

**Comité de Basilea
sobre Supervisión Bancaria**

Documento de Consulta

**Debida Diligencia de Clientes
para bancos**

Emitido para comentarios para el 31 de marzo de 2001

Enero 2001

BANCO DE PAGOS INTERNACIONALES

Tabla de Contenido

Resumen Ejecutivo

- I. Introducción
 - II. Importancia de los estándares KYC para supervisores y bancos
 - III. Elementos esenciales de los estándares KYC
 - 1. **Política de aceptación de clientes**
 - 2. **Identificación de clientes**
 - 2.1 Requerimientos generales de identificación
 - 2.2 Temas específicos de identificación
 - 2.2.1 Cuentas de fideicomiso, del intermediario y fiduciarias o cuentas de clientes abiertas por intermediarios profesionales.
 - 2.2.2 Negocios de introducción
 - 2.2.3 Riesgo potencial
 - 2.2.4 Clientes indirectos (no cara a cara)
 - 3. Monitoreo recurrente de cuentas de alto riesgo
 - 4. Administración de riesgo
 - IV. El rol de los supervisores
 - V. Implementación de los estándares KYC en un contexto internacional
 - VI. **Proceso de consulta**
- Anexo 1: Requerimientos de identificación general
- Anexo 2: Fragmento de la *Metodología de los Principios Básicos*
- Anexo 3: Fragmento de las recomendaciones FATF

Grupo de Trabajo sobre Banca Internacional

Co-presidentes:

Mr. Charles Freeland, Secretario Delegado General, Comité de Basilea sobre Supervisión Bancaria

Mr. Colin Powell, Presidente, Grupo Offshore de Supervisores Bancarios

Bermuda Monetary Authority	Mr. D. Munro Sutherland
Cayman Islands Monetary Authority	Mr. John Bourbon Mrs. Anna McLean
Commission Bancaire, France	Mr. Laurent Etori
Federal Banking Supervisory Office of Germany	Mr. Jochen Sanio
Guernsey Financial Services Commission	Mr. Peter G. Crook
Banca d'Italia	Mr. Giuseppe Godano
Financial Services Agency, Japan	Mr. Kiyotaka Sasaki
Commission de Surveillance du Secteur Financier, Luxembourg	Mr. Arthur Philippe
Monetary Authority of Singapore	Mrs. Foo-Yap Siew Hong
Swiss Federal Banking Commission	Mr. Daniel Zuberbühler Ms. Dina Balleyguier
Financial Services Authority, United Kingdom	Mr. Richard Chalmers
Board of Governors of the Federal Reserve System	Mr. William Ryback
Federal Reserve Bank of New York	Ms. Nancy Bercovici
Office of the Comptroller of the Currency	Mr. Jose Tuya Ms. Tanya Smith
Secretaría	Mr. Luo Ping

Debida diligencia de clientes para bancos

Resumen Ejecutivo

1. Los supervisores alrededor del mundo están reconociendo más la importancia de asegurar que sus bancos tengan controles y procedimientos adecuados establecidos para que no sean usados para propósitos criminales o fraudulentos. La adecuada debida diligencia en los clientes nuevos y existentes es una parte clave de estos controles. Sin esta debida diligencia, los bancos pueden llegar a estar sujetos a riesgos de reputación, operacional, legal y de concentración que pueden resultar en un costo financiero significativo para los mismos.
2. Sin embargo, como lo reveló la encuesta de 1999, muchos supervisores alrededor del mundo no han desarrollado las prácticas de supervisión básicas y han estado buscando en el Comité de Basilea en la Vigilancia Banca un panorama de los pasos apropiados a tomar. Consiguientemente, el Comité ha desarrollado una serie de recomendaciones que proveen un marco de referencia básico para supervisores y bancos. Los supervisores deben trabajar con sus instituciones supervisadas para asegurar que estas directrices se consideran en el desarrollo de las prácticas conozca a su cliente (KYC, por sus siglas en inglés).
3. Las iniciativas de anti-lavado de dinero tradicionalmente han sido el campo del Grupo de Trabajo de Acción Financiera (FATF, por sus siglas en inglés) y no es intención del Comité duplicar estos esfuerzos. Por el contrario, el interés del Comité es de una perspectiva prudencial más amplia. Las políticas y procedimientos KYC son esenciales en la protección de la seguridad y solidez de los bancos y la integridad de los sistemas bancarios.
4. Las directrices previas del Comité de Basilea sobre debida diligencia de clientes y los esfuerzos de anti-lavado de dinero han sido incluidos en tres documentos. *La prevención de uso criminal del sistema bancario para propósitos de anti-lavado de dinero* fue emitido en 1988 y estipula varios principios básicos, animando a los bancos a identificar a clientes, rechazar transacciones sospechosas y cooperar con las agencias de aplicación de la ley. *Los Principios Básicos de 1997 para una Supervisión Bancaria Efectiva* establecen que, como parte de un ambiente sólido de control interno, los bancos deben tener políticas, prácticas y procedimientos adecuados establecidos que “promuevan estándares éticos y profesionales en el sector financieros y prevengan a la banco de ser usada, intencional o no intencionalmente, por elementos criminales”.¹ Además, se anima a los supervisores a adoptar las recomendaciones relevantes del FATF, con relación a la identificación y tenencia de registros de clientes, reporte de transacciones sospechosas, y medidas para tratar con países con insuficientes o ninguna pauta de anti-lavado de dinero. *La Metodología de los Principios Básicos de 1999* adicionalmente elabora los *Principios Básicos* listando un número de criterios esenciales y adicionales.

¹ Principio 15, Principios Básicos para una Supervisión Bancaria Efectiva.

5. Con base en los estándares KYC internacionales, los supervisores nacionales esperan delinear una práctica de supervisión para regir los programas KYC de los bancos. Los elementos esenciales como se presentan en este documento deben proporcionar una guía clara para que los supervisores procedan con el trabajo del diseño o mejora de la práctica de supervisión nacional.

- (a) Los supervisores nacionales son los responsables de asegurar que los bancos tengan estándares mínimos y controles internos que les permitan conocer en forma adecuada a sus clientes. Los códigos de conducta voluntarios emitidos por las organizaciones o asociaciones de la industria están por fomentarse pero no son suficientes por ellos mismos para asegurar la integridad del mercado o la administración sólida del riesgo. (*parábola 14*)
- (b) El programa KYC de un banco debe incluir políticas y procedimientos para la aceptación del cliente, identificación del cliente, monitoreo continuo de las cuentas de alto riesgo y administración del riesgo. (*parábola 16*)
- (c) Los bancos deben desarrollar políticas y procedimientos claros de aceptación de clientes, incluyendo una descripción de clientes que pueden no estar autorizados a abrir cuentas. Deben de establecerse procedimientos para verificar la identidad de nuevos clientes; los bancos no deben involucrarse dentro de una relación de negocios hasta que la identidad esté establecida satisfactoriamente. (*parábulas 17-19*)
- (d) Un banco también debe llevar a cabo revisiones regulares de su base de clientes para asegurar que comprende la naturaleza de sus cuentas y los riesgos potenciales.
- (e) Los bancos que ofrecen servicios de banca privada son particularmente vulnerables al riesgo de reputación. La operación bancaria privada no debe funcionar autónomamente, o como un “banco dentro de un banco”, pero debe estar sujeto a los procedimientos KYC. Todos los cliente y cuentas nuevas deben estar aprobados por lo menos por una persona además del banquero privado. Si están establecidos resguardos particulares internos para proteger la confidencialidad de los clientes de banca privada y sus negocios, los bancos deben también asegurar que estas cuentas estén sujetas a escrutinio apropiado. (*parábola 21*)
- (f) Los bancos no deben abrir cuentas o realizar negocios con un cliente que insiste en el estado de anonimato o portador o quien da un nombre ficticio. En el caso de cuentas confidenciales numeradas, las identidades de los beneficiarios deben ser conocidas por el personal de cumplimiento, para que el proceso de debida diligencia pueda realizarse en forma satisfactoria. Los bancos también necesitan estar alertar en prevenir a las entidades de negocio corporativas de ser usadas por personas naturales como un método de operación de cuentas anónimas. (*parábulas 24-25*)

