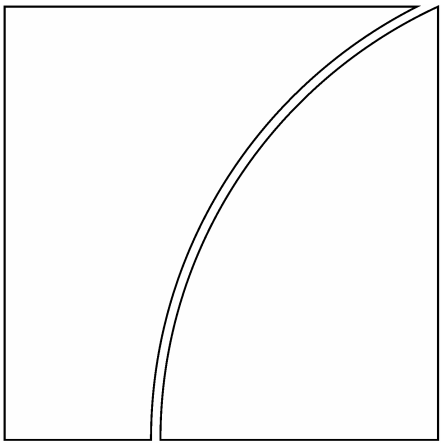
Comité de Supervisión Bancaria de Basilea



Gestión consolidada del riesgo *KYC*

Octubre de 2004

BANCO DE PAGOS INTERNACIONALES

Para obtener nuestras publicaciones y para inscribirse o darse de baja de nuestra lista de distribución, puede dirigirse a:

Banco de Pagos Internacionales
Press & Communications
CH-4002 Basilea (Suiza)

E-mail: publications@bis.org

Fax: +41 61 280 9100 y +41 61 280 8100

Índice

Introducción

1. La adopción de normas eficaces para "conocer a su clientela" (*KYC*, por las siglas en inglés de "*know your customer*") es parte esencial de las prácticas bancarias para la gestión del riesgo. Los bancos que cuentan con programas inadecuados para la gestión del riesgo *KYC* pueden tener que hacer frente a problemas significativos, relativos especialmente al riesgo legal y de reputación. Contar con políticas y procedimientos *KYC* adecuados no sólo contribuirá a la seguridad y solidez general del banco, sino que también protegerá la integridad del sistema bancario, al reducir la posibilidad de que los bancos se conviertan en instrumentos para blanquear dinero, financiar el terrorismo o realizar otras actividades ilegales. Las últimas iniciativas destinadas a fortalecer la lucha contra el terrorismo han puesto de relieve la importancia de la vigilancia que realizan los bancos de las operaciones de sus clientes.

2. En octubre de 2001, el Comité de Supervisión Bancaria de Basilea (BCBS) publicó un documento titulado *Debida diligencia con la clientela de los bancos*[1] (DDC), al que en febrero de 2003 se adjuntaron unas *Orientaciones para la apertura de cuentas y la identificación del cliente*. En el DDC se recogen cuatro elementos primordiales para la buena gestión de un programa *KYC*, a saber: (i) política de aceptación de clientes; (ii) identificación de clientes; (iii) seguimiento continuo de las cuentas de mayor riesgo; y (iv) gestión del riesgo. Estos principios han sido ampliamente aceptados y adoptados en las distintas jurisdicciones como punto de referencia para bancos comerciales y como mejores prácticas para otro tipo de instituciones financieras.

3. Al aplicar estas políticas y procedimientos, es muy importante considerar cómo se van a hacer extensivos a todo el grupo bancario. Dado que los riesgos legales y reputacionales identificados en el primer párrafo se presentan a escala internacional, resulta fundamental que cada grupo desarrolle un programa integral de gestión del riesgo, avalado por políticas que incorporen estándares *KYC* para el grupo en su totalidad. Así pues, las políticas y procedimientos que se apliquen en cada filial o sucursal habrán de ser congruentes y compatibles con las normas *KYC* del grupo, incluso cuando por motivos locales o empresariales estas políticas y procedimientos no sean idénticos a los que se siguen en todo el grupo[2].

4. Por gestión consolidada del riesgo *KYC* se entiende el proceso centralizado que se ha establecido para coordinar y promulgar políticas y procedimientos a escala del grupo, así como los sistemas sólidamente dispuestos para compartir información dentro del mismo. Estas políticas y procedimientos han de estar diseñados no sólo para cumplir al pie de la letra toda la legislación y regulación pertinente, sino también en un sentido más amplio, para identificar, vigilar y reducir los riesgos de reputación, de concentración, operativo y legal. Al igual que ocurre con los riesgos de crédito, de mercado y operativo, para controlar eficazmente el riesgo *KYC* en base consolidada es necesario que los bancos coordinen sus actividades de gestión de riesgos en todo el grupo, tanto en la sede central como entre las distintas filiales y sucursales.

5. El BCBS reconoce que la correcta aplicación de procedimientos *KYC* en todo el grupo resulta más complicada que para otros riesgos, ya que en la mayoría de los casos el riesgo *KYC* atañe al pasivo (y no al activo) del balance de situación del banco, así como a los saldos que se contabilizan como partidas fuera de balance. En aras de la privacidad, algunas jurisdicciones continúan restringiendo la capacidad de sus bancos para revelar el nombre de sus clientes y el saldo de sus pasivos, mientras que apenas hay países que en la actualidad mantengan barreras similares con respecto al activo del balance de situación. A la hora de realizar un seguimiento eficaz del grupo en su conjunto, es esencial que los bancos gocen de total libertad para que, siempre bajo una adecuada protección jurídica, la información sobre sus pasivos y activos llegue no sólo a su sede central o banco matriz, sino también a sus filiales y sucursales. Las condiciones para lograr todo ello quedan establecidas en los párrafos 20 a 23.

---

[1] Comité de Supervisión Bancaria de Basilea, octubre de 2001.

[2] El término "grupo" se emplea aquí en el sentido de una organización formada por uno o más bancos, así como las filiales y sucursales que lo componen. Por su parte, el término "sede central" se utiliza para hacer referencia al banco matriz o a la unidad en la que se lleva a cabo la gestión del riesgo *KYC* para toda una línea de negocios.

6. Las distintas jurisdicciones deberán facilitar la gestión consolidada del riesgo *KYC* mediante un marco jurídico adecuado que permita el intercambio transfronterizo de información. Asimismo, deberá eliminarse cualquier obstáculo jurídico que impida una adecuada gestión consolidada del riesgo *KYC*.

Proceso integral para la gestión del riesgo *KYC*

7. Los cuatros elementos fundamentales para crear un programa *KYC* adecuado deberán incorporarse a los procesos con los que cuenta el banco para gestionar y controlar sus riesgos, para asegurar que todos los aspectos relacionados con el riesgo *KYC* han sido identificados y mitigados. Así pues, los bancos deberán aplicar en todas sus filiales y sucursales las mismas técnicas de gestión de riesgos, las mismas políticas y procedimientos de aceptación e identificación de clientes y los mismos procesos de seguimiento de las cuentas, tanto dentro como fuera de sus fronteras. No se deberán escatimar esfuerzos a la hora de asegurar que los componentes del grupo puedan obtener y analizar la información que necesiten de conformidad con sus normas *KYC* internacionales, sin que pueda afectarles la modificación de políticas o procedimientos locales a instancias jurídicas locales. A este respecto, los bancos deberán contar con un sólido sistema de intercambio de información entre la sede central y todas sus filiales y sucursales. Cuando existan divergencias entre los requisitos *KYC* que impone el país en el que se ubica la sede central y el país en el que se encuentra alguna de sus filiales o sucursales, deberá aplicarse el estándar más estricto de los dos, respetando siempre la consigna recogida en el párrafo 66 del documento DDC.

Gestión de riesgos

8. Los programas de gestión del riesgo *KYC* para todo el grupo incluirán sistemas y controles adecuados para la vigilancia gerencial, segregación de responsabilidades, formación y otras políticas relacionadas (véase el párrafo 55 de DDC). Además, dicho programa deberá aplicarse a escala mundial. Las responsabilidades dentro del banco habrán de distribuirse de manera explícita para asegurar que las políticas y procedimientos para la gestión del riesgo se llevan a cabo con eficacia y resultan conformes con las normas generales del banco para la identificación de clientes, el seguimiento continuo de sus cuentas y operaciones, así como el intercambio de información.

9. El personal del banco encargado de comprobar el cumplimiento de la normativa y realizar auditorías internas (o los auditores externos en su caso) deberán evaluar la adherencia del grupo a las normas *KYC* en todos sus aspectos, incluida la eficacia de las funciones para la gestión *KYC* centralizada y los requisitos para intercambiar información con otros miembros del grupo y para responder a preguntas de la sede central. Los grupos bancarios internacionales necesitan tanto una función de auditoría interna como otra para el cumplimiento internacional de la normativa, pues suelen ser los principales mecanismos (y en ocasiones, los únicos) para comprobar la aplicación de las normas *KYC* en todo el banco y para avalar sus políticas y procedimientos, incluida su eficacia para compartir la información en el seno del grupo.

Política para la aceptación e identificación de clientes

10. Cada banco deberá desarrollar políticas y procedimientos claros para la aceptación de clientes, donde se incluya información sobre qué tipo de clientes tiene tendencia a plantear más riesgo de lo habitual (véase el párrafo 20 de DDC); cuando sea necesario, podrá contemplarse la intervención de la dirección del banco para estudiar la aceptación de cada uno de estos clientes.

11. Igualmente, el banco deberá establecer un procedimiento sistemático basado en el riesgo para comprobar la identidad de nuevos clientes (véase el párrafo 22 de DDC). Para ello, establecerá pautas sobre qué datos habrá que obtener y conservar para la identificación de clientes en todo el mundo, imponiendo requisitos de debida diligencia más estrictos para aquellos clientes que planteen más riesgo.

12. El banco tendrá que ser capaz de conseguir los oportunos datos identificativos y conservarlos en un formato de acceso inmediato, para poder así identificar adecuadamente a sus clientes[3], cumpliendo al mismo tiempo con cualquier requisito de información impuesto por las autoridades locales. Para el intercambio de datos, tanto la sede central como las filiales y sucursales del grupo bancario deberán tener acceso a cualquier información que resulte pertinente. Asimismo, cada oficina tendrá que cumplir con las normas mínimas sobre identificación y accesibilidad que se apliquen en la sede.

13. Estas normas para la aceptación e identificación de clientes y para el archivo de sus datos deberán aplicarse mediante políticas y procedimientos coherentes en toda la organización, ajustándolos cuando sea necesario para tener en cuenta los distintos niveles de riesgo en las diferentes líneas de negocio y áreas geográficas. Asimismo, puede resultar necesaria la aplicación de diferentes modelos para obtener y conservar la información en cada jurisdicción de conformidad con los requisitos reguladores locales o con los factores de riesgo relativos.

Seguimiento de cuentas y operaciones

14. Para hacer frente a riesgos mayores, es esencial vigilar los movimientos de las cuentas bancarias de una manera coordinada en todo el grupo, independientemente de si las posiciones se mantienen dentro o fuera de balance, si son activos en gestión o se administran en fideicomiso (véase el párrafo 16 de DDC). Así pues, los bancos deberán contar con normas que les permitan realizar un seguimiento de operaciones potencialmente sospechosas en las cuentas de sus clientes, aplicando en todas sus filiales y sucursales las políticas y procedimientos que estimen oportuno, las cuales deberán basarse en el riesgo y enfatizar la necesidad de vigilar cualquier operación significativa dentro de la propia cuenta o hacia otra cuenta.

15. Cada oficina deberá mantener y vigilar la información que posee sobre sus cuentas y operaciones, a lo que deberá añadirse un sólido proceso de intercambio de información entre la sede central y sus filiales y sucursales a propósito de aquellas cuentas y operaciones que puedan plantear mayores riesgos.

16. En los últimos años, muchos bancos han comenzado a centralizar algunos de sus sistemas de procesamiento de información y bases de datos con el fin de mejorar su gestión interna del riesgo o su eficiencia en general. En tales casos, los bancos deberían añadir a la vigilancia que realizan a escala local el seguimiento de operaciones realizadas en la base centralizada. De este modo, los bancos tienen la oportunidad de detectar patrones de comportamiento sospechoso que no podrían haberse descubierto desde su base local.

Intercambio de información en todo el grupo

17. Los bancos deberán centralizar la coordinación del intercambio de información en todo el grupo. Habrá que exigir que tanto filiales como sucursales faciliten a iniciativa propia datos relacionados con clientes y actividades de alto riesgo que resulten pertinentes para la gestión integral del riesgo jurídico y de reputación, al tiempo que se les instará a responder de manera oportuna a cualquier solicitud de información sobre cuentas que les remita la sede central o el banco matriz. Las políticas y procedimientos del banco deberán incluir una descripción del proceso a seguir para investigar e informar sobre actividades potencialmente sospechosas.

18. La función centralizada encargada de la gestión *KYC* deberá evaluar los riesgos que podrían presentar las actividades sobre las que le han informado sus filiales y sucursales, estimando cuando sea necesario su grado de exposición a un determinado cliente a escala internacional. Los

[3] Véanse los requisitos para la identificación de clientes recogidos en las *Orientaciones para la apertura de cuentas y la identificación del cliente*, documento adjunto a *Debida diligencia con la clientela de los bancos*, publicado por el Comité de Basilea (octubre de 2001).

bancos deberán contar con políticas y procedimientos que le permitan determinar si dicho cliente mantiene cuentas en otras filiales o sucursales y evaluar los riesgos de reputación, de concentración y legal para el conjunto del grupo. Asimismo, deberá disponer de procedimientos que rijan las cuentas internacionales consideradas potencialmente sospechosas, donde se detallen procedimientos de reajuste y pautas para restringir su actividad, incluido el cierre de la cuenta si fuera necesario.

19. Asimismo, los bancos y sus oficinas locales deberían mostrarse cooperativos ante cualquier petición de información sobre el titular de alguna de sus cuentas que puedan remitirle sus respectivas fuerzas de orden público, con el fin de luchar contra el blanqueo de dinero y la financiación del terrorismo. Igualmente, la oficina central ha de poder exigir a sus oficinas locales que busquen en sus archivos el nombre de cualquier organización o individuo sospechoso de colaboración o participación delictiva en dichas actividades fraudulentas, y que le informen de sus resultados.

La labor del supervisor

20. Los supervisores comprobarán que en el banco existen controles internos adecuados para el riesgo *KYC* y que éstos son conformes a las pautas actuales de supervisión y regulación. El proceso de supervisión incluirá no sólo la evaluación de políticas y procedimientos, sino también el examen de archivos de clientes y el muestreo de cuentas (véase el párrafo 61 de DDC).

21. En un contexto transfronterizo, cuando los supervisores del país de origen[4] realicen inspecciones *in situ* en otro país, deberán estar exentos de todo obstáculo que les impida comprobar que sus filiales o sucursales cumplen las políticas y procedimientos *KYC* para todo el grupo. Durante estas inspecciones, podría ser necesario consultar datos de los clientes o realizar un muestreo de cuentas, por lo que los supervisores del país de origen deben tener acceso a la información sobre las cuentas de los clientes seleccionados, en la medida en que sea necesario para evaluar el cumplimiento de las normas *KYC* y de las prácticas de gestión de riesgo, sin impedimento de ningún tipo por parte de la legislación local sobre secreto bancario. En el caso de filiales o sucursales de grupos bancarios internacionales, el supervisor del país de acogida continúa siendo el responsable de comprobar el cumplimiento de la regulación *KYC* local, lo que podría incluir una evaluación de la pertinencia de los procedimientos empleados.

22. La función del auditor es de enorme importancia para comprobar la observancia de las normas *KYC* en base consolidada, por lo que los supervisores del país de origen deberán asegurarse de que la frecuencia, los recursos y los procedimientos de las auditorías son adecuados y que los auditores gozan de total acceso a cualquier informe pertinente o a documentos de trabajo que hayan sido elaborados a lo largo del proceso de auditoría.

23. Son necesarias medidas de salvaguardia que garanticen que la información sobre las cuentas goza del mismo grado de confidencialidad que se aplica a otros datos recabados durante la supervisión. En este sentido, podría resultar útil una declaración de cooperación mutua que facilite el intercambio de información entre los dos supervisores (véase el párrafo 68 de DDC).

Impedimentos de naturaleza jurídica

24. A pesar de que la mayoría de jurisdicciones dispone de canales para que los bancos puedan intercambiar con sus sedes centrales información necesaria para la gestión de sus riesgos, algunos países poseen rigurosas leyes sobre el secreto bancario o sobre protección de información que impiden, o puede interpretarse que impiden, la transferencia de dichos datos. En tales circunstancias, las oficinas extranjeras de estