAVALL: An Application of TRAMO-SEATS: Automatic Procedure and Sectoral Aggregation. The Japanese Foreign Trade Series.
- 0208 REGINA KAISER AND AGUSTÍN MARAVALL: A Complete Model-Based Interpretation of the Hodrick-Prescott Filter: Spuriousness Reconsidered.
- 0209 ANDREW BENITO AND GARRY YOUNG: Financial Pressure and Balance Sheet Adjustment by UK Firms.
- 0210 S. G. CUENTAS NACIONALES (INSTITUTO NACIONAL DE ESTADÍSTICA): Ajuste estacional y extracción de señales en la Contabilidad Nacional Trimestral.
- 0211 ALBERTO CABRERO, GONZALO CAMBA-MÉNDEZ, ASTRID HIRSCH AND FERNANDO NIETO: Modelling the Daily Banknotes in Circulation in the Context of the Liquidity Management of the European Central Bank.
- 0212 ALPO WILLMAN AND ÁNGEL ESTRADA: The Spanish block of the ESCB-Multi-Country model.
- 0213 ENRIQUE ALBEROLA, ANA BUISÁN AND SANTIAGO FERNÁNDEZ DE LIS: The quest for nominal and real convergence through integration in Europe and Latin America.
- 0214 IGNACIO HERNANDO AND ANDRÉ TIOMO: Financial constraints and investment in France and Spain: a comparison using firm level data.
- 0215 PIERPAOLO BENIGNO AND J. DAVID LÓPEZ-SALIDO: Inflation Persistence and Optimal Monetary Policy in the Euro Area.
- 0216 ALICIA GARCÍA HERRERO, JAVIER SANTILLÁN, SONSOLES GALLEGO, LUCÍA CUADRO AND CARLOS EGEA: Latin American financial development in perspective.

- 0217 SONSOLES GALLEGO, ALICIA GARCÍA HERRERO AND JESÚS SAURINA: The Asian and European Banking Systems: The case of Spain in the quest for development and stability.
- 0218 JOSÉ RAMÓN MARTÍNEZ RESANO AND LILIANA TOLEDO FALCÓN: Futuros sobre acciones: Demanda e implicaciones sobre los mercados de renta variable.
- 0219 JOSÉ MANUEL CAMPA AND JOSÉ M. GONZÁLEZ MÍNGUEZ: Differences in exchange rate passthrough in the euro area.
- 0220 LUIS JULIÁN ÁLVAREZ GONZÁLEZ Y JAVIER JAREÑO MORAGO: ISIS: Un indicador sintético integral de los Servicios de Mercado.
- 0221 MARCO HOEBERICHTS: The Credibility of Central Bank Announcements.
- 0222 KLAUS DESMET: Asymmetric Shocks, Risk Sharing, and the Latter Mundell.

EDICIONES VARIAS (1)

- SERVICIOS JURÍDICOS DEL BANCO DE ESPAÑA: Legislación de entidades de depósito y otros intermediarios financieros: normativa *autonómica* (1990). Segunda edición. 36,06 € (*).
- BANCO DE ESPAÑA: Monedas de Oro de la Colección del Banco de España (1991). 48,08 € (*).
- PEDRO MARTÍNEZ MÉNDEZ: Los beneficios de la banca (1970-1989) (1991). 12,50 € (*).
- SERVICIOS JURÍDICOS DEL BANCO DE ESPAÑA: Legislación de Entidades de Crédito: normativa general. 3ª ed. (1994). 36,06 € (*).
- MARÍA JOSÉ TRUJILLO MUÑOZ: La potestad normativa del Banco de España: el régimen dual establecido en la Ley de Autonomía (1995). 3,13 € (*).
- BANCO DE ESPAÑA: Tauromaquia. Catálogo comentado sobre la Tauromaquia, de Francisco de Goya, referido a una primera tirada de esta serie, propiedad del Banco de España (1996). 5 € (*).
- JUAN LUIS SÁNCHEZ-MORENO GÓMEZ: Circular 8/1990, de 7 de septiembre. Concordancias legales (1996). 6,25 € (*).
- RAMÓN SANTILLÁN: Memorias (1808-1856) (1996) (***).
- BANCO DE ESPAÑA. SERVICIO DE ESTUDIOS (ed.): La política monetaria y la inflación en España (1997) (**).
- BANCO DE ESPAÑA: La Unión Monetaria Europea: cuestiones fundamentales (1997). 3,01 € (*).
- TERESA TORTELLA: Los primeros billetes españoles: las «Cédulas» del Banco de San Carlos (1782-1829) (1997). 28,13 € (*).
- JOSÉ LUIS MALO DE MOLINA, JOSÉ VIÑALS AND FERNANDO GUTIÉRREZ (eds.): Monetary policy and inflation in Spain (1998) (****).
- SERVICIO JURÍDICO DEL BANCO DE ESPAÑA: Legislación de Entidades de Crédito. 4ª ed. (1999). 36,06 € (*).
- VICTORIA PATXOT: Medio siglo del Registro de Bancos y Banqueros (1947-1997) (1999). Libro y disquete: 5,31 € (*).
- PEDRO TEDDE DE LORCA: El Banco de San Fernando (1829-1856) (1999) (**).
- BANCO DE ESPAÑA (ed.): Arquitectura y pintura del Consejo de la Reserva Federal (2000). 12,02 € (*).
- PABLO MARTÍN ACEÑA: El Servicio de Estudios del Banco de España (1930-2000) (2000). 9,02 € (*).
- TERESA TORTELLA: Una guía de fuentes sobre inversiones extranjeras en España (1780-1914) (2000). 9,38 € (*).
- VICTORIA PATXOT Y ENRIQUE GIMÉNEZ-ARNAU: Banqueros y bancos durante la vigencia de la Ley Cambó (1922-1946) (2201). 5,31 € (*).
- BANCO DE ESPAÑA (ed.): El camino hacia el euro. El real, el escudo y la peseta (2001). 45 €.

(1) Las publicaciones marcadas con un asterisco (*) son distribuidas por el Banco de España, Sección de Publicaciones. Los precios llevan incluido el 4 % de IVA. Las publicaciones marcadas con dos asteriscos (**) son distribuidas por Alianza Editorial. Las publicaciones marcadas con tres asteriscos (***) son distribuidas por Editorial Tecnos. Las publicaciones marcadas con cuatro asteriscos (****) son distribuidas por Macmillan (Londres).

DISTRIBUCIÓN, TARIFAS Y MODALIDADES DE SUSCRIPCIÓN (2003)

BANCO DE ESPAÑA

I. ESTUDIOS E INFORMES

PERIÓDICOS

Informe anual (ediciones en español e inglés)
Balanza de Pagos de España (anual) (ediciones en español e inglés)
Boletín económico (mensual) (hay una versión en inglés de periodicidad trimestral)
Central de Anotaciones. Memoria (anual)
Memoria del Servicio de Reclamaciones (anual)
Estabilidad financiera (semestral)
Memoria de la Supervisión Bancaria en España (anual) (hay una versión en inglés)

NO PERIÓDICOS

Estudios Económicos (Serie azul)
Estudios de Historia Económica (Serie roja)
Documentos de Trabajo
Central de Balances: estudios de encargo
Notas de estabilidad financiera
Ediciones varias
Manual de la Central de Anotaciones

II. DIFUSIÓN ESTADÍSTICA

Boletín estadístico (mensual) (actualización diaria en Internet)
Cuentas financieras de la economía española (series trimestrales, publicación anual) (edición bilingüe: español e inglés) (actualización trimestral en Internet)
Central de Balances. Resultados anuales de las empresas no financieras (monografía anual) (hay una edición en CD Rom)
Central de Balances Trimestral (se incluye en los boletines económicos de marzo, junio, septiembre y noviembre)
Boletín de anotaciones en cuenta (diario) (solo disponible en versión electrónica en la página *web*)

III. LEGISLACIÓN FINANCIERA Y REGISTROS OFICIALES

Circulares a entidades de crédito
Circulares del Banco de España (recopilación) (cuatrimestral)
Registros de entidades (anual)

IV. FORMACIÓN

Textos del Área de Desarrollo de Recursos Humanos

BANCO CENTRAL EUROPEO

Informe anual, Boletín mensual y Otras publicaciones.

INFORMACIÓN, SUSCRIPCIÓN Y VENTA

Todas las publicaciones que el Banco de España edite a partir de este momento, a excepción del *Boletín de la Central de Anotaciones*, *Textos del Área de Desarrollo de Recursos Humanos* y *Ediciones varias*, se harán simultáneamente en impresión y en formato electrónico, que estará disponible en la página *web* del Banco de España (www.bde.es), donde podrán ser descargadas GRATUITAMENTE, así como un elevado número de publicaciones anteriores. La relación de las publicaciones descargables puede ser consultada en el Catálogo, que está publicado en la página anteriormente mencionada.

PUBLICACIONES IMPRESAS

Todas las publicaciones, a excepción del *Boletín estadístico*, *Central de Balances: estudios de encargo*, *Circulares* (recopilación), *Textos del Área de Desarrollo de Recursos Humanos* y *Ediciones varias*, se pueden obtener gratuitamente, solicitándolas a la Sección de Publicaciones mediante escrito a la dirección postal que figura al final de esta página. El Banco de España reserva un número limitado de ejemplares a este fin, agotados los cuales no se compromete a su reedición, pudiendo reducir el número de ejemplares demandados por un mismo solicitante.

El Banco de España admite la incorporación a la lista de distribución de las siguientes publicaciones: *Boletín económico*, *Boletín Mensual del Banco Central Europeo*, *Documentos de Trabajo*, *Estabilidad financiera* y *Notas de estabilidad financiera*, reservándose el derecho de suspender el envío sin preaviso de ningún tipo, así como de reducir el número de ejemplares demandados por un mismo solicitante. Las personas interesadas en ser incluidas en estas listas deberán solicitarlo a la Sección de Publicaciones, mediante escrito a la dirección postal que figura al final de esta página.

PUBLICACIONES	TARIFAS (1)			
	VENTA		SUSCRIPCIÓN	
	ESPAÑA (IVA incluido)	EXTRANJERO (sin IVA)	ESPAÑA (IVA incluido)	EXTRANJERO (sin IVA)
Boletín estadístico	12,50 €	18,03 €	125,01 €	186,31 €
Circulares del Banco de España: recopilación completa	43,75 €	84,14 €	43,75 €	84,14 €
Circulares del Banco de España (recopilación): actualización anual			18,75 €	36,06 €
Central de Balances: estudios de encargo	Consultar al Servicio de Difusión de la Central de Balances (tels. 913 386 931, 913 386 929 y 913 386 930, fax 913 386 880; envíos postales a calle Alcalá, 50, 28014 Madrid).			
Textos del Área de Desarrollo de Recursos Humanos	Consultar precios en el Catálogo			
Ediciones varias				

(1) Los precios para España llevan incluido el 4 % de IVA. Canarias, Ceuta, Melilla y extranjero están exentos del IVA, así como los residentes en el resto de la Unión Europea que comuniquen el NIF.

Los interesados en suscribirse (indicar la suscripción deseada) o en adquirir alguna de las publicaciones anteriores podrán hacerlo mediante: transferencia a la cuenta corriente 9000.0001.20.0250974114, abierta en el Banco de España en Madrid, a favor de Publicaciones del Banco de España; cheque nominativo a favor de Publicaciones del Banco de España; o en la ventanilla de Publicaciones, Alcalá, 50, 28014 Madrid. En el caso de optar por el pago por transferencia, tendrán que remitir copia de la orden de dicha transferencia, por correo o por fax (913 386 488); si elige el pago mediante cheque, podrá hacerlo, bien por correo, o bien en ventanilla.

Información: Banco de España, Sección de Publicaciones, Alcalá, 50, 28014 Madrid. Teléfono 913 386 364.
 e-mail: publicaciones@bde.es

Información más detallada en: www.bde.es