- (g) Pueden surgir temas especiales con relación a la identificación del propietario beneficiario en el caso de cuentas de fideicomiso, del intermediario y fiduciarias. Existen también temas sobre la apertura de cuentas de clientes por intermediarios profesionales, y cuando los bancos usan los servicios de introductores. El FATF actualmente está revisando estos temas, y el documento reconoce la necesidad de ser consistente con el FATF. (*parábulas 27-32*).
- (h) Las relaciones de negocio con individuales que mantienen posiciones públicas importantes o con personas o compañías claramente relacionadas a ellos pueden exponer a un banco a riesgos significativos de reputación y/o legales cuando estas personas son corruptas. Dichas personas son conocidas comúnmente como “personalidades”, incluyen jefes de estados, ministros, funcionarios públicos influyentes, jueces y comandantes militares. Las decisiones de involucrarse en relaciones de negocio con personalidades deben ser tomadas a nivel de la alta dirección y los bancos deben particularmente vigilar el monitoreo de dichas cuentas. Es incompatible con la conducta apropiada y adecuada de las operaciones bancarias aceptar o mantener una relación si el banco sabe o asume que los fondos derivados de la corrupción o mal uso de activos públicos. (*parábulas 17, 33 y 34*)
- (i) Las aperturas de cuentas indirecta (no cara a cara) ha incrementado significativamente con el llegada de la banca por correo, telefónica y electrónica. Se les requiere a los bancos aplicar equitativamente los procedimientos efectivos de identificación de clientes y estándares de monitoreo para los clientes indirectos como para aquellos que pueden presentarse por sí mismos para entrevista. (*parábulas 35*)
- (j) El monitoreo continuo de cuentas y transacciones de cuentas de alto riesgo es un elemento esencial de KYC. Los bancos deben obtener y mantener actualizados los documentos de identificación del cliente, y mantenerlos por lo menos por cinco años después de que la cuenta sea cerrada. Deben mantener todos los registros de transacciones financieras de por lo menos cinco años después de que se ha realizado la transacción. Los bancos deben también tener sistemas de información capaces de monitorear las cuentas de cliente y patrones potenciales sospechosos de actividad. (*parábola 37*)
- (k) El consejo de directores de un banco debe cumplir completamente a un programa efectivo KYC, adoptando políticas y procedimientos para la propiedad de la vigilancia, sistemas y controles, segregación de responsabilidades, capacitación y otras políticas relacionadas, incluyendo procedimientos para el reporte de transacciones sospechosas. Las funciones de cumplimiento y auditoría interna deben monitorear el cumplimiento del banco con estas políticas y procedimientos. (*parábulas 38 y 40*).
- (l) Los supervisores deben asegurar que los bancos tengan controles internos apropiados, que estén de conformidad con la directriz de supervisión sobre KYC y tomar la acción para corregir cualesquiera deficiencias identificadas.

Los supervisores también necesitan tomar las acciones apropiadas contra aquellos cuyas prácticas son inadecuadas. (*parábolas 44-45*)

- (m) Todos los supervisores deben esperar que los grupos bancarios apliquen un estándar mínimo aceptable de políticas y procedimientos para sus operaciones locales y extranjeras. Cuando existan impedimentos legales en un país anfitrión para la implementación de estándares KYC más altos de país sede, los supervisores del país anfitrión deben usar sus mejores esfuerzos para tener las leyes y reglamentos cambiados. Mientras tanto, las sucursales y subsidiarias extranjeras deben estar seguras de que la oficina matriz o frontal y su supervisor de país sede estén informados de la situación. Cuando el problema se considera ser suficientemente severo, los supervisores deben considerar establecer controles adicionales sobre los bancos que operan en esas jurisdicciones y finalmente tal vez alentar su retiro. (*parábolas 46-50*)

6. Este documento está siendo emitido para consulta. Se agradecerán los comentarios de supervisores y bancos nacionales antes del 31 de marzo de 2001. Estos serán enviados a la Secretaria del Comité de Basilea sobre Supervisión Bancaria con copias a las autoridades de supervisión nacionales cuando sea apropiado.

I. Introducción

1. En la revisión de los hallazgos de una encuesta interna de banca internacional en 1999, el Comité de Basilea identificó deficiencias en un gran número de políticas conozca a sus clientes (KYC) para bancos. Juzgadas desde una perspectiva de supervisión, las políticas KYC en algunos países tienen vacíos y en otros ni existen. Aún entre los países con mercados financieros bien desarrollados, el alcance de robustez KYC varía. Consiguientemente, el Comité de Basilea solicitó al Grupo de Trabajo sobre Banca Internacional² examinar los procedimientos KYC actualmente establecidos y diseñar estándares recomendados aplicables a los bancos en todos los países. Este documento representa los hallazgos y conclusiones del Grupo de Trabajo. El Comité de Basilea ha endosado el documento y ahora está distribuyéndolo alrededor del mundo con la esperanza de que el marco de referencia KYC presentado aquí llegará a ser la referencia para que los supervisores establezcan prácticas nacionales y para que los bancos diseñen sus propios programas.

2. KYC está asociado más cercanamente con la lucha contra el lavado de dinero, que es esencialmente el campo del Grupo de Trabajo de Acción Financiera (FATF).³ Mientras el Comité de Basilea continúa apoyando fuertemente la adopción e implementación de las recomendaciones FATF, particularmente las relacionadas a los bancos, también mantiene que los procedimientos KYC sólidos deben ser considerados como un elemento crítico en la administración efectiva de los riesgos bancarios. Los resguardos KYC van más allá de la simple apertura y registro de cuentas y requiere que los bancos formulen una política de aceptación de clientes y un programa intenso de identificación de clientes que involucre una debida diligencia más extensiva para cuentas de riesgo más alto, e incluya el monitoreo proactivo de cuentas para actividades sospechosas.

3. El interés del Comité de Basilea en los estándares KYC sólidos se origina de sus preocupaciones para la integridad de mercado y ha sido elevado por pérdidas directas e indirectas incurridas por los bancos debido a su falta de diligencia en la aplicación de procedimientos apropiados. Estas pérdidas podrían probablemente haber sido evitadas y el daño a la reputación de los bancos haberse disminuido significativamente si los bancos hubieran mantenido programas KYC efectivos.

² Este es un grupo conjunto consistente de miembros del Comité de Basilea y el Grupo Offshore de Supervisores Bancarios.

³ El FATF es un cuerpo intergubernamental que desarrolla y promueve políticas, nacional e internacionalmente, para combatir el lavado de dinero. Tienen 29 países miembros y dos organizaciones regionales. Trabaja en cooperación cercana con otros cuerpos internacionales involucrados en esta área como la Oficina de las Naciones Unidas para el Control de las Drogas y la Prevención del Crimen, el Consejo de Europa, el Grupo Asia-Pacífico sobre Lavado de Dinero y el Grupo de Trabajo de Acción Financiera Caribbean.

4. Este documento refuerza los principios establecidos en los documentos anteriores del Comité proveyendo una guía más precisa sobre los elementos esenciales de los estándares KYC y su implementación. En el desarrollo de esta guía, el Grupo de Trabajo ha abarcado prácticas en países miembros y tomado en cuenta los desarrollos evolutivos de supervisión. Los elementos esenciales presentados en este documento son directrices para implementación alrededor del mundo. En muchos casos, estos estándares pueden necesitar ser complementados y/o fortalecidos por medidas adicionales que se adapten a condiciones y riesgos particulares en el sistema bancario de países individuales.

II. Importancia de estándares KYC por supervisores y bancos

5. El FATF y otras agrupaciones internacionales han trabajado intensamente sobre temas KYC, y las Cuarenta Recomendaciones del FATF sobre el combate de lavado de dinero⁴ tienen reconocimiento y aplicación internacional. No es la intención de este documento duplicar ese trabajo.

6. Al mismo tiempo, los procedimientos KYC sólidos tienen particular relevancia a la seguridad y solidez de los bancos, en que:

- ayudan a proteger la reputación de los bancos y la integridad de los sistemas bancarios reduciendo la probabilidad de que los bancos lleguen a ser un vehículo o una víctima de crimen financiero y sufran daños de reputación consecuentes;
- constituyen una parte esencial de la administración de riesgo sólida (por ej., proveyendo la base para identificar, limitar y control las exposiciones de riesgo en los activos y pasivos, incluyendo activos bajo administración).

7. La inadecuación o ausencia de estándares KYC puede sujetar a los bancos a serios riesgos de cliente y contraparte, especialmente **riesgos de reputación, operacional, legal y de concentración**. Vale la pena hacer notar que todos estos riesgos están interrelacionados. Sin embargo, cualquiera de ellos puede resultar en un costo financiero significativo a los bancos (por ej, mediante el retiro de fondos por depositantes, la finalización de servicios interbancarios, reclamos contra el banco, costos de investigación, accesos y congelamientos de activos, y pérdidas por préstamo).

8. El **riesgo de reputación** plantea una mayor amenaza a los bancos, ya que la naturaleza de sus negocios requiere el mantenimiento de la confianza de los depositantes, acreedores y el lugar de mercado general. El riesgo de reputación es definido como el potencial de que la publicidad adversa con respecto a las prácticas de negocio de un banco, ya sean precisas o no, causarían una pérdida de confianza en la integridad de la institución. Los bancos son especialmente vulnerables al riesgo de reputación debido a que pueden fácilmente llegar a ser un vehículo o un víctima de actividades ilegales perpetradas por sus clientes.

⁴ Ver las recomendaciones 10 a la 19 del FATF que se reproducen en Anexo 3.

Necesitan protegerse a sí mismos por medio de una vigilancia continua mediante y programa KYC efectivo.

9. El **riesgo operacional** puede ser definido como el riesgo de pérdidas directas o indirectas resultantes de procesos, personas y sistemas internos inadecuados o fracasados, o de eventos externos. La mayoría del riesgo operacional en el contexto KYC se refiere a debilidades en la implementación de los programas de los bancos, procedimientos de control inefectivos y fallas en practicar la debida diligencia. Una percepción pública de que un banco no sea capaz de manejar su riesgo operacional efectivamente puede interrumpir o adversamente afectar el negocio del banco.

10. El **riesgo legal** es la posibilidad de que los procesos, juicios o contratos adversos que se vuelven no ejecutables puedan interrumpir o afectar en forma adversa las operaciones o condición de un banco. Los bancos pueden llegar a estar sujetos a procesos resultantes de la falla en observar estándares KYC obligatorios o de la falla en prácticas la debida diligencia. Consiguientemente, los bancos pueden, por ejemplo, sufrir multas, responsabilidades criminales y penalidades especiales impuestas por supervisores. De hecho, un caso de corte que involucra un banco puede tener implicaciones de muy gran costo por sus negocios que solamente los costos legales. Los bancos no serán capaces de protegerse a sí mismos efectivamente de dichos riesgos legales si no se comprometen en una debida diligencia en la identificación de sus clientes y comprensión de sus negocios.

11. La preocupación del supervisor sobre el **riesgo de concentración** principalmente se aplica en el lado de los activos del balance general. Como práctica común, los supervisores no solamente requieren que los bancos tengan sistemas de información para identificar las concentraciones crediticias sino también establecen límites prudenciales para restringir las exposiciones de los bancos a prestatarios o grupos únicos 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 concentración. Esto es particularmente relevante en el contexto de contrapartes relacionadas o préstamos vinculados.

12. En el lado de los pasivos, el riesgo de concentración está estrechamente asociado con el riesgo de financiamiento, particularmente el riesgo de retiros tempranos y sorpresivos de fondos por grandes depositantes, con consecuencias de daño potenciales para la liquidez del banco. El riesgo de concentración es más probable de ser más alto en el caso de los bancos pequeños y aquellos que están menos activos en los mercados mayoristas que en los bancos grandes. El análisis de las concentraciones de depósito naturalmente requiere que un banco comprenda las características de sus depositantes, incluyendo no solamente sus identidades sino también el alcance al cual sus acciones pueden estar vinculadas con aquellas de otros depositantes. Es esencial que los gerentes de pasivos en los bancos pequeños no solamente conozcan sino mantengan una relación estrecha con los grandes depositantes, o correrán el riesgo de perder sus fondos particularmente durante las emergencias.

13. Es también importante monitorear el riesgo de concentración en activos bajo la administración. Los clientes de alto activo neto frecuentemente tienen cuentas múltiples con el mismo banco, pero en oficinas localizadas en diferentes países. Para manejar en forma efectiva el riesgo de reputación, de cumplimiento y legal que surge de dichas cuentas, los bancos deben ser capaces de agregar y monitorear balances y actividad en esas cuentas en una base global consolidada.

14. El Comité de Basilea y el Grupo Offshore de Supervisores Bancarios están totalmente convenidos de que las prácticas KYC efectivas deben ser parte de los sistemas de administración de riesgo y de control interno en todos los bancos alrededor del mundo. Los supervisores nacionales son responsables de asegurar que los bancos tengan los estándares mínimos y controles internos que les permitan adecuadamente conocer a sus clientes. Los códigos de conducta voluntarios⁵ emitidos por organizaciones o asociaciones de industria son para ser fomentados pero no son por sí mismos suficientes para asegurar la integridad del mercado o la administración de riesgo sólida.

III. Elementos esenciales de los estándares KYC

15. La directriz del Comité de Basilea en KYC ha sido incluida en los tres siguientes documentos y reflejan la evolución del pensamiento de supervisión durante el tiempo. *La Prevención del Uso Criminal del Sistema Bancario para propósitos de Lavado de Dinero* emitido en 1988 estipula los principios básicos éticos y anima a los bancos a establecer procedimientos efectivos para identificar a clientes, rechazar transacciones sospechosas y cooperar con las agencias de aplicación de la ley. Los Principios Básicos para una Supervisión Bancaria Efectiva (CP) expone, en una discusión más amplia de controles internos, que los bancos deben tener políticas, prácticas y procedimientos adecuados establecidos, incluyendo reglas estrictas de “conozca a sus clientes”; específicamente, los supervisores deben fomentar la adopción de las recomendaciones relevantes del FATF. Estas se relacionan a la identificación y registro de clientes, diligencia mejorada por instituciones financieras en la detección y reporte de transacciones sospechosas, y medidas para tratar con países con reglas inadecuadas anti-lavado de dinero. *La Metodología de los Principios Básicos 1999* (CPM, por sus siglas en inglés) elabora más los Principios Básicos listando un número de criterios esenciales y adicionales. (El anexo 2 delinea extractos relevantes de los Principios Básicos y la Metodología).

16. Se debe requerir a todos los bancos “tener establecidas políticas, prácticas y procedimientos que promuevan estándares altos de ética y profesionalismo y prevengan al banco de ser usados, intencional o no intencionalmente, por elementos criminales”.⁶ Ciertos elementos clave deben ser incluidos por los bancos en el diseño de programas KYC que ajusten mejor sus circunstancias. Dichos

⁵ Un ejemplo de un código de la industria son las “Directrices globales anti-lavado de dinero para la Banca Privada” (también conocidas como Principios Wolfsberg) que se diseñaron recientemente por los doce bancos más importantes con involucramiento significativo en la banca privada.

⁶ *Metodología de los Principios Básicos*, Criterio Esencial 1.

elementos esenciales deben iniciar de la administración de riesgo y procedimientos de control de los bancos y deben incluir (1) política de aceptación de clientes, (2) identificación de clientes, (3) monitoreo continuo de cuentas de alto riesgo y (4) administración de riesgo. Los bancos no solamente establecen la identidad de sus clientes, sino deben también monitorear la actividad de la cuenta para determinar aquellas transacciones que no estén de conformidad con las transacciones normales o esperadas para ese tipo de cliente o tipo de cuenta. KYC debe ser una característica básica de la administración de riesgo y procedimientos de control de los bancos, y ser complementada por revisiones de cumplimiento y auditorías internas regulares. No obstante, es importante que los requerimientos no lleguen a ser muy restrictivos que nieguen el acceso a los servicios bancarios, especialmente para las personas que están financiera o socialmente en desventaja.⁷

1. Política de aceptación de clientes

17. Los bancos deben desarrollar políticas y procedimientos claros de aceptación de clientes, incluyendo una descripción de los tipos de clientes que son inaceptables a la administración bancaria. En la preparación de dichas políticas, los factores como antecedentes, país de origen, posición pública o de perfil alto, actividades de negocio de los clientes u otros indicadores de riesgo deben ser considerados. Los bancos deben desarrollar políticas y procedimientos graduados de aceptación de clientes que requieran una debida diligencia más extensa para clientes de alto riesgo. Por ejemplo, las políticas pueden requerir los requerimientos de apertura de cuenta más básicos para un individuo trabajador con un balance de cuenta pequeño, mientras que una debida diligencia bastante extensa puede ser considerada esencial para un individuo con un activo neto alto cuya fuente de fondos es incierta. Las decisiones para involucrarse en relaciones de negocio con clientes de alto riesgo, como personalidades (ver más adelante), deben ser tomadas exclusivamente a nivel de la alta dirección.

2. Identificación de clientes

18. La identificación de clientes es un elemento esencial de los estándares KYC. Un cliente se define como cualquier persona o entidad que tiene un cuenta con un banco y cualquier persona o entidad en cuyo nombre se mantiene una cuenta, como también los beneficiarios de transacciones realizadas por intermediarios financieros profesionales. Específicamente, un cliente debe incluir un mantenimiento de cuenta y el propietario de beneficio de una cuenta. Un cliente debe también incluir el beneficiario de un fideicomiso, un fondo de inversión, un fondo de pensión o una compañía cuyos activos son administrados por un gerente de activos, o el otorgador de un fideicomiso.

⁷ Por ejemplo, podría ser difícil para las minorías, estudiantes, ancianos o personas inválidas producir los documentos preferentes que confirmen su identidad.

19. Los bancos deben establecer un procedimiento sistemático para verificar la identidad de nuevos clientes y nunca debe involucrarse en una relación de negocios hasta que la identidad de un nuevo cliente esté satisfactoriamente establecida. Los bancos deben “documentar y poner en vigor políticas para la identificación de clientes y aquellos que actúan en su nombre”.⁸ Los mejores documentos para verificar la identidad de los clientes son aquellos más difíciles de obtener y de falsificar.

20. El proceso de identificación de clientes se aplica naturalmente al inicio de la relación, pero también existe una necesidad de aplicar los estándares KYC a cuentas de clientes existentes. En donde dichos estándares han sido introducidos recientemente y aún no se aplican completamente a los clientes existentes, un ejercicio de evaluación de riesgo puede ser llevado a cabo y dar prioridad a obtener la información necesaria, donde sea deficiente, en respecto de los casos de riesgo más alto. Un momento apropiado para revisar la información disponible en los clientes existentes es cuando una transacción de importancia toma lugar, o cuando existe un cambio material en la forma en que la cuenta es operada. Sin embargo, si un banco está alerta de que carece de información suficiente sobre un cliente de alto riesgo existente, debe tomar los pasos necesarios para asegurar que toda la información relevante sea obtenida tan pronto como sea posible. Además, el supervisor necesita establecer una fecha objetivo apropiada para la finalización de una revisión KYC y regularización de todas las cuentas existentes. En cualquier evento, un banco debe realizar revisiones regulares de su base de clientes para establecer que tiene información actualizada y un conocimiento apropiado de la identidad de los tenedores de cuentas y de sus negocios.

21. Los bancos que ofrecen servicios bancarios privados están particularmente expuestos al riesgo de reputación. La banca privada por naturaleza involucra una gran medida de confidencialidad. Las cuentas de banca privada pueden ser abiertas a nombre de un individuo, un negocio comercial, un fideicomiso, un intermediario o una compañía personalizada de inversión. En cada caso el riesgo reputación puede surgir si el banco no sigue diligentemente los procedimientos KYC establecidos. En ninguna circunstancia las operaciones de banca privada deben funcionar autónomamente, o como un “banco dentro de un banco”,⁹ y ninguna parte del banco debe escapar de los procedimientos requeridos. Esto significa que todos los clientes nuevos y cuentas nuevas deben ser aprobadas por lo menos por una persona además del gerente de relación de banca privada. Si se establecen resguardos internamente para proteger la confidencialidad de los clientes de banca privada y sus negocios, los bancos deben asegurarse que por lo menos un escrutinio equivalente y monitoreo de estos clientes y sus negocios puedan ser realizados., por ej., deben estar abiertos a revisión por parte de los funcionarios de cumplimiento y auditores.

⁸ *Metodología de los Principios Básicos*, Criterio Esencial 2.

⁹ Algunos bancos aíslan sus funciones de banca privada o crean paredes Chinas como medio de provisión de protección adicional para la confidencialidad de clientes.

2.1 Requerimientos generales de identificación

22. Los bancos necesitan obtener toda la información necesaria para establecer a su total satisfacción la identidad de cada cliente nuevo y el propósito y naturaleza intencionada de la relación del negocio. El alcance y naturaleza de la información depende del tipo de solicitante (personal, corporativo, etc.) y el tamaño previsto de la cuenta. Los supervisores nacionales están animados a proveer una guía para ayudar a los bancos en el diseño de sus propios procedimientos de identificación. Se describen algunos ejemplos del tipo de información que sería apropiada en el Anexo 1.

23. Los bancos deben aplicar todos sus procedimientos KYC a solicitantes que planean transferir un balance abierto de otra institución financiera, teniendo en mente que el gerente de cuenta previo puede haber solicitado que la cuenta sea removida debido a preocupaciones sobre las actividades dudosas o ambiguas.

24. Los bancos no deben acordar abrir una cuenta o realizar negocios continuos con un cliente que insiste en un estado de anonimato o “portador” o quien da un nombre ficticio. Tampoco las cuentas confidenciales numeradas¹⁰ deben funcionar como cuentas anónimas sino deben estar sujetas a exactamente los mismos procedimientos KYC como todas las cuentas de clientes, aún si la prueba es realizada por personal seleccionado. Considerando que una cuenta numerada puede ofrecer protección adicional para la identidad del cuentahabiente, la identidad debe ser conocida a un número de personal para operar la debida diligencia apropiada. Dichas cuentas no deben en ninguna circunstancia ser usadas para ocultar la identidad del cliente de la función de cumplimiento o de los supervisores de un banco.

25. Los bancos necesitan estar alertas en prevenir que las entidades corporativas de negocio sean usadas por personas naturales como un método para operar cuentas anónimas. Los vehículos de tenencia de activos personales, como compañías de negocio internacionales (IBCs, por sus siglas en inglés), pueden hacer dificultosa la identificación apropiada de clientes o propietarios beneficiarios. Un banco debe tomar las medidas necesarias para satisfacerse a sí mismo de que conoce la identidad real del último propietario de dichas entidades.

2.2 Temas específicos de identificación

26. Existe un número de temas más detallados relacionados a la identificación de clientes que necesitan ser abarcados. Se agradecerán comentarios particulares sobre los temas mencionados en esta sección. Muchos de ellos actualmente están bajo consideración del FATF como parte de una revisión general de sus 40 recomendaciones, y el Grupo de Trabajo reconoce la necesidad de ser consistente con el FATF.

¹⁰ En una cuenta numerada, el nombre del propietario beneficiario es conocido al banco pero es sustituido por un número de cuenta o nombre de código en la documentación subsiguiente.

2.2.1 Cuentas de fideicomiso, de intermediario y fiduciarias o cuentas de clientes abiertas por intermediarios profesionales.

27. Las cuentas de fideicomiso, de intermediario y fiduciarias pueden ser usadas para evitar los procedimientos de identificación de clientes. Mientras esto puede ser legítimo bajo ciertas circunstancias para proporcionar un capa extra de seguridad para proteger la confidencialidad de los clientes de banca privada legítimos, es esencial que la relación real sea comprendida. Los bancos deben establecer si el cliente está actuando a nombre de otra persona como fideicomisario, agente o intermediario profesional (por ej., un abogado o un contador). De ser así, una condición previa necesaria es el recibo de evidencia satisfactoria de la identidad de cualesquiera intermediarios y de las personas bajo el nombre en que están actuando, como también detalles de la naturaleza del fideicomiso u otros convenios establecidos.

28. Los bancos pueden mantener cuentas “agrupadas” (pooled) (por ej., cuentas de clientes manejadas por firmas legales) o cuentas abiertas por parte de las entidades agrupadas, como gerentes de fondos mutuos o monetarios. En tales casos, los bancos deben decidir, dado a las circunstancias, si el cliente es el intermediario, o si sería más apropiado por medio del intermediario buscar a los últimos propietarios beneficiarios. En cada caso, la identidad del cliente que está sujeto a debida diligencia debe estar claramente establecida. Los propietarios beneficiarios deben ser verificados cuando sea posible. Cuando no sea así, los bancos deben desempeñar debida diligencia sobre el intermediario y establecer a su entera satisfacción que el intermediario tiene un proceso sólido de debida diligencia para cada uno de sus clientes.

29. Necesita ejercitarse un especial cuidado al iniciar transacciones de negocio con compañías que tienen accionistas o acciones de intermediarios en forma de portador. Es necesario obtener una evidencia satisfactoria de la identidad de los propietarios beneficiarios de todas las compañías.

30. Los procedimientos anteriores pueden demostrar dificultad al seguirlos en algunos países. En el caso de intermediarios profesionales como abogados, podría existir códigos de conducta profesionales en la prevención de la diseminación de información con respecto a sus clientes. El FATF actualmente está involucrado en una revisión de los procedimientos KYC que rigen a las cuentas abiertas por abogados por parte de clientes. El Grupo de Trabajo por consiguiente no ha tomado una posición definitiva sobre este tema.

3.2.2 Negocios de introducción

31. El desarrollo de procedimientos de identificación puede ser un consumidor de tiempo y existe un deseo natural de limitar cualquier inconveniente para los nuevos clientes. En algunos países, no obstante ha llegado a ser habitual para los descansar en los procedimientos realizados por otros bancos o introductores cuando se refiere a negocios. De hacerlo así, el riesgo de que los bancos confíen excesivamente en los procedimientos de debida diligencia que esperan que los

introdutores hayan desarrollado. La confianza en la debida diligencia realizada por un introductor, aunque de reputación, en ninguna forma remueve la responsabilidad última del banco receptor de conocer a sus clientes y sus negocios. En particular, los bancos no deben confiar en los introductores que están sujetos a estándares débiles que aquellos regidos por los propios procedimientos KYC de los bancos o que están dispuestos a compartir copias de la documentación de debida diligencia.

32. El FATF actualmente está involucrado en una revisión de la adecuación de los introductores elegibles, es decir, si deben ser confinados a bancos con reputación únicamente o deben extenderse a las instituciones reguladas, si un banco debe establecer una relación contractual con sus introductores y si es apropiado confiar en un introductor tercera parte por completo. El Grupo de Trabajo aún está desarrollado su opinión sobre este tópico.

2.2.3 *Riesgo de personalidad*

33. Las relaciones de negocio con individuos que mantienen posiciones públicas importantes y con personas o compañías claramente vinculadas a ellos pueden exponer a un banco a riesgos de reputación y/o legales significativos. Dichas personas, comúnmente conocidas como “personalidades”, incluyen jefes extranjeros de estado, ministros, funcionarios públicos influyentes, jueces y comandantes militares. Existe siempre una posibilidad, especialmente en países donde la corrupción está muy difundida, que dichas personas abusan de sus poderes públicos para su propio enriquecimiento ilícito mediante el recibo de sobornos, malversación, etc.

34. La aceptación y administración de fondos de personalidades corruptas daña severamente la propia reputación del banco y puede socavar la confianza pública en los estándares éticos de un centro financiero completo, ya que dichos casos usualmente reciben una atención extensiva y reacción política fuerte, aún si el origen ilegal de los activos a menudo es difícil probar. Además, el banco puede estar sujeto a solicitudes costosas de información y órdenes de acceso de autoridades de aplicación de la ley o judiciales (incluyendo procedimientos de asistencia internacional mutua en asuntos criminales) y podría ser responsable de acciones por daños por el estado interesado o la víctimas de un régimen. Bajo ciertas circunstancias, el banco y/o sus funcionarios y empleados por sí mismos podrían estar expuestos a cargas de lavado de dinero, si saben o deben saber que los fondos provenientes de corrupción u otros crímenes serios. De hecho, algunos países recientemente han enmendado o están en proceso de enmendar sus leyes y regulaciones para la corrupción activa criminalizada de servidores civiles extranjeros y funcionarios públicos de acuerdo con la convención internacional relevante.¹¹ En estas jurisdicciones la corrupción extranjera llega a ser una ofensa manifestada por el lavado de dinero y todas las regulaciones y leyes anti-lavado de dinero aplicadas (por ej., reporte de transacciones sospechosas, prohibición sobre la información al cliente, congelamiento interno de fondos, etc.). Pero aún en

¹¹ Ver la *Convención sobre El Combate al Soborno de Funcionarios Públicos Extranjeros en Transacciones Internacionales de Negocios*, adoptado por la Conferencia de Negociación el 21 de noviembre de 1997.

ausencia de dicha base legal explícita en la ley criminal, es claramente indeseable, no ético e incompatible con la conducta justa y apropiada de las operaciones bancarias aceptar o mantener una relación de negocio si el banco conoce o debe asumir que los fondos derivados de corrupción o mal uso de activos públicos. Existe la obligación necesaria para que los bancos consideren una relación con una personalidad para identificar que la persona como también las personas y compañías que están claramente vinculadas a las personalidades.

2.2.4 Clientes indirectos (no cara a cara)

35. Los bancos están solicitando incrementadamente abrir cuentas a nombre de clientes que no se presentan a una entrevista personal. Esto ha sido siempre un evento frecuente en el caso de clientes no residentes, pero se ha incrementado significativamente con la reciente llegada de la banca postal, telefónica y electrónica. Los bancos deben aplicar igualmente los procedimientos efectivos de identificación de clientes y estándares de monitoreo continuo para clientes indirectos como para aquellos disponibles para entrevista. Un tema que ha surgido en esta conexión es la posibilidad de verificación independiente por una tercera parte de reputación. Este tema completo de clientes indirectos está siendo discutido por el FATF, y también está sujeto de un anteproyecto de Norma EC, y el tópico por consiguiente permanece sujeto a revisión por el Grupo de Trabajo.

36. Un ejemplo típico de un cliente indirecto es alguien que desea realizar banca electrónica vía Internet o tecnología similar. La banca electrónica actualmente incorpora una serie amplia de productos y servicios entregados sobre redes de telecomunicaciones. La naturaleza anónima y sin límites de la banca electrónica combinado con la velocidad de la transacción inevitablemente crea dificultad en la identificación y verificación de clientes. Como una política básica, los supervisores esperan que los bancos deban proactivamente evaluar varios riesgos situados por tecnologías emergentes y diseño de procedimientos de identificación de clientes respecto a dichos riesgos.¹²

3. Monitoreo continuo de cuentas de alto riesgo

37. Sin dicho conocimiento, probablemente fracasarán en su responsabilidad de reportar transacciones sospechosas a las autoridades apropiadas en casos donde se solicita hacerlo así. El proceso de monitoreo continuo incluye los siguiente:

- Los bancos deben desarrollar “estándares claros sobre los registros que deben ser guardados sobre la identificación del cliente y transacciones

¹² El Grupo de Banca Electrónica del Comité de Basilea actualmente está desarrollando principios directrices para la administración prudente del riesgo de las actividades de banca electrónica y específicamente delineará expectativas de supervisión apropiadas con respecto a los enfoques que los bancos deben tener en la identificación, evaluación, administración y control de los riesgos asociados con la banca electrónica. Estos principios también incluyen una directriz sobre cómo autenticas e identificar a clientes en el contexto de banca electrónica.

individuales y el período de retención”.¹³ Como el punto de partida y seguimiento natural del proceso de identificación, los bancos deben obtener y mantener actualizados los documentos de identificación y retenerlos por lo menos cinco años después de que la cuenta fue cerrada. Deben también retener todos los registros de transacción financiera por lo menos cinco años después de que la transacción se haya realizado.

- La alta dirección de un banco a cargo de negocios de banca privada debe conocer las circunstancias personales de los clientes importantes/grandes de los bancos y estar alertas a fuentes de información de tercera parte. Cada banco debe diseñar su propia distinción entre los clientes grandes/importantes y otros, y establecer los indicadores de inicio para ellos consiguientemente, tomando en cuenta el país de origen y otros factores de riesgo. Las transacciones significativas por clientes de alto riesgo deben ser aprobadas por un alto administrador.
- Los bancos deben tener sistemas establecidos para detectar patrones inusuales o sospechosos de actividad. Esto puede hacerse estableciendo límites para una clase o categoría particular de cuentas. Se debe prestar particular atención a las transacciones que exceden estos límites. Ciertos tipos de transacciones deben alertar a los bancos de la posibilidad de que el cliente está realizando actividades indeseables. Ellas pueden incluir transacciones que no tienen sentido económico o comercial, o que involucra grandes cantidades de depósitos de efectivo que no son consistentes con las transacciones normales o esperadas del cliente. Un alto volumen de operaciones de cuenta, inconsistente con el tamaño del balance, puede indicar que los fondos están siendo “lavados” mediante una cuenta. Una lista de actividades sospechosas diseñada por supervisores puede ser muy útil a los bancos.
- Los bancos deben desarrollar una política, directrices, procedimientos y controles internos claros y permanecer especialmente alertas con respecto a las relaciones de negocio con personalidades e individuos de alto perfil o con personas o compañías que están claramente vinculadas o asociadas con ellos.¹⁴

¹³ *Metodología de Principios Básicos*, Criterio Esencial 2.

¹⁴ Es irrealista esperar que el banco conozca o investigue cada familia, político o conexión de negocios distantes de un cliente extranjero. La necesidad de perseguir sospechosos dependerá del tamaño de los activos o volumen de operaciones, patrón de transacciones, antecedentes económicos, reputación del país, admisión de explicaciones de clientes, etc. También se debe hacer notar que las personalidades (o más bien a los miembros y amigos de la familia) no necesariamente se presentarán a sí mismos en esas capacidades, sino más bien como personas de negocios ordinarios (aunque saludables), enmascarando el hecho de que deben su alta posición en una corporación de negocios legítima únicamente a su relación privilegiada con el propietario de la oficina pública.

4. Administración de Riesgo

38. Los procedimientos efectivos KYC adoptan rutinas para apropiadas vigilancia administrativa, sistemas y controles, segregación de responsabilidades, capacitación y otras políticas relacionadas. El consejo de directores del banco debe completamente comprometerse en un programa efectivo KYC estableciendo procedimientos apropiados para asegurar su efectividad. Los bancos deben designar a un alto funcionario con responsabilidad explícita para asegurar que las políticas y procedimientos del banco, están por lo mínimo, de acuerdo con prácticas locales de supervisión. Los bancos deben tener procedimientos escritos claros, comunicados a todo el personal, para que el personal reporte transacciones sospechosas a un alto director específico. Ese director debe entonces evaluar si las obligaciones estatutorias del banco bajo regímenes reconocidos de reporte de actividades sospechosas requieran que la transacción sea reportada a las autoridades de supervisión y aplicación de la ley apropiadas.

39. Todos los bancos deben tener un programa continuo de capacitación a empleados para que el personal del banco esté adecuadamente entrenado en los procedimientos KYC. La programación y contenido de capacitación para varios sectores tiene un enfoque diferente para el personal nuevo, personal de primera línea, personal de cumplimiento o personal que trata con nuevos clientes. El nuevo personal debe ser educado en la importancia de las políticas KYC y los requerimientos básicos en el banco. Los miembros del personal de primera línea que tratan directamente con el público deben ser capacitados para verificar la identidad del cliente para nuevos clientes, para ejercitar la debida diligencia en el manejo de cuentas de clientes existentes en una base continuo y para detectar patrones de actividad sospechosa. Se debe proveer una capacitación regular refrescante para asegurar que el personal está conciente de sus responsabilidades y se mantiene informado de nuevos desarrollos. Es crucial que todo el personal relevante comprenda totalmente la necesidad e implementación de políticas KYC consistentemente. Una cultura dentro de los bancos que promueva dicha comprensión es la clave para una implementación exitosa.

40. Las funciones de auditoría interna y cumplimiento de los bancos tiene responsabilidades importantes en la evaluación y seguridad de adherencia a políticas y procedimientos KYC. Como regla general, la función de cumplimiento provee una evaluación independiente de las propias políticas y procedimientos del banco, incluyendo requerimientos legales y regulatorios. Sus responsabilidades deben incluir el monitoreo continuo del desempeño del personal mediante una prueba de muestreo de cumplimiento y revisión de reportes de excepción para alertar a la alta dirección o al Consejo de Directores si se cree que la administración está fallando en abarcar los procedimientos KYC en una forma responsable.

41. La auditoría juega un papel importante en la evaluación independiente de la administración y controles del riesgo, descargando la responsabilidad al Comité de Auditoría del Consejo de Directores o un cuerpo de vigilancia similar mediante evaluaciones periódicas de la efectividad del cumplimiento con políticas y procedimientos KYC. La Administración debe asegurarse que las funciones de auditoría sean provistas al personal adecuadamente con individuos que estén bien

instruidos en dichas políticas y procedimientos. Además, los auditores internos deben ser proactivos en el seguimiento de sus hallazgos y críticas.

42. En muchos países, los auditores externos también tienen un papel importante que jugar en el monitoreo de los controles y procedimientos internos de los bancos, y en la confirmación que de están de conformidad con la práctica de supervisión.

IV. El papel de los supervisores

43. Basado en estándares internacionales existentes KYC, los supervisores nacionales esperan establecer las prácticas de supervisión rigen los programas KYC de los bancos. Los elementos esenciales como se presentan en este documento deben proporcionar una guía clara para que los supervisores procedan con el trabajo de diseño o mejora de la práctica de supervisión nacional.

44. Además al establecimiento de los elementos básicos a seguir por los bancos, los supervisores tienen la responsabilidad de monitorear que los bancos estén aplicando procedimientos sólidos KYC y estén sosteniendo estándares éticos y profesionales en una base continua. Los supervisores deben asegurar que están establecidos los controles internos apropiados y que los bancos están de conformidad con la directriz de supervisión. El proceso del supervisor debe incluir no solamente una revisión de políticas y procedimientos, sino también una revisión de los archivos del cliente y el muestreo de algunas cuentas. Los supervisores deben tener siempre el derecho de acceder a toda la documentación relacionada a cuentas mantenidas en esa jurisdicción, incluyendo cualquier análisis que el banco haya efectuado para detectar transacciones sospechosas.

45. Los supervisores tienen la responsabilidad de no solamente asegurar que sus bancos mantengan altos estándares KYC para proteger su propia seguridad y solidez sino también proteger la integridad de sus sistema bancario nacional. Los supervisores deben poner en claro que tomarán las acciones apropiadas, que pueden ser severas y publicas si las circunstancias garantizan, contra los bancos y sus funcionarios quienes fehacientemente fracasen en seguir sus propios procedimientos internos. Además, los supervisores deben asegurar que los bancos estén alertas y presten particular atención a las transacciones que involucran jurisdicciones donde los estándares son considerados inadecuados. El FATF y algunas autoridades nacionales han listado un número de países y jurisdicciones que están consideradas tener convenios legales y administrativos que no cumplen con estándares internacionales para combatir el lavado de dinero. Dichos hallazgos deben ser un componente de las políticas y procedimientos KYC de un banco.

V. Implementación de los Estándares KYC en un contexto internacional

46. Los supervisores alrededor del mundo deben buscar, al mejor de sus esfuerzos, construir e implementar sus estándares nacionales KYC completamente en línea con estándares internacionales para evitar arbitraje potencial regulatorio y resguardo de la integridad de los sistemas bancarios nacionales e internacionales. La implementación y evaluación de dichos estándares pone el resto de la voluntad de los supervisores de cooperar con cada otro en una forma muy práctica, como también la habilidad de los bancos en controlar los riesgos en una base de grupo. Esta es una tarea desafiante para los bancos y supervisores.

47. Los supervisores esperan que los grupos bancarios apliquen un estándar mínimo aceptado de políticas y procedimientos KYC a sus operaciones locales e internacionales. La supervisión de la banca internacional puede únicamente realizarse efectivamente en una base consolidada, y el riesgo de reputación como también otros riesgos bancarios no están limitados a límites nacionales. Los bancos matriz deben comunicar sus políticas y procedimientos a sus sucursales y subsidiarias internacionales, incluyendo entidades no bancarias como compañías de fideicomiso privado, y tener una rutina para examinar el cumplimiento contra los estándares KYC del país sede y del anfitrión a fin de que sus programas operan efectivamente en forma global. Dichos exámenes de cumplimiento también serán probados por auditores externos y supervisores. Por consiguiente, es importante que la documentación KYC sea adecuadamente archivada y esté disponible para su inspección. Hasta donde se refiera a los chequeos de cumplimiento, los supervisores y auditores externos desearán en la mayoría de los casos examinar los sistemas y controles y revisar el monitoreo de las cuentas y transacciones de clientes como parte del proceso de muestreo.

48. No obstante de que un establecimiento internacional es pequeño, se debe designar un alto funcionario para ser directamente responsable de la seguridad de que todo el personal relevante está capacitado, y observe los procedimientos KYC que cumplen los estándares de la sede y del anfitrión. Mientras que este funcionario tendrá la principal responsabilidad, he debe ser apoyado por los auditores internos y funcionarios de cumplimiento de las oficinas locales y de principales cuando sea apropiado.

49. En donde los estándares KYC mínimos de los países sede y anfitriones sean diferentes, las sucursales y subsidiarias en las jurisdicciones anfitrionas deben aplicar estándares el estándar más alto de los dos. En general, no debe existir impedimento para prevenir a un banco de adoptar estándares que son más grandes que los mínimos requeridos a nivel local. Si, sin embargo, las leyes y regulaciones locales (especialmente provisiones de secreto) prohíben la implementación de los estándares KYC del país sede, cuando estos últimos son más rígidos, los supervisores del país anfitrión deben usar sus mejores esfuerzos para tener la ley y las regulaciones cambiadas. Mientras tanto, las sucursales y subsidiarias internacionales tendrían que cumplir con los estándares del país anfitrión, pero deben estar seguros de que la oficina principal o banco matriz y su supervisor de país sede estén totalmente informados de la naturaleza de la diferencia.

50. Los elementos criminales probablemente están diseñados hacia las jurisdicciones con dichos impedimentos. De allí que los bancos deben estar alertas del alto riesgo de reputación de la realización de negocios en estas jurisdicciones. Los bancos matriz deben tener un procedimiento para revisar la vulnerabilidad de las unidades individuales operativas e implementar resguardos adicionales cuando sea apropiado. En casos extremos, los supervisores deberían considerar establecer controles adicionales en los bancos que operan en esas jurisdicciones y finalmente tal vez animar su retiro.

51. Durante las inspecciones in situ, los supervisores o auditores del país sede deben no deben afrontar impedimentos en la verificación del cumplimiento de la unidad con políticas y procedimientos KYC. Este requerirá una revisión de los archivos de cliente y algún muestreo al azar de cuentas. Los supervisores del país sede deben tener acceso a información sobre cuentas de clientes individuales muestreadas al alcance necesario para permitir un evaluación apropiada de la aplicación de los estándares KYC y una evaluación de las prácticas de administración de riesgo, y no deben ser impedidas por las leyes de secreto bancario locales. Cuando el supervisor de país sede requiere un reporte consolidado de depósitos o concentraciones de prestatario o notificación de fondos bajo administración, no deben existir impedimentos. Además, con vistas a monitorear las concentraciones de depósito o el riesgo de financiamiento de los depósitos que son retirados, los supervisores sede pueden aplicar pruebas de materialidad y establecer algunos comienzos para que si el depósito de un cliente excede un cierto porcentaje del balance general, los bancos los deben reportar al supervisor sede. Sin embargo, se necesitan resguardos para asegurar que la información sobre cuentas individuales sean usadas para propósitos de supervisión únicamente y no pasen a terceras partes no supervisoras.

52. En algunos casos podría existir un conflicto serio entre las políticas KYC de un banco matriz impuestas por su autoridad sede y lo que está permitido en una oficina internacional. Podrían ser, por ejemplo, leyes locales que previenen inspecciones por funcionarios de cumplimiento, auditores internos o supervisores de país sede de los bancos matriz o los que permiten a los clientes bancarios usar nombres ficticios o esconderse detrás de sus agentes o intermediarios a quienes se les prohíbe revelar quiénes son sus clientes. En tales casos, se le recomienda al supervisor sede comunicarse con el supervisor anfitrión para confirmar si verdaderamente existen impedimentos legales genuinos y si son aplicables extraterritorialmente. Si prueban ser insuperables, el supervisor sede debe poner en claro al anfitrión que el banco puede decidir por sí mismo, p ser requerido por su supervisor sede, a cerrar la operación en cuestión. En el análisis final, cualesquiera convenios que señalan dichas inspecciones in situ debe proveerse un mecanismo que permita una evaluación de que es satisfactorio al supervisor sede. Los convenios de cooperación o memoranda de entendimiento que establecen las mecánicas de los convenios puede ser útiles. El acceso a información por supervisores de país sede no debe ser tan restrictivo como sea posible, cubriendo las políticas y procedimientos generales de los bancos para la debida diligencia de clientes y para tratar con sospechosos.

VI. Proceso de consulta

53. Este documento está siendo publicado para consulta. Se agradecerán los comentarios de supervisiones nacionales, organizaciones y bancos internacionales relevantes para el 31 de marzo de 2001, después de lo cual el documento final será emitido. Los comentarios deben ser enviados a la Secretaría del Comité de Basilea en Supervisión Bancaria (Dirección: The Basel Committee on Banking Supervision, Bank for International Settlements, CH-4002 Basel. Switzerland; Fax: 41 61 2809100) con copias a las autoridades de supervisión nacionales, cuando se apropiado.

Anexo 1

Requerimientos generales de identificación

Este anexo presenta una lista sugerida de requerimientos de identificación para clientes personales y corporaciones. Se anima a que los supervisores nacionales proveen una guía para ayudar a los bancos en el diseño de sus propios procedimientos de identificación.

Clientes personales

Para clientes personales, los bancos necesitan obtener la siguiente información:

- Nombre y/o nombres usados,
- dirección residencial permanente,
- fecha y lugar de nacimiento,
- nombre del empleador o naturaleza del auto-empleo/negocio
- muestra de firma, y
- fuentes de fondos.

La información adicional se relacionaría a la nacionalidad o país de origen, posición pública o de alto perfil, etc. Los bancos deben verificar la información contra los documentos originales de identidad emitida por una autoridad oficial (algunos ejemplos incluyen las tarjetas y pasaportes de identidad). Dichos documentos deben ser aquellos que son más difíciles de obtener en forma ilícita. En países donde nuevos clientes no poseen documentos de identidad de antemano, por ej., tarjetas de identidad, pasaportes o licencias de conducir, se debe requerir alguna flexibilidad. Sin embargo, se debe prestar cuidado particular en aceptar documentos que son fácilmente falsificados o que pueden ser cómodamente obtenidos con falsas identidades. Donde existe un contrato cara a cara, la apariencia debe ser verificada contra un documento oficial que tenga una fotografía. Cualesquiera cambios subsiguientes a la información anterior debe también ser registrado y verificado.

Clientes corporativos y de otros negocios

Para clientes corporativos y de otros negocios, los bancos deben obtener evidencia de su estatus legal, como un documento de incorporación, convenio de sociedad, documentos de asociación o una licencia de negocios. Para las cuentas corporativas grandes debe también obtenerse un estado financiero del negocio o una descripción de la línea de negocios principal del cliente. Además, si ocurren subsiguientemente algunos cambios significativos a la estructura o propiedad de la compañía, se deben realizar chequeos adicionales. En todos los casos, los bancos necesitan verificar que la corporación o entidad de negocio existe y se compromete en su negocio establecido. Los documentos originales o copias certificadas de los certificados deben ser producidas para verificación.

Anexo 2

Excepciones de la Metodología de los Principios Básicos

Principio 15. Los supervisores bancarios deben determinar que los bancos tienen establecidos políticas, prácticas y procedimientos adecuados, incluyendo reglas estrictas de “conozca a sus clientes”, que promueven altos estándares éticos y profesionales en el sector financiero y prevenir al banco de ser usado, intencional y no intencionalmente por elementos criminales.

Criterios esenciales

1. El supervisor determina que los bancos tengan establecidos políticas, prácticas y procedimientos adecuados que promuevan estándares éticos y profesionales y prevengan al banco de ser usado, intencional o no intencionalmente, por elementos criminales. Esto incluye la prevención y detección de actividad criminal o fraude, y reporte de dichas actividades sospechosas a las autoridades apropiadas.
2. El supervisor determina que los bancos tengan políticas documentadas y en vigor para la identificación de clientes y aquellos que actúan en su nombre como parte de su programa de anti-lavado de dinero. Existen reglas claras sobre qué registros se deben guardar sobre la identificación del cliente y transacciones individuales y el período de retención.
3. El supervisor determina que los bancos tengan procedimientos formales para reconocer transacciones potencialmente sospechosas. Estas podrían incluir autorización adicional para depósitos grandes de efectivo (o similar) o retiros y procedimientos especiales para transacciones inusuales.
4. El supervisor determina que los bancos designen a un alto funcionario con responsabilidad explícita para asegurar que las políticas y procedimientos del banco están, por lo mínimo, de acuerdo con los requerimientos estatutarios y regulatorios de anti-lavado de dinero.
5. El supervisor determina que los bancos tengan claros procedimientos, comunicados a todo el personal, para que el personal reporte transacciones sospechosas a una alto funcionario superior responsable para el cumplimiento de anti-lavado de dinero.
6. El supervisor determina que los bancos han establecido líneas de comunicación a la administración y a una función de seguridad interna (guardián) para reportar los problemas.
7. Además del reporte a las autoridades criminales apropiadas, los bancos informan al supervisor de las actividades sospechosas o incidentes de fraude material a la seguridad, solidez y reputación del banco.
8. Las leyes, regulaciones y/o políticas de los bancos aseguran que un miembro de personal que reporta transacciones sospechosas en buena fe al alto funcionario

superior, función de seguridad interna, o directamente a la autoridad relevante no pueden tenerse como responsables.

9. El supervisor periódicamente chequea que los controles de lavado de dinero de los bancos y sus sistemas para la prevención, identificación e información del fraude sean suficientes. El supervisor tiene facultades adecuadas (regulatorias y/o de procedimiento criminal) para tomar acción contra un banco que no cumple con sus obligaciones de anti-lavado de dinero.
10. El supervisor es responsable, directa o indirectamente, de compartir con las autoridades de supervisión del sector financiero extranjero y nacional la información relacionada a actividades criminales de sospechosas o reales.
11. El supervisor determina que los bancos tengan un establecimiento de política sobre ética y comportamiento profesional que esté claramente comunicada a todo el personal.

Criterios adicionales

1. Las leyes y/o regulaciones incluyen prácticas internacionales sólidas, como cumplimiento con las 40 Recomendaciones del Grupo de Trabajo de Acción Financiera emitido en 1990 (revisado en 1996).
2. El supervisor determina que el personal bancario esté adecuadamente capacitado sobre la detección y prevención de lavado de dinero.
3. El supervisor tiene la obligación legal de informar las autoridades criminales relevantes de cualesquiera transacciones sospechosas.
4. El supervisor es responsable, directa o indirectamente, de compartir a las autoridades judiciales información relacionada a actividades criminales de sospecha o reales.
5. Si no se desempeña por otra agencia, el supervisor tiene recursos en casa con experiencia especializada sobre fraude financiero y obligaciones de anti-lavado de dinero.

Anexo 3

Excepciones de las recomendaciones FATF

C. Papel del sistema financiero en el combate de lavado de dinero

Reglas de identificación y registro de clientes

10. Las instituciones financieras no deben mantener cuentas anónimas o cuentas en nombres obviamente ficticios: se les debe requerir (por ley, por regulaciones, por convenios entre autoridades de supervisión e instituciones financieras o por convenios de auto regulación entre instituciones financieras) identificar, en base a un documento de identificación oficial u otro confiable, y registrar la identidad de sus clientes, ya sea ocasionales o usuales, cuando se establecen relaciones de negocio o se realizan transacciones (en particular la apertura de cuentas o libretas bancarias, registro de transacciones fiduciarias, renta de cajillas de seguridad, desarrollo de las grandes transacciones en efectivo).

Para cumplir con los requerimientos de identificación con relación a las entidades legales, las instituciones financieras deben, cuando sea necesario, tomar medidas:

- (i) para verificar la existencia y estructura legal del cliente obteniendo ya sea de un registros público o del cliente o ambos, pruebas de incorporación, incluyendo información con respecto al nombre, forma legal, dirección, directores y provisiones que regulan el poder para obligar a la entidad.
 - (ii) verificar que cualquier persona que pretendan actuar en nombre del cliente está autorizada así e identificar a esa persona.
11. Las instituciones financieras deben tomar las medidas razonables para obtener información sobre la verdadera identidad de las personas en cuyo nombre se abre una cuenta o se realiza una transacción, si existen algunas dudas como si estos clientes están actuando en su propio nombre, por ejemplo, en el caso de compañías domiciliarias (es decir, instituciones, corporaciones, fundaciones, fideicomisos, etc. que no realizan algún negocio comercial o de manufactura o alguna otra forma de operación comercial en el país donde se localiza su oficina registrada.
 12. Las instituciones financieras deben mantener, por lo menos por cinco años, todos los registros y transacciones necesarios, nacionales e internacionales, para permitirles cumplir rápidamente con solicitudes de información de las autoridades competentes. Dichos registros deben ser suficientes para permitir la reconstrucción de transacciones individuales (incluyendo las cantidades y tipos de moneda involucrados si los hubiera) para proveer, si es necesario, evidencia para procedimiento de comportamiento criminal.

Las instituciones financieras deben mantener registros sobre la identificación de clientes (por ej., copias o registros de documentos oficiales de identificación como pasaportes, tarjetas de identidad, licencias de conducir o documentos similares),

archivos de cuentas y correspondencia de negocios de por lo menos cinco años después de que la cuenta fue cerrada.

Estos documentos deben estar disponibles a las autoridades competentes nacionales en el contexto de procedimientos e investigaciones criminales relevantes.

13. Los países deben prestar atención especial a las amenazas de lavado de dinero inherentes en las nuevas tecnologías que pueden favorecer el anonimato, y tomar medidas, si es necesario, para prevenir su uso en los esquemas de lavado de dinero.

Diligencia Incrementada de Instituciones Financieras

14. Las instituciones financieras deben prestar atención especial a todas las transacciones complejas grandes inusuales, y todos los patrones no comunes de transacciones, que no tienen una propósito legal aparente económico o visible. Los antecedentes y propósito de dichas transacción deben, tanto como sea posible, ser examinadas, los hallazgos deben estar establecidos en papel, 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 provienen de actividad criminal, se les debe requerir reportar rápidamente sus sospechas a las autoridades competentes.
16. Las instituciones financieras, sus directores, funcionarios y empleados deben estar protegidos por provisiones legales de responsabilidad civil o criminal por ruptura de cualquier restricción en la divulgación de información impuesta por contrato o por cualquier provisión legislativa, regulatoria o administrativa, aún no conocen precisamente lo que la actividad criminal subyacente fue, y sin considerar su alguna actividad ilegal realmente ocurrió.
17. Las instituciones financieras, sus directores, funcionarios y empleados no deben, o, cuando sea apropiado, no deben estar autorizados a, alertar a los clientes cuando la información relacionadas a ellos está siendo reportada a las autoridades competentes.
18. Las instituciones financieras que reportan sus sospechas deben cumplir con 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 administrativo, y procedimientos adecuados de protección para asegurar altos estándares cuando se contratan empleados.
 - (ii) un programa continuo de capacitación a empleados;
 - (iii) una función de auditoría para probar el sistema.