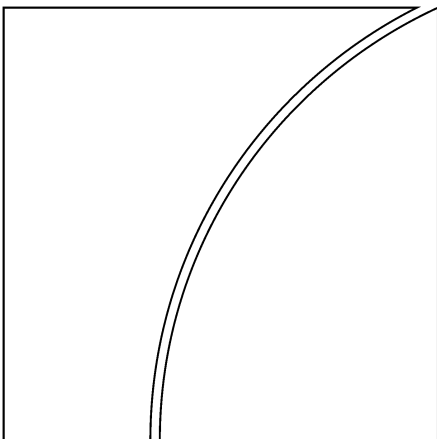


Basel Committee on Banking Supervision



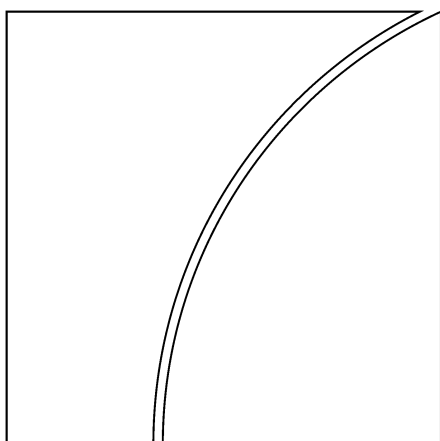
Debida diligencia con la clientela de los bancos

Octubre de 2001



BANK FOR INTERNATIONAL SETTLEMENTS

Comité de Supervisión Bancaria de Basilea



Debida diligencia con la clientelade los bancos

*Este documento ha sido traducido por ASBA y editado por
el BPI*

Octubre de 2001



BANCO DE PAGOS INTERNACIONALES

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
Sutherland

Sr. D Munro

Autoridad Monetaria de las Islas Caimán

Sr. John Bourbon
Sra. Anna McLean

Banco de Francia / Comisión Bancaria

Sr. Laurent Etori

Oficina Federal de Supervisión Bancaria de Alemania

Sr. Jochen Sanio
Sr. Peter Kruschel

Comisión de Servicios Financieros de Guernesey

Sr. Peter G Crook (hasta
abril 2001)
Sr. Philip Marr (desde
abril 2001)

Banco de Italia
Godano

Sr. Giuseppe

Agencia de Servicios Financieros de Japón

Sr. Kiyotaka Sasaki
(hasta julio 2001)
Sr. Hisashi Ono (desde
julio 2001)

Comisión de Supervisión del Sector Financiero de Luxemburgo

Sr. Romain Strock

Autoridad Monetaria de Singapur
Hong

Sra. Foo-Yap Siew

Srta. Teo Lay Har

Comisión Federal de Bancos de Suiza
Zuberbühler

Sr. Daniel

Srta. Dina Balleyguier

Autoridad de Servicios Financieros del Reino Unido

Sr. Richard Chalmers

Junta de Gobernadores del Sistema de la Reserva Federal
de EEUU
Ryback

Sr. William

Banco de la Reserva Federal de Nueva York
Bercovici

Oficina del Contralor de la Moneda de EEUU

Secretaría
Khoo

Srta. Nancy

Sr. José Tuya
Srta. Tanya Smith

Sr. Andrew

Índice

I.	Introducción.....	2
II.	Importancia de las normas KYC para supervisores y bancos.....	3
III.	Elementos esenciales de las normas KYC.....	6
	1. Política de aceptación de clientes.....	6
	2. Identificación de clientes.....	7
	2.1 Requisitos generales de identificación.....	8
	2.2 Cuestiones específicas de identificación.....	9
	2.2.1 Cuentas de fideicomiso, de nominatario y fiduciarias....	9
	2.2.2 Vehículos corporativos.....	10
	2.2.3 Negocios presentados.....	10
	2.2.4 Cuentas de clientes abiertas por intermediarios profesionales.....	11
	2.2.5 Personas del medio político.....	12
	2.2.6 Clientes no presentes.....	13
	2.2.7 Banca corresponsal.....	14
	3. Seguimiento continuo de las cuentas y transacciones.....	15
	4. Gestión de riesgos.....	16
IV.	El papel de los supervisores.....	17
V.	Aplicación de las normas KYC en un contexto transterritorial.....	18
	Anexo 1: Extractos de <i>Metodología de los Principios Básicos</i>	21
	Anexo 2: Extractos de las Recomendaciones FATF.....	23

Debida diligencia con la clientela de los bancos

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 Transterritorial¹ 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 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

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.

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 sólo 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 recomienda 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 KYC 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 dinero³ 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:

³ Ver las recomendaciones FATF números 10 a 19 reproducidas en el Anexo 2.

- 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 reputación 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, se negocie 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 sólo 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 voluntarios⁴ 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 KYC

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 estipula 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

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.

Básicos, e incluye una lista de criterios esenciales 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:

- 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.

⁵ “Metodología de Principios Básicos”, Criterio Esencial 1.

22. Los bancos deberían poner en práctica un procedimiento sistemático de identificación de nuevos clientes y establecer una relación bancaria sólo 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 sólo 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 mismos⁷. 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 director 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 periodo 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.

⁶ “Metodología de Principios Básicos”, Criterio Esencial 2.

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

⁸ “Metodología de Principios Básicos”, Criterio Esencial 2.

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.

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 numeradas¹⁰ 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, ésta 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 de la función de cumplimiento del banco o de 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

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

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

de la identidad de cualquier intermediario y de las personas que representan quienes 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 beneficiarios¹¹.

2.2.2 Vehículos corporativos

33. Los bancos deben estar alertos para evitar que las personas físicas utilicen a las entidades comerciales corporativas como un método 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 deberá 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 presentador¹²:

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

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.

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 posible 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 abogados¹³ 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

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

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.

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 pertinente¹⁴. 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.

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.

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 y 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 las 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 aquél 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 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 riesgos¹⁵.

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.

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.

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 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. Sólo 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 sólo 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 ellas¹⁶. Como no todas las PEP son identificables desde un principio y, además, los 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

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.

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 procedimientos 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, a ejercer permanentemente debida diligencia en el manejo de las cuentas de los clientes y a 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 sólo 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 nacional¹⁷. 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. 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 KYC 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. Ésta 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.

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

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 éstas 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 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 mutua¹⁸ para facilitar el intercambio de información entre los dos supervisores.

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

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

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 periodo 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 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 (reguladores 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 ésta 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 de la 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 FATF

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 éstos 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 e 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.