Comité de Basilea sobre Supervisión Bancaria

Diligencia debida de los Clientes para los bancos

Octubre 2001

BANK FOR INTERNATIONAL SETTLEMENTS

Grupo de Trabajo sobre Banca Internacional

Co-Presidentes :

Sr. Charles Freeland, Subsecretario General, Comité de Basilea sobre Supervisión Bancaria.

Sr. Colin Powel, Presidente del Grupo Extranjero de Supervisores Bancarios, y Presidente de la Comisión de Servicios Financieros de Jersey.

Autoridad Monetaria de Bermuda	Sr. D. Munro Sutherland
Autoridad Monetaria de Islas Cayman	Sr. John Bourbon
Banco de Francia / Comisión Bancaria	Sr. Laurent Ettori
Oficia de Supervisión Bancaria Federal, Alemania	Sr. Jochen Sanio
	Sr. Peter Kurschel
Comisión de Servicios Financieros de Guernsey	Sr. Peter G. Crook (hasta Abril 2001)
	Sr. Philip Marr (desde Abril 2001)
Banca d'Italia	Sr. Giuseppe Godano
Agencia de Servicios Financieros, Japón	Sr. Kiyotaka Sasaki (hasta Julio 2001)
	Sr.Hisashi Ono (desde Julio 2001)
Comisión de Supervisión del Sector Financiero Luxemburgo	Sr. Romain Strock
Autoridad Monetaria de Singapur	Sra. Foo-Yap Siew Hong
	Srta. Teo Lay Har
Comisión Bancaria Federal Suiza	Sr. Daniel Zuberbühler
	Srta. Dina Balleyguier
Autoridad de Servicios Financieros, Reino Unido	Sr. Richard Chalmers
Junta de Gobernadores del Sistema de la Reserva Federal	Sr. William Ryback
Banco de la Reserva Federal de Nueva York	Srta. Nancy Bercovici
Interventor de Bancos Nacionales	Sr. José Tuya
	Srta Tanya Smith
Secretario	Sr. Andrew Khoo

Indice

N.T. : **KYC** (**K**now **Y**our **C**ustomer : Conozca a su cliente)

Diligencia debida de Clientes para los Bancos

I. Introducción

1. Los supervisores en todo el mundo están reconociendo de manera creciente la importancia de asegurarse de que sus bancos tengan instalados controles y procedimientos adecuados de modo que ellos conozcan a los clientes con quienes están operando. Una adecuada diligencia debida sobre los clientes nuevos y los existentes es una parte clave de estos controles. Sin esta diligencia debida, los bancos pueden llegar a estar sujetos a riesgos en su reputación, riesgos operativos, legales y de concentración que pueden resultar en un costo financiero significativo.

2. Al revisar los hallazgos en una investigación interna de bancos internacionales in 1999, el Comité de Basilea identificó deficiencias en las políticas de "conozca-a-su-cliente" (KYC) para los bancos en un gran número de países**.** Juzgado desde una perspectiva de supervisión, las políticas KYC en algunos países tienen brechas significativas y en otros las mismas son inexistentes. Aún entre los países con mercados financieros bien desarrollados, la medida de la robustez de las KYC varía. En consecuencia, el Comité de Basilea solicitó al Grupo de Trabajo sobre Banca Internacional que examinara los procedimientos KYC instalados actualmente y que delineara las normas recomendadas aplicables a los bancos en todos los países. El escrito resultante fue emitido como un documento de consulta en Enero 2001. Luego de una revisión de los comentarios recibidos, el Grupo de Trabajo ha revisado el documento y el Comité de Basilea lo está distribuyendo ahora en todo el mundo en la esperanza de que el marco de KYC presentado aquí se volverá un punto de referencia para que los supervisores establezcan prácticas nacionales y para que los bancos diseñen sus propios programas. Es importante reconocer que las prácticas de supervisión de algunas jurisdicciones ya cumplen o exceden el objetivo de este documento y, como resultado, puede ser que ellos no necesiten implementar ningún cambio.

3. KYC está muy asociada con la lucha contra el lavado de dinero, que es esencialmente el área de la Fuerza de Tareas de Acción Financiera (FATF, por sus siglas en inglés). No es intención del Comité duplicar los esfuerzos de la FATF. Por el contrario, el interés del Comité es desde una perspectiva prudencial más amplia. Políticas y procedimientos KYC sólidos son esenciales en la protección de la seguridad y la solidez de los bancos y la integridad de los sistemas bancarios. El Comité de Basilea y el Grupo Internacional de Supervisores Bancarios (OGBS, por sus siglas en inglés) continúan apoyando fuertemente la adopción e implementación de las recomendaciones de la FATF, particularmente aquéllas relativas a los bancos y pretenden que las normas en este documento sean coincidentes con las recomendaciones de la FATF. El Comité y el OGBS considerarán también la adopción de cualquier norma más alta introducida por la FATF como resultado de su actual revisión de las 40 recomendaciones. En consecuencia, el Grupo de Trabajo ha estado y continuará estando en estrecho contacto con la FATF a medida que desarrolla sus ideas.

4. El enfoque del Comité de Basilea hacia las KYC es desde una perspectiva prudencial más amplia, no sólo contra el lavado de dinero**.** Los procedimientos KYC sólidos deben ser vistos como un elemento esencial en el manejo efectivo de los riesgos bancarios. Las salvaguardas KYC van más allá de la simple apertura y mantenimiento del registro de cuentas y requieren que los bancos formulen una política de aceptación de clientes y un programa de identificación de clientes importantes que involucre una diligencia debida más extensa para las cuentas de más alto riesgo e incluya un monitoreo de cuentas proactivo para actividades sospechosas.

5. El interés del Comité de Basilea en normas KYC sólidas se origina en su preocupación por la integridad de los mercados y se ha incrementado por las pérdidas directas e indirectas en las que han incurrido los bancos debido a su falta de diligencia al aplicar procedimientos adecuados. Estas pérdidas probablemente podrían haber sido evitadas y el daño a la reputación de los bancos habría disminuido significativamente si los bancos hubieran mantenido programas de KYC efectivos.

6. Este documento refuerza los principios establecidos en anteriores documentos del Comité suministrando una guía más precisa sobre los elementos esenciales de las normas KYC y su implementación. Al desarrollar esta guía, el Grupo de Trabajo ha extraído de las prácticas en los países miembros y tomado en cuenta la evolución de los cambios en supervisión. Los elementos esenciales presentados en este documento son una guía en cuanto a los standards mínimos para la implementación mundial para todos los bancos. Estos standards pueden necesitar ser complementados y/o reforzados por medidas adicionales diseñadas a la medida de los riesgos de instituciones particulares y los riesgos en el sistema bancario de países individuales. Por ejemplo, se requiere una mayor diligencia en el caso de cuentas de riesgo más alto o para los bancos que específicamente apuntan a atraer clientes de alto patrimonio neto. En un número de secciones específicas de este documento, hay recomendaciones de mayores standards de diligencia debida para áreas de riesgo más alto dentro de un banco, según corresponda.

7. La necesidad de standards rigurosos de diligencia debida para los clientes no está restringida a los bancos**.** El

Comité de Basilea cree que se debe desarrollar una guía similar para todas las instituciones financieras no bancarias e intermediarios profesionales de servicios financieros tales como abogados y contadores.

II. Importancia de las normas KYC para supervisores y bancos

8. La FATF y otras agrupaciones internacionales han trabajado intensamente sobre los temas de KYC, y las 40 Recomendaciones de la FATF sobre la lucha contra el lavado de dinero tienen reconocimiento y aplicación internacional**.** No es intención de este documento duplicar ese trabajo.

9. Al mismo tiempo**,** los procedimientos sólidos de KYC tienen relevancia particular para la seguridad y solidez de los bancos en (el sentido de) que :

> Los mismos ayudan a proteger la reputación de los bancos y la integridad de los sistemas bancarios reduciendo la probabilidad de que los bancos se conviertan en un vehículo o una víctima del delito financiero y de que sufran el consiguiente daño en su reputación.
>
> Ellos constituyen una parte esencial del manejo sólido del riesgo (por ejemplo, suministrando las bases para la identificación, la limitación y el control de las exposiciones al riesgo en activos y y pasivos, incluyendo los activos bajo administración).

10. La falta de adecuación o la ausencia de normas KYC pueden someter a los bancos a serios riesgos de clientes y contrapartes, especialmente **riesgos sobre su reputación, riesgos operativos, legales y de concentración.** Vale la pena notar que todos estos riesgos están interrelacionados. Sin embargo, cualquiera de ellos puede resultar en un costo financiero significativo para los bancos (por ej., por medio del retiro de fondos de los depositantes, la terminación de las facilidades interbancarias, demandas contra el banco, costos de investigación, embargos y congelamientos de activos, y pérdidas en préstamos), como así también la necesidad de distraer tiempo y energía considerables de la gerencia para resolver los problemas que surjan.

11. **El riesgo sobre la reputación** impone una amenaza importante a los bancos, dado que la naturaleza de su negocio requiere la confianza de los depositantes, los acreedores y el mercado en general. El riesgo sobre la reputación se define como la posibilidad de que la publicidad adversa con respecto a las prácticas operativas y las asociaciones de un banco, ya sea exacta o no, cause una pérdida de confianza en la integridad de la institución. Los bancos son especialmente vulnerables al riesgo sobre su reputación debido a que ellos pueden fácilmente llegar a ser un vehículo o una víctima de actividades ilegales perpetradas por sus clientes. Ellos necesitan protegerse por medio de una continua vigilancia a través de un efectivo programa de KYC. Los activos bajo administración, o mantenidos en forma fiduciaria, pueden plantear peligros particulares sobre la reputación.

12. **El Riesgo Operativo** puede definirse como el riesgo de pérdida directa o indirecta resultante de procesos, personas y sistemas internos inadecuados o fallados o de acontecimientos externos. La mayor parte del riesgo operativo en el contexto de las KYC se refiere a la debilidad en la implementación de los programas de los bancos, a los inefectivos procedimientos de control y la omisión de practicar la diligencia debida. Una percepción pública de que un banco no puede manejar de manera efectiva su riesgo operativo puede alterar o afectar adversamente el negocio del banco.

13. **El Riesgo Legal** es la posibilidad de que juicios, sentencias adversas o contratos que resulten ser inexigibles puedan alterar o afectar adversamente las operaciones o la situación de un banco. Los bancos pueden llegar a estar sujetos a juicios resultantes de la omisión de observar normas KYC obligatorias o de la omisión de practicar la diligencia debida. En consecuencia, los bancos pueden, por ejemplo, sufrir multas, responsabilidades penales y sanciones especiales impuestas por los supervisores. De hecho, un caso en tribunales que involucre a un banco puede tener implicancias de costo mucho mayores para su negocio que sólo costos legales. Los bancos no podrán protegerse efectivamente de tales riesgos legales si ellos no se comprometen con la diligencia debida al identificar a sus clientes y entender sus negocios.

14. La preocupación de los supervisores acerca del riesgo de concentración se aplica mayormente sobre el lado del activo del balance**.** Como práctica común, los supervisores no sólo requieren de los bancos que tengan sistemas de información para identificar las concentraciones de créditos sino que la mayoría fija también límites prudenciales para restringir las exposiciones de los bancos a prestatarios individuales o a grupos de prestatarios relacionados. Sin conocer precisamente quiénes son los clientes, y su relación con otros clientes, no será posible para un banco medir su riesgo de concentración. Esto es particularmente relevante en el contexto de contrapartes relacionadas y préstamos conectados.

15. En el lado del pasivo, el riesgo de concentración está estrechamente asociado al riesgo en el fondeo, particularmente el riesgo de retiro anticipado y repentino de fondos por parte de grandes depositantes, con consecuencias potencialmente dañinas para la liquidez del banco. El riesgo en el fondeo tiene más posibilidad de ser mayor en el caso de los bancos pequeños y de aquéllos que sean menos activos en los mercados mayoristas que en los bancos grandes. El análisis de las concentraciones de depósitos requiere de los bancos entender las características de sus depositantes, incluyendo no sólo sus identidades sino también la medida en la que sus acciones puedan estar ligadas con las de otros depositantes. Es esencial que los gerentes de pasivos en los bancos pequeños no sólo conozcan sino que mantengan una estrecha relación con los grandes depositantes, o ellos correrán el riesgo de perder sus fondos en tiempos críticos.

16. Los clientes frecuentemente tienen cuentas múltiples con el mismo banco, pero en oficinas situadas en diferentes países. Para manejar efectivamente el riesgo sobre la reputación, el riesgo de cumplimiento y el legal que surge de dichas cuentas, los bancos deben poder agrupar y monitorear saldos significativos y la actividad en estas cuentas en forma mundial totalmente consolidada, sin considerar si las cuentas se mantienen en el balance, fuera del balance, como activos bajo administración, o en forma fiduciaria.

17. Tanto el Comité de Basilea como el Grupo Internacional de Supervisores Bancarios están totalmente convencidos de que las prácticas efectivas de KYC deben ser parte del manejo de riesgo y los sistemas de control interno en todos los bancos del mundo. Los supervisores nacionales son responsables de asegurar que los bancos tengan standards mínimos y controles internos que les permitan conocer adecuadamente a sus clientes. Los códigos voluntarios de conducta emitidos por las organizaciones o asociaciones de la industria pueden ser de considerable valor para apuntalar una guía regulatoria, dando asesoramiento práctico a los bancos sobre asuntos operativos. Sin embargo, dichos códigos no pueden ser considerados como un substituto de una guía regulatoria formal.

III. Elementos esenciales de las normas KYC

18. La guía del Comité de Basilea sobre las KYC ha sido contenida en los siguientes tres documentos y ellos reflejan la evolución del pensamiento de supervisión a través del tiempo. La Prevención del Uso Delictivo del Sistema Bancario con el Propósito de Lavado de Dinero emitido en 1988 estipula los principios éticos básicos e impulsa a los bancos a instalar procedimientos efectivos para identificar a los clientes, declinar transacciones sospechosas y cooperar con las agencias de aplicación de la ley. Los Principios Centrales para la Efectiva Supervisión Bancaria de 1997 dice, en una discusión más amplia de los controles internos, que los bancos deben tener instalados políticas, prácticas y procedimientos adecuados, incluyendo estrictas normas de "conozca-a-su-cliente"; específicamente, los supervisores deben impulsar la adopción de las recomendaciones pertinentes de la FATF. Estas se refieren a la identificación y el mantenimiento del registro de clientes, una mayor diligencia por parte de las instituciones financieras en la detección y el reporte de transacciones sospechosas, y las medidas para operar con países con medidas inadecuadas contra el lavado de dinero. La Metodología de Principios Centrales de 1999 elabora además los Principios Centrales detallando un número de criterios esenciales y adicionales. (Anexo 1 detalla los extractos pertinentes de los Principios Centrales y la Metodología).

19. Debe requerirse a todos los bancos que "tengan instalados políticas, prácticas y procedimientos adecuados que promuevan altos standards éticos y profesionales y que eviten que el banco sea utilizado, intencionalmente o no, por elementos delictivos. Ciertos elementos clave deben ser incluidos por los bancos en el diseño de los programas KYC. Dichos elementos esenciales deben comenzar con el manejo del riesgo y los procedimientos de control de los bancos y deben incluir (1) política de aceptación del cliente, (2) identificación del cliente, (3) monitoreo continuo de cuentas de alto riesgo y (4) manejo del riesgo. Los bancos no sólo deben establecer la identidad de sus clientes sino que también deben monitorear la actividad de las cuentas para determinar aquéllas transacciones que no están conformes a las transacciones normales o esperadas para ese cliente o tipo de cuenta. Las KYC deben ser una característica central del manejo del riesgo y los procedimientos de control de los bancos, y deben ser complementadas por revisiones de cumplimiento regulares y por auditoría interna. La intensidad de los programas de KYC más allá de estos elementos esenciales debe ser diseñada según el grado de riesgo.

1. Política de aceptación del cliente

20. Los bancos deben desarrollar políticas y procedimientos claros de aceptación del cliente, incluyendo una descripción de los tipos de clientes que tienen probabilidades de plantear a un banco un riesgo más alto que el promedio. Al preparar dichas políticas, deben considerarse factores tales como los antecedentes de los clientes, el país de origen, la posición pública o de alto perfil, las cuentas relacionadas, las actividades comerciales u otros indicadores de riesgo. Los bancos deben desarrollar políticas y procedimientos graduales de aceptación del cliente que requieran una diligencia debida más amplia para los clientes de riesgo más alto. Por ejemplo, las políticas pueden exigir la mayoría de los requisitos básicos para la apertura de cuentas para un individuo que trabaja con un pequeño saldo en la cuenta. Es importante que la política de aceptación del cliente no sea tan restrictiva que resulte en una denegación del

acceso a servicios bancarios para el público en general, especialmente para la gente que está financiera o socialmente en desventaja. Por otro lado, una diligencia debida bastante extensa sería esencial para un individuo con un alto patrimonio neto cuya fuente de fondos no es clara. Las decisiones de entrar en relaciones comerciales con clientes de más alto riesgo, tales como las personas expuestas públicamente (ver sección 2.2.3 debajo), deben ser exclusivamente a nivel gerencial senior.

2. Identificación del cliente

21. La identificación del cliente es un elemento esencial de las normas KYC. A los fines de este documento, un cliente incluye :

* la persona o entidad que mantiene una cuenta con el banco o aquéllos a nombre de quienes se mantiene una cuenta (es decir, sus propietarios beneficiarios);

* los beneficiarios de transacciones conducidas por intermediarios profesionales; y

* cualquier persona o entidad conectada con una transacción financiera que pueda plantear al banco un riesgo sobre la reputación o de otra índole.

22. Los bancos deben establecer un procedimiento sistemático para identificar nuevos clientes y no debe establecer una relación bancaria hasta que la identidad del nuevo cliente no sea verificada satisfactoriamente.

23. Los bancos deben "documentar y aplicar políticas para la identificación de los clientes y de aquéllos que actúan en su nombre". Los mejores documentos para verificar la identidad de los clientes son aquéllos más difíciles de obtener ilícitamente y de falsificar. Se debe ejercer especial atención en el caso de clientes no residentes y en ningún caso debe un banco acortar los procedimientos de identidad sólo porque el nuevo cliente no puede presentarse para la entrevista. El banco debe preguntarse siempre porqué el cliente ha elegido abrir una cuenta en una jurisdicción extranjera.

24. El proceso de identificación del cliente se aplica naturalmente al iniciarse la relación. Para asegurarse de que los registros permanezcan actualizados y vigentes, hay una necesidad para los bancos de realizar revisiones regulares de los registros existentes. Un momento apropiado para hacerlo es cuando una transacción de significación tiene lugar, cuando los standards de documentación del cliente cambian substancialmente, o cuando hay un cambio importante en la forma en que es operada la cuenta. Sin embargo, si un banco se da cuenta en algún momento de que le falta información suficiente sobre un cliente existente, debe dar pasos para asegurarse de que toda la información pertinente se obtenga lo más rápidamente posible.

25. Los bancos que ofrecen servicios bancarios privados están particularmente expuestos a riesgo sobre su reputación, y deben, por lo tanto, aplicar diligencia debida mayor a tales operaciones. Las cuentas bancarias privadas, que por naturaleza involucran una gran medida de confidencialidad, pueden abrirse a nombre de un individuo, un negocio comercial, un fideicomiso, un intermediario o una compañía de inversión personalizada. En cada caso puede surgir riesgo sobre la reputación si el banco no sigue diligentemente los procedimientos KYC establecidos. Todos los nuevos clientes y las nuevas cuentas deben ser aprobadas al menos por una persona, de antigüedad apropiada, diferente del gerente de relaciones de bancaria privada. Si se instalan salvaguardas particulares internamente para proteger la confidencialidad de los clientes de banca privada y de sus negocios, los bancos deben aún asegurarse de que se puede conducir un escrutinio y monitoreo al menos equivalente de estos clientes y de sus negocios, por ejemplo, ellos deben estar abiertos para revisación por parte de los funcionarios de cumplimiento y los auditores.

26. Los bancos deben desarrollar "normas claras sobre qué registros deben mantenerse sobre la identificación del cliente y las transacciones individuales y su período de retención". Tal práctica es esencial para permitir a un banco monitorear su relación con el cliente, entender los negocios en curso del cliente y, si fuera necesario, suministrar evidencia en el caso de disputas, de acción legal, o de una investigación financiera que pudiera llevar a condena penal. Como punto inicial y continuación natural del proceso de identificación, los bancos deben obtener los papeles de identificación del cliente y retener las copias de los mismos al menos por cinco años luego del cierre de la cuenta. Ellos deben también retener todos los registros de las operaciones financieras al menos por cinco años después de que la operación haya tenido lugar.

2.1 Requisitos generales de identificación

27. Los Bancos necesitan obtener toda la información necesaria para establecer a su entera satisfacción la identidad de cada cliente nuevo y el propósito y la pretendida naturaleza de la relación comercial. La extensión y la naturaleza de la

información depende del tipo de solicitante (personal, corporativo, etc.) y el volumen esperado de la cuenta. Se impulsa a los supervisores nacionales a suministrar una guía para asistir a los bancos en el diseño de sus propios procedimientos de identificación. El Grupo de Trabajo pretende desarrollar los elementos esenciales de los requisitos de identificación del cliente.

28. Cuando una cuenta ha sido abierta, pero surgen problemas de verificación en la relación bancaria que no pueden ser resueltos, el banco debe cerrar la cuenta y devolver los dineros a la fuente de donde fueron recibidos.

29. Mientras que la transferencia de un saldo de apertura de una cuenta a nombre del cliente en otro banco sujeta a la misma norma KYC puede suministrar algún confort, los bancos deben considerar, sin embargo, la posibilidad de que el anterior gerente de cuentas pueda haber solicitado la remoción de la cuenta debido a la preocupación acerca de actividades dudosas. Naturalmente, los clientes tienen el derecho de mover sus negocios de un banco a otro. Sin embargo, si un banco tiene algún motivo para creer que se le está negando a un solicitante facilidades bancarias por parte de otro banco, debe aplicar procedimientos de mayor diligencia hacia el cliente.

30. Los bancos no deben nunca acceder a abrir una cuenta o conducir negocios en curso con un cliente que insiste en el anonimato o que da un nombre ficticio. Ni tampoco deben las cuentas numeradas confidenciales funcionar como cuentas anónimas sino que las mismas deben estar sujetas exactamente a los mismos procedimientos de KYC que todas las demás cuentas de los clientes, aún si la verificación se lleva a cabo por parte de personal seleccionado. Mientras que una cuenta numerada puede ofrecer protección adicional para la identidad del tenedor de la cuenta, la identidad debe ser conocida para un número suficiente de personal para operar la diligencia debida apropiada. Dichas cuentas no deben, en ninguna circunstancia, ser utilizadas para ocultar la identidad del cliente del funcionario de cumplimiento de un banco o de los supervisores.

2.2. Temas de identificación específicos

31. Existe un número de temas más detallados relativos a la identificación del cliente que necesitan comentarse. Varios de éstos están actualmente bajo consideración por parte de la FATF como parte de una revisión general de sus 40 recomendaciones, y el Grupo de Trabajo reconoce la necesidad de ser coincidente con la FATF.

2.2.1 Cuentas en fideicomiso, nominales y fiduciarias

32. Las cuentas en fideicomiso, nominales y fiduciarias pueden usarse para evadir los procedimientos de identificación. Mientras que puede ser legítimo bajo ciertas circunstancias suministrar una cobertura extra de seguridad para proteger la confidencialidad de clientes bancarios privados legítimos, es esencial que la verdadera relación esté entendida. Los bancos deben establecer si el cliente está tomando el nombre de otro cliente, si está actuando como una "fachada" o si está actuando en nombre de otra persona como fideicomisario, apoderado u otro intermediario. Si es así, una necesaria precondición es el recibo de evidencia satisfactoria de la identidad de cualquier intermediario/s y de las personas a cuyo nombre ellos están actuando, como así también los detalles de la naturaleza del fideicomiso o de otros arreglos fijados. Especialmente, la identificación de un fideicomiso debe incluir los fideicomisarios, pagadores/otorgantes y los beneficiarios.

2.2.2 Vehículos corporativos

33. Los Bancos necesitan estar vigilantes para evitar que las entidades de negocios corporativos sean utilizadas por personas físicas como un método para operar cuentas anónimas. Los vehículos de tenencia de activos personales, tales como las compañías de negocios internacionales, pueden dificultar la adecuada identificación de clientes o propietarios beneficiarios. Un banco debe entender la estructura de la compañía, determinar la fuente de los fondos, e identificar la identidad de los propietarios beneficiarios y de aquéllos que tienen control sobre los fondos.

34. Se necesita ejercer especial cuidado al iniciar transacciones comerciales con compañías que tienen accionistas nominados o acciones al portador. Se necesita obtener evidencia satisfactoria de la identidad de los propietarios beneficiarios de todas esas compañías. En el caso de entidades que tienen una proporción significativa de capital en forma de acciones al portador, se requiere vigilancia extra. Un banco puede ignorar completamente que las acciones al portador han cambiado de manos. Es responsabilidad de los bancos establecer procedimientos satisfactorios para monitorear la identidad de los propietarios beneficiarios importantes. Esto puede requerir que el banco inmovilice las acciones, por ej. reteniendo en custodia las acciones al portador.

2.2.3 Negocios presentados

35. La realización de procedimientos de identificación puede insumir tiempo y existe un deseo natural a limitar

cualquier inconveniente para los nuevos clientes. En algunos países, por lo tanto, se ha vuelto habitual para los bancos el confiar en los procedimientos emprendidos por otros bancos o presentadores cuando un negocio es transferido. Al hacerlo, los bancos se arriesgan a poner excesiva confianza en los procedimientos de diligencia debida que ellos esperan que los presentadores hayan realizado. Confiar en la diligencia debida conducida por un presentador, por

más reputación que tenga, no quita, de ninguna manera, la responsabilidad última del banco receptor de conocer a sus clientes y sus negocios. En particular, los bancos no deben confiar en presentadores que estén sujetos a normas más débiles que las que rigen los propios procedimientos KYC de los bancos o que sean renuentes a compartir copias de la documentación de diligencia debida.

36. El Comité de Basilea recomienda que los bancos que utilizan presentadores deben evaluar cuidadosamente si los presentadores son "correctos y adecuados" y están ejerciendo la necesaria diligencia debida de acuerdo con las normas fijadas en este documento. La responsabilidad última de conocer a los clientes siempre recae en el banco. Los bancos deben usar los siguientes criterios para determinar si se puede confiar en un presentador :

* debe cumplir con las prácticas mínimas de diligencia debida identificadas en este documento con relación al cliente.

* los procedimientos de diligencia debida del presentador con relación al cliente deben ser tan rigurosos como aquéllos que el banco mismo habría llevado adelante para con el cliente.

* el banco mismo debe estar satisfecho en cuando a la confiabilidad de los sistemas instalados por el presentador para verificar la identidad del cliente.

* el banco debe llegar a un acuerdo con el presentador de que se permitirá verificar la diligencia debida realizada por el presentador en cualquier etapa; y

* todos los datos de identificación pertinentes y demás documentación correspondiente a la identidad del cliente debe ser presentada inmediatamente por el presentador al banco, quien debe revisar cuidadosamente la documentación suministrada. Dicha información debe estar disponible para revisación por parte del supervisor y la unidad de inteligencia financiera o agencia de aplicación equivalente, cuando se haya obtenido la apropiada autorización legal.

Además, los bancos deben llevar adelante revisiones periódicas para asegurarse de que un presentador en el cual confía cumpla con los criterios fijados precedentemente.

2.2.4 Cuentas de clientes abiertas por intermediarios profesionales.

37. Cuando un banco tiene conocimiento o motivo para creer que una cuenta de cliente abierta or un intermediario profesional es a nombre de un sólo cliente, ese cliente debe ser identificado.

38. Los bancos a menudo mantienen cuentas "conjuntas" manejadas por intermediarios profesionales a nombre de entidades tales como fondos mutuales, fondos de pensión y fondos monetarios. Los bancos mantienen también cuentas conjuntas manejadas por abogados o agentes de bolsa que representan fondos mantenidos en depósito o en cuentas de garantía para una gama de clientes. Cuando los fondos mantenidos por el intermediario no están mezclados en el banco sino que hay "sub-cuentas" que pueden ser atribuidas a cada propietario beneficiario, todos los propietarios beneficiarios de la cuenta mantenida por el intermediario deben ser identificados.

39. Cuando los fondos están mezclados, el banco debe investigar a los propietarios beneficiarios. Puede haber circunstancias en donde el banco no necesite ir más allá del intermediario, por ejemplo, cuando el intermediario esté sujeto a la misma legislación regulatoria y a los mismos procedimientos sobre lavado de dinero, y en particular, que esté sujeto a las mismas normas que el banco sobre diligencia debida con respecto a su base de clientes. La guía de supervisión nacional debe fijar claramente esas circunstancias en las que el banco no necesita ver más allá del intermediario. Los bancos deben aceptar dichas cuentas sólo a condición de que los mismos puedan establecer que el intermediario ha emprendido un sólido proceso de diligencia debida y que tiene los sistemas y controles para asignar los activos a los respectivos beneficiarios en las cuentas conjuntas. Al evaluar el proceso de diligencia debida del intermediario, el banco debe aplicar los criterios fijados en el párrafo 36 precedente, con respecto a los negocios presentados, con el fin determinar si se puede confiar en un intermediario profesional.

40. Cuando el intermediario no está autorizado a suministrar al banco la información requerida sobre los beneficiarios, por ejemplo, los abogados están obligados por los códigos de secreto profesional o cuando ese intermediario no esté

sujeto a las normas de diligencia debida equivalentes a las estipuladas en este documento o a los requisitos de legislación amplia contra el lavado de dinero, entonces el banco no debe permitir que el intermediario abra una cuenta.

2.2.5 Personas expuestas políticamente

41. Las relaciones comerciales con individuos que tienen cargos públicos importantes y con personas o compañías claramente relacionadas con ellas, pueden exponer al banco a significativos riesgos para su reputación y/o legales. Tales personas expuestas políticamente ("PEPs", por sus siglas en inglés) son individuos a quienes se confían o a quienes se han confiado funciones públicas importantes, incluyendo jefes de estado o de gobierno, políticos senior, funcionarios senior gubernamentales, judiciales o militares, ejecutivos senior de corporaciones de propiedad pública y funcionarios importantes de partidos políticos. Siempre existe la posibilidad, especialmente en los países en donde la corrupción está expandida, que tales personas abusen de sus poderes públicos para su propio enriquecimiento ilícito por medio del recibo de sobornos, peculado, etc.

42. Aceptar y manejar fondos de personas públicas corruptas dañará severamente la propia reputación del banco y puede minar la confianza pública en las normas éticas de todo un centro financiero, dado que usualmente esos casos reciben una amplia atención de los medios y una fuerte reacción política, aún cuando el origen ilícito de los activos sea a menudo difícil de probar. Además, el banco puede estar sujeto a costosos pedidos de información y órdenes de embargo de autoridades de aplicación de la ley o judiciales (incluyendo procedimientos internacionales de asistencia mutua en asuntos delictivos) y puede ser pasible de demandas por daños por parte del estado involucrado o de las víctimas de un régimen. Bajo ciertas circunstancias, el banco y/o sus mismos funcionarios y empleados pueden estar expuestos a cargos por lavado de dinero, si ellos conocen o deberían haber sabido que los fondos derivaron de la corrupción o de otros delitos serios.

43. Algunos países han modificado recientemente o están en proceso de modificar sus leyes y reglamentaciones para penalizar la corrupción activa de empleados civiles y funcionarios públicos extranjeros de conformidad con la pertinente convención internacional. En estas jurisdicciones la corrupción extranjera se vuelve un delito predicado para el lavado de dinero y se aplican todas las leyes y reglamentaciones pertinentes contra el lavado de dinero (por ej. el reporte de operaciones sospechosas, la prohibición de informar al cliente, el congelamiento interno de los fondos, etc.). Pero aún en ausencia de tales bases legales explícitas en la ley penal, es claramente indeseable, falto de ética e incompatible con la correcta y adecuada conducción de operaciones bancarias el aceptar o mantener una relación comercial si el banco conoce o debe presumir que los fondos derivan de la corrupción o el uso indebido de fondos públicos. Hay una necesidad acuciante para un banco que está considerando una relación con una persona y sospecha que es una persona pública, de identificar completamente a esa persona, como así también a la gente y las empresas que están claramente relacionadas con él/ella.

44. Los bancos deben reunir suficiente información de un cliente nuevo, y verificar la información disponible públicamente, con el fin de establecer si el cliente es o no una persona pública. Los bancos deben investigar la fuente de los fondos antes de aceptar una persona pública. La decisión de abrir una cuenta para una persona pública debe ser tomada a un nivel gerencial senior.

2.2.6 Clientes que no se presentan personalmente (cara a cara).

45. De manera creciente se solicita a los bancos la apertura de cuentas en nombre de clientes que no se presentan ellos mismos para la entrevista personal. Esto ha sido siempre un evento frecuente en el caso de clientes no residentes, pero se ha incrementado significativamente con la reciente expansión de la banca postal, telefónica y electrónica. Los bancos deben aplicar procedimientos de identificación de clientes igualmente efectivos y normas de monitoreo constantes para los clientes que no se presentan personalmente (cara a cara) así como para aquéllos que estén disponibles para la entrevista. Un tema que ha surgido en conexión con esto es la posibilidad de verificación independiente por parte de un tercero con reputación. Todo este tema de la identificación del cliente que no se presenta cara a cara está siendo discutido por la FATF, y está también bajo revisión en el contexto de la modificación de la Directiva de la EEC de 1991.

46. Un ejemplo típico de cliente que no se presenta personalmente (cara a cara) es uno que desea llevar banca electrónica via Internet o tecnología similar. La banca electrónica incorpora actualmente una amplia gama de productos y servicios prestados por medio de las redes de telecomunicaciones. La naturaleza impersonal y sin fronteras de la banca electrónica combinada con la velocidad de la transacción inevitablemente crea dificultad en la identificación y verificación del cliente. Como una política básica, los supervisores esperan que los bancos evalúen pro activamente los distintos riesgos planteados por las tecnologías emergentes y diseñen procedimientos de identificación de los clientes con la debida consideración de tales riesgos.

47. Si bien la misma documentación puede ser suministrada por los clientes que se presentan cara a cara y los que no lo hacen, existe una dificultad mayor para hacer coincidir el cliente con la documentación en el caso de los clientes que no se presentan personalmente (cara a cara). Con la banca telefónica y electrónica, el problema de verificación se hace aún más difícil.

48. Al aceptar negocios de clientes que no se presentan personalmente (cara a cara) :

* los bancos deben aplicar procedimientos de identificación de clientes igualmente efectivos para los clientes que no se presentan personalmente (cara a cara) que para los que están disponibles para la entrevista; y

* debe haber medidas específicas y adecuadas para mitigar el riesgo mayor.

Los ejemplos de medidas para mitigar el riesgo incluyen :

* certificación de los documentos presentados;

* pedido de documentos adicionales para complementar los que se requieren para los clientes que se presentan personalmente (cara a cara);

* contacto independiente con el cliente por parte del banco;

* presentación de un tercero: por ejemplo un presentador sujeto a los criterios establecidos en el párrafo 36; o

* requerimiento de que el primer pago se lleve a cabo por medio de una cuenta a nombre del cliente con oto banco sujeto a normas similares de diligencia debida del cliente.

2.2.7 La corresponsalía bancaria

49. La corresponsalía bancaria es la provisión de servicios bancarios por parte de un banco (el "banco corresponsal") a otro banco (el "banco respondiente"). Utilizadas por los bancos en todo el mundo, las cuentas de corresponsalía posibilitan a los bancos llevar adelante negocios y suministrar servicios que los bancos no ofrecen directamente. Las cuentas de corresponsalía que merecen particular cuidado incluyen la provisión de servicios en jurisdicciones en donde los bancos respondientes no tienen presencia física. Sin embargo, si los bancos omiten aplicar a esas cuentas un nivel apropiado de diligencia debida, ellos se exponen a la serie de riesgos identificados anteriormente en este documento, y pueden encontrarse manteniendo y/o transfiriendo dinero ligado a la corrupción, el fraude u otra actividad ilegal.

50. Los bancos deben reunir suficiente información acerca de sus bancos respondientes para entender completamente la naturaleza de los negocios del respondiente. Los factores a considerar incluyen: información acerca del gerenciamiento del banco respondiente, las principales actividades comerciales, dónde están situados y sus esfuerzos para la prevención y detección del lavado de dinero; la identidad de cualquier tercera entidad que utilizará los servicios de corresponsalía bancaria; y la condición de reglamentación y supervisión bancaria en el país del respondiente. Los bancos deben establecer relaciones de corresponsalía sólo con bancos extranjeros que estén supervisados de manera efectiva por las autoridades pertinentes. Por su parte, los bancos respondientes deben tener políticas efectivas de KYC y de aceptación de clientes.

51. En particular, los bancos deben rehusarse a iniciar o continuar una relación de corresponsalía bancaria con un banco registrado en una jurisdicción en la cual no tiene ninguna presencia física y que no está afiliado a un grupo financiero regulado (es decir bancos "cáscara"). Los bancos deben prestar particular atención cuando continúan relaciones con bancos respondientes situados en jurisdicciones que tienen normas pobres de KYC o que han sido identificados como "no cooperativos" en la lucha contra el lavado de dinero. Los bancos deben establecer que sus bancos respondientes tienen normas de diligencia debida según las estipuladas en este documento, y emplear procedimientos mejorados de diligencia debida con respecto a transacciones llevadas a cabo a través de cuentas de corresponsales.

52. Los bancos deben estar particularmente alertas al riesgo de que las cuentas de corresponsales puedan ser usadas por terceros para operar negocios en su propio nombre (por ej., cuentas pagaderas a través de ellos). Tales arreglos dan origen a la mayoría de las mismas consideraciones aplicables a los negocios presentados y deben ser tratados de acuerdo con el criterio indicado en el párrafo 36.

3. Monitoreo constante de cuentas y transacciones

53. El monitoreo constante es un aspecto esencial de los procedimientos efectivos de KYC. Los bancos sólo pueden controlar efectivamente y reducir el riesgo si ellos tienen una comprensión de la actividad normal y razonable de la cuenta de sus clientes de modo que tengan un medio de indentificar las transacciones con caigan fuera del patrón usual de actividad de una cuenta. Sin tal conocimiento, ellos probablemente no cumplan con su deber de reportar las operaciones sospechosas a las autoridades apropiadas en los casos en que se les requiera hacerlo. El nivel del monitoreo debe ser sensible al riesgo. Para todas las cuentas, los bancos deben tener sistemas instalados para detectar patrones de actividad inusuales o sospechosos. Esto puede hacerse estableciendo límites para una clase o categoría particular de cuentas. Se debe prestar particular atención a las transacciones que excedan estos límites. Ciertos tipos de transacciones deben alertar a los bancos sobre la posibilidad de que el cliente esté llevando adelante actividades inusuales o sospechosas. Las mismas pueden incluir transacciones que no parecen tener sentido económico o comercial, o que involucran grandes importes de depósitos en efectivo que no son coincidentes con las transacciones normales y esperadas del cliente. Un rendimiento muy alto de la cuenta, no coincidente con el volumen del saldo, puede indicar que se están "lavando" fondos a través de la cuenta. Los ejemplos de actividades sospechosas pueden ser muy útiles para los bancos y deben ser incluidos como parte de los procedimientos y/o guía contra el lavado de dinero de una jurisdicción.

54. Debe haber un monitoreo intensificado para las cuentas de más alto riesgo. Cada banco debe fijar indicadores clave para tales cuentas, tomando nota de los antecedentes del cliente, tales como el país de origen y la fuente de los fondos, el tipo de operaciones involucradas, y otros factores de riesgo. Para las cuentas de riesgo más alto :

* Los bancos deben asegurarse de que ellos tienen sistemas informáticos gerenciales adecuados para suministrar a los gerentes y a los funcionarios de cumplimiento la información oportuna que se necesite para identificar, analizar y monitorear efectivamente las cuentas de clientes de más alto riesgo. Los tipos de informes que pueden necesitarse incluyen informes de documentación faltante para la apertura de la cuenta, transacciones efectuadas a través de una cuenta de cliente que sean inusuales, y la agrupación de la totalidad de la relación del cliente con el banco.

* La gerencia senior encargada de los negocios de banca privada deben conocer la circunstancias personales de los clientes de más alto riesgo del banco y deben estar alerta a las fuentes de información de terceros. Las transacciones significativas por parte de estos clientes deben ser aprobadas por un gerente senior.

Los bancos deben desarrollar una política clara y guías, procedimientos y controles internos y deben permanecer especialmente atentos con respecto a las relaciones comerciales con las personas públicas y los individuos de alto perfil o con personas y compañías que están claramente relacionadas o asociadas con ellos. Dado que no todas las personas públicas pueden ser identificadas inicialmente y dado que los clientes existentes pueden adquirir estado público posteriormente, se deben emprender revisiones regulares al menos de los clientes más importantes.

4. Manejo del riesgo

55. Los procedimientos efectivos de KYC incluyen rutinas para la adecuada vigilancia gerencial, los sistemas y controles, la separación de deberes, entrenamiento y otras políticas relacionadas. El directorio del banco debe estar totalmente comprometido con un efectivo programa de KYC estableciendo los procedimientos apropiados y asegurando su efectividad. Se debe asignar responsabilidad explícita dentro del banco para asegurar que las políticas y procedimientos del banco sean manejados con efectividad y que estén, como mínimo, de acuerdo con la práctica de supervisión local. Los canales para informar las transacciones sospechosas deben estar claramente especificados por escrito, y deben ser comunicados a todo el personal. Debe haber también procedimientos internos para evaluar si las obligaciones estatutarias del banco bajo los regímenes reconocidos de información sobre actividades sospechosas requieren que la transacción sea reportada a las autoridades apropiadas de aplicación de la ley y/o de supervisión.

56. Los funcionarios de auditoría interna y de cumplimiento tienen responsabilidades importantes en la evaluación y en asegurarse del cumplimiento de las políticas y procedimientos de KYC. Como regla general, los funcionarios de cumplimiento deben suministrar una evaluación independiente de las propias políticas y procedimientos del banco, incluyendo los requisitos legales y regulatorios. Sus responsabilidades deben incluir monitoreo constante del rendimiento del personal a través de pruebas de muestreo de cumplimiento y revisión de informes de excepción para alertar a la gerencia senior o al Directorio si cree que la gerencia está omitiendo dirigir los procedimientos de KYC de manera responsable.

57. La auditoría interna juega un papel importante en la evaluación independiente del manejo del riesgo y de los controles, descargando su responsabilidad al Comité de Auditoría del Directorio u órgano de supervisión similar a través de evaluaciones periódicas de la efectividad del cumplimiento de la políticas y procedimientos de KYC, incluyendo el correspondiente entrenamiento del personal. La gerencia debe asegurarse de que los funcionarios de auditoría estén provistos de personal adecuado con individuos que sean bien versados en tales políticas y

procedimientos. Además, los auditores internos deben ser pro activos en el seguimiento de sus descubrimientos y críticas.

58. Todos los bancos deben tener un programa constante de entrenamiento de empleados de modo que el personal del banco esté adecuadamente entrenado en los procedimientos de KYC. El tiempo y el contenido del entrenamiento para los distintos sectores del personal necesitará ser adaptado por el banco a sus propias necesidades. Los requerimientos de entrenamiento deben tener un enfoque diferente para el personal nuevo, el personal de línea frontal, el personal de cumplimiento o el personal que trata con los nuevos clientes. El personal nuevo debe ser instruido en la importancia de las políticas de KYC y los requerimientos básicos en el banco. Los miembros del personal de línea frontal que tratan directamente con el público deben ser entrenados para verificar la identidad de los nuevos clientes, para ejercer la diligencia debida en el manejo de las cuentas de los clientes existentes en forma constante y para detectar patrones de actividad sospechosa. Se debe suministrar entrenamiento regular de recordatorio para asegurarse de que se recuerde al personal sus responsabilidades y que se mantenga informado de los nuevos cambios. Es crucial que todo el personal pertinente comprenda totalmente la necesidad de políticas de KYC e implemente las implemente en consecuencia. Una cultura dentro de los bancos que promueva tal comprensión es la clave para la implementación exitosa.

59. En muchos países, los auditores externos tienen también un papel importante que cumplir en el monitoreo de los controles y procedimientos internos de los bancos, y en la confirmación de que los mismos estén en cumplimiento de la práctica de supervisión.

IV. El papel de los supervisores

60. En base a las normas internacionales de KYC existentes, se espera que los supervisores nacionales fijen la práctica de supervisión que rija los programas de KYC de los bancos. Los elementos esenciales, según se presentan en este documento, deben suministrar una guía clara para que los supervisores procedan con el trabajo de diseñar o mejorar la práctica de supervisión nacional.

61. Además de fijar los elementos básicos para que sigan los bancos, los supervisores tienen la responsabilidad de monitorear que los bancos estén aplicando procedimientos sólidos de KYC y que estén sosteniendo normas éticas y profesionales en forma continua. Los supervisores deben asegurarse de que se establezcan controles internos adecuados y que los bancos estén cumpliendo con la guía de supervisión y la regulatoria. El proceso de supervisión debe incluir no sólo una revisión de las políticas y procedimientos sino también una revisión de los archivos de los clientes y el muestreo de algunas cuentas. Los supervisores deben tener siempre el derecho a acceso a toda la documentación relativa a las cuentas mantenidas en esa jurisdicción, incluyendo cualquier análisis que el banco haya hecho para detectar operaciones inusuales o sospechosas.

62. Los supervisores tienen el deber no sólo de asegurarse de que sus bancos mantengan altos standards de KYC para proteger su propia seguridad y solidez, sino también para proteger la integridad de su sistema bancario nacional. Los supervisores deben aclarar que ellos tomarán la medida apropiada, la cual puede ser severa y pública, si las circunstancias lo justifican, contra los bancos y sus funcionarios que, en forma demostrable omitieren seguir sus propios procedimientos y requisitos internos. Además, los supervisores deben asegurarse de que los bancos estén en conocimiento de las transacciones que involucren jurisdicciones con normas que sean consideradas inadecuadas y de que presten particular atención a las mismas. La FATF y algunas autoridades nacionales han detallado un número de países y jurisdicciones que se considera tienen arreglos legales y administrativos que no cumplen con las normas internacionales para combatir el lavado de dinero. Tales hallazgos deben ser un componente de las políticas y procedimientos de KYC del banco.

V. Implementación de normas de KYC en un contexto extranjero

63. Los supervisores en todo el mundo deben buscar, haciendo el mejor de sus esfuerzos, desarrollar e implementar sus normas nacionales de KYC en línea con las normas internacionales de modo de evitar un potencial arbitraje regulatorio y salvaguardar la integridad de los sistemas bancos nacionales e internacionales. La implementación y evaluación de tales normas ponen a prueba la voluntad de los supervisores de cooperar entre ellos en una forma práctica, como así también la habilidad de los bancos para controlar los riesgos en todo el grupo. Es ésta una tarea de desafío para los bancos y los supervisores por igual.

64. Los supervisores esperan que los grupos bancarios apliquen una norma mínima aceptada de políticas y procedimientos de KYC tanto para sus operaciones locales como para las internacionales. La supervisión de la banca internacional sólo puede ser llevada a cabo efectivamente en forma consolidada, y el riesgo sobre la reputación como así también otros riesgos bancarios no están limitados a las fronteras nacionales. Los bancos matrices deben comunicar sus políticas y procedimientos a sus sucursales y subsidiarias en el exterior, incluyendo las entidades no bancarias tales como compañías fiduciaras, y tener una rutina para verificar el cumplimiento en comparación con normas de KYC tanto

internas como del país anfitrión con el fin de que sus programas operen efectivamente en forma global. Tales pruebas de cumplimiento serán también efectuadas por auditores y supervisores externos. Por lo tanto, es importante que la documentación de KYC esté apropiadamente archivada y disponible para su inspección. En lo que concierne a las verificaciones de cumplimiento, los supervisores y auditores externos deben, en la mayoría de los casos, examinar los sistemas y controles y mirar las cuentas del cliente y el monitoreo de las transacciones como parte del proceso de muestreo.

65. Por más pequeño que sea un establecimiento en el exterior, se debe asignar un funcionario senior para que sea directamente responsable de asegurarse de que todo el personal pertinente esté entrenado y observe que los procedimientos de KYC cumplan las normas tanto internas como del país anfitrión. Mientras que este funcionario llevará la responsabilidad primaria, él debe ser apoyado por auditores internos y funcionarios de cumplimiento tanto en las oficinas locales como en la casa matriz, según corresponda.

66. Cuando las normas mínimas de KYC en el país de origen y en el país anfitrión difieren, las sucursales y subsidiarias en las jurisdicciones anfitrionas deben aplicar la norma más alta de las dos. En general, no debiera haber ningún impedimento que evite que un banco adopte normas que son más altas que la mínima requerida localmente. Sin embargo, si las leyes y reglamentaciones locales (especialmente las disposiciones de secreto) prohiben la implementación de las normas de KYC del país de origen, cuando estas últimas sean más restrictivas, los supervisores del país anfitrión deben usar sus mejores esfuerzos para hacer que la ley y las reglamentaciones cambien. Mientras tanto, las sucursales y subsidiarias en el exterior tendrían que cumplir con las normas del país anfitrión, pero ellos deben asegurarse de que la casa central o banco matriz y su supervisor en el país de origen estén totalmente informados de la naturaleza de la diferencia.

67. Los elementos delictivos probablemente se llevarán hacia jurisdicciones con tales impedimentos. De allí que los bancos deberían ser conscientes del alto riesgo para su reputación de llevar adelante negocios en estas jurisdicciones. Los bancos matrices deben tener un procedimiento para revisar la vulnerabilidad de las unidades operativas individuales e implementar salvaguardas adicionales cuando sea apropiado. En casos extremos, los supervisores deben considerar la colocación de controles adicionales sobre los bancos que operan en esas jurisdicciones y en última instancia quizás alentar su retiro.

68. Durante las inspecciones in-situ, los supervisores o auditores del país de origen no deben enfrentar ningún impedimento al verificar el cumplimiento de la unidad con las políticas y procedimientos de KYC. Esto requerirá una revisión de los archivos de clientes y el muestreo de algunas cuentas al azar. Los supervisores del país de origen deben tener acceso a la información sobre las cuentas de clientes individuales del muestreo en la medida necesaria para posibilitar su correcta evaluación de la aplicación de las normas KYC y una evaluación de las prácticas del manejo de riesgo, y no deben ser impedidos por las leyes locales sobre secreto bancario. Cuando el supervisor del país de origen requiera un reporte consolidado de depósitos o concentraciones de prestatarios o la notificación de fondos bajo administración, no debería haber impedimento alguno. Además, con vistas a monitorear las concentraciones de depósitos o el riesgo de fondeo de que el depósito sea retirado, los supervisores pueden aplicar pruebas esenciales y establecer algunos umbrales de modo que si el depósito de un cliente excede un cierto porcentaje del balance, los bancos deban reportarlo al supervisor del país anfitrión. Sin embargo, se necesitan salvaguardas para asegurar que la información concerniente a las cuentas individuales sea utilizada exclusivamente a los fines de supervisión legal, y que pueda estar protegida por el receptor en forma satisfactoria. Una declaración de mutua cooperación para facilitar que se comparta la información entre los dos supervisores sería útil en este aspecto.

69. En ciertos casos, puede haber un serio conflicto entre las políticas de KYC de un banco matriz impuestas por su autoridad local y lo que se permite en la oficina exterior. Puede haber, por ejemplo, leyes que impidan las inspecciones por parte de los funcionarios de cumplimiento de los bancos matrices, los auditores internos o los supervisores del país de origen, o que posibiliten a los clientes locales usar nombres ficticios u ocultar detrás de agentes e intermediarios a quienes se prohibe revelar quiénes son sus clientes. En tales casos, el supervisor del país de origen debe comunicarse con el supervisor anfitrión con el fin de confirmar si existen en verdad impedimentos legales genuinos y si ellos se aplican extra territorialmente. Si ellos prueban ser insuperables, y no hay arreglos de alternativa satisfactoria, el supervisor del país de origen debe aclarar al supervisor anfitrión que el banco puede decidir por sí mismo, o que su supervisor de origen puede requerirle cerrar la operación cuestión. En el análisis final, cualquier arreglo que sustente tales exámenes in-situ debe suministrar un mecanismo que permita una evaluación que sea satisfactoria para el supervisor de origen. Las declaraciones de cooperación o memorandos de entendimiento que fijen los mecanismos de los arreglos pueden ser útiles. El acceso a la información por parte de los supervisores del país de origen deben ser tan irrestrictos como sea posible, y como mínimo, deben tener acceso libre a las políticas y procedimientos generales de los bancos para la diligencia debida del cliente y para tratar las sospechas.

ANEXO 1
Extractos de la Metodología de Principios Centrales

Principio 15 : Los supervisores bancarios deben determinar que los bancos tienen instalados políticas, prácticas y procedimientos adecuados**,** incluyendo estrictas normas de "conozca-a-su-cliente", que promuevan altos standards éticos y profesionales en el sector financiero y prevengan que el banco sea utilizado, intencionalmente o no, por elementos delictivos.

Criterios esenciales

1. El supervisor determina que los bancos tienen instalados políticas, prácticas y procedimientos adecuados que promueven altos standards éticos y profesionales y que previenen que el banco sea utilizado, intencionalmente o no, por elementos delictivos. Esto incluye la prevención y detección de actividad delictiva o fraude, y el reporte de tales actividades sospechadas a las autoridades apropiadas.

2. El supervisor determina que los bancos han documentado y aplicado políticas para la identificación de los clientes y de aquéllos que actúen en su nombre, como parte de su programa contra el lavado de dinero. Existen reglas claras sobre qué registros se deben mantener sobre la identificación de los clientes y las transacciones individuales y el período de retención.

3. El supervisor determina que los bancos tienen procedimientos formales para reconocer transacciones potencialmente sospechosas. Estos podrían incluir una autorización adicional para grandes depósitos o retiros en efectivo (o similar) y procedimientos especiales para transacciones inusuales.

4. El supervisor determina que los bancos designan un funcionarios senior con responsabilidad explícita de asegurarse que las políticas y procedimientos del banco están, como mínimo, de acuerdo con las exigencias estatutarias y regulatorias locales contra el lavado de dinero.

5. El supervisor determina que los bancos tienen procedimientos claros, comunicados a todo el personal, para que el plantel reporte transacciones sospechosas al funcionario senior dedicado responsable por el cumplimiento contra el lavado de dinero.

6. El supervisor determina que los bancos han establecido líneas de comunicación tanto con la gerencia como con un funcionario de seguridad interna (guardia) para reportar los problemas.

7. Además de informar a las autoridades penales apropiadas, los bancos reportan al supervisor las actividades sospechosas y los incidentes de fraude importantes para la seguridad, solidez o reputación del banco.

8. Las leyes, reglamentaciones y/o políticas de los bancos aseguran que un miembro del personal que reporta transacciones sospechosas de buena fe al funcionario senior dedicado, al funcionario de seguridad interna, o directamente a la autoridad pertinente, no puede ser tenido por responsable.

9. El supervisor verifica periódicamente que los controles de lavado de dinero de los bancos y sus sistemas de prevención, identificación y reporte de fraude sean suficientes. El supervisor tiene adecuados poderes de aplicación (procesamiento regulatorio y/o penal) para accionar contra un banco que no cumple con sus obligaciones contra el lavado de dinero.

10. El supervisor puede, directa o indirectamente, compartir con las autoridades locales o extranjeras supervisoras del sector financiero la información relativa a actividades delictivas sospechadas o reales.

11. El supervisor determina que los bancos tienen una declaración de política sobre ética y comportamiento profesional que está claramente comunicada a todo el personal.

Criterios adicionales

1. Las leyes y/o reglamentaciones incluyen prácticas internacionales sólidas tales como el cumplimiento de las cuarenta Recomendaciones de la Fuerza de Tareas de Acción Financiera emitidas en 1990 (revisada en 1996).

2. El supervisor determina que el personal del banco está adecuadamente entrenado sobre la detección y prevención del lavado de dinero.

3. El supervisor tiene la obligación legal de informar a las autoridades penales pertinentes de cualquier transacción sospechosa.

4. El supervisor puede, directa o indirectamente, compartir con las autoridades judiciales pertinentes la información relativa a actividades delictivas sospechadas o reales.

5. Si no lo realiza otra agencia, el supervisor tiene recursos internos con peritos especialistas en fraude financiero y obligaciones contra el lavado de dinero.

ANEXO 2
Extractos de las recomendaciones de la FATF

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

Reglas sobre la Identificación de los Clientes y el mantenimiento de Registros

10. Las instituciones financieras no deben mantener cuentas anónimas o cuentas a nombres obviamente ficticios : se les debe exigir (por ley, por reglamentaciones, por acuerdos entre las autoridades supervisoras y las instituciones financieras o por convenios auto-regulatorios entre las instituciones financieras) que identifiquen sobre la base de un documento oficial u otro documento de identificación confiable, y registren la identidad de sus clientes, ya sean ocasionales o habituales, cuando establezcan relaciones comerciales o lleven adelante operaciones (en particular abriendo cuentas o libros de pases, participando en transacciones fiduciarias, alquilando cajas de seguridad, realizando grandes transacciones en efectivo).

    Con el fin de cumplir con los requisitos de identificación concernientes a las entidades legales, las instituciones financieras deben, cuando sea necesario, tomar medidas :

    (i) verificar la existencia legal y la estructura del cliente obteniendo ya sea de un registro público o bien del cliente, o de ambos, prueba del registro, incluyendo información concerniente al nombre del cliente, su forma legal, la dirección los directores y las disposiciones que regulan la autorización para obligar a la entidad.

    (ii) verificar que cualquier persona que diga actuar en nombre del cliente esté autorizada a ello e identificar a esa persona.

11. Las instituciones financieras deben tomar medidas razonables para obtener información acerca de la verdadera identidad de las personas en cuyo nombre se abre una cuenta o se lleva adelante una transacción si existe alguna duda en cuanto a si estos clientes o personas están actuando en su propio nombre, por ejemplo, en el caso de compañías domiciliarias (es decir, instituciones, compañías, fundaciones, fiduciarias, etc. que no conducen ningún negocio comercial o fabril ni ninguna otra forma de operación comercial en el país donde está situada su oficina registrada).

12. Las instituciones financieras deben mantener, al menos por cinco años, todos los registros necesarios sobre las transacciones, tanto nacionales como internacionales, para posibilitarles cumplir rápidamente con los pedidos de información de las autoridades competentes. Dichos registros deben ser suficientes para permitir la reconstrucción de operaciones individuales (incluyendo los importes y tipos de moneda involucrados, si los hubiere) de modo de proveer, si fuera necesario, evidencia para el procesamiento de comportamiento delictivo.

    Las instituciones deben mantener registros sobre la identificación de los clientes (por ej. copias o registros de documentos de identificación oficiales como pasaportes, carnets de identidad, permisos de conducir o documentos similares), archivos de cuentas y correspondencia comercial al menos por cinco años luego de cerrada la cuenta.

    Estos documentos deben estar disponibles para las autoridades locales competentes en el contexto de los procesamientos e investigaciones delictivas pertinentes.

13. Los países deben prestar especial atención a las amenazas de lavado de dinero inherentes en las tecnologías nuevas o en desarrollo que podrían favorecer el anonimato, y tomar medidas, si se necesitaran, para prevenir su uso en planes de lavado de dinero.

Incremento de Diligencia de las Instituciones Financieras

14. Las instituciones financieras deben prestar especial atención a todas las grandes transacciones complejas e inusuales, y a todos los patrones inusuales de transacciones, que no tienen ningún propósito económico o legal visible aparente. Los antecedentes y el propósito de tales transacciones deben ser examinados, tanto como sea posible, los hallazgos deben ser establecidos por escrito, y estar disponibles para ayudar a los supervisores, auditores y agencias de aplicación de la ley.

15. Si las instituciones financieras sospechan que los fondos derivan de una actividad delictiva, se les debe exigir que reporten con prontitud sus sospechas a las autoridades competentes.

16. Las instituciones financieras, sus directores, funcionarios y empleados deben estar protegidos por las disposiciones legales de la responsabilidad penal o civil, por el incumplimiento de alguna restricción sobre la revelación de información impuesta por contrato o por alguna disposición legislativa, regulatoria o administrativa, si ellos informan sus sospechas de buena fe a las autoridades competentes, aún cuando ellos no supieran exactamente cuál era esa actividad delictiva subyacente.

17. Las instituciones financieras, sus directores, funcionarios y empleados no deben, o, cuando corresponda, no se les debe permitir, advertir a sus clientes cuando la información con relación a ellos está siendo reportada a las autoridades competentes.

18. Las instituciones financieras que informen sus sospechas deben cumplir con las instrucciones de las autoridades competentes.

19. Las instituciones financieras deben desarrollar programas contra el lavado de dinero. Estos programas deben incluir, como mínimo :

(i) el desarrollo de políticas, procedimientos y controles internos, incluyendo la designación de funcionarios de cumplimiento a nivel gerencial, y adecuados procedimientos de selección para asegurar altos standards al contratar empleados.

(ii) un programa constante de entrenamiento de los empleados.

(iii) un funcionario de auditoría para controlar el sistema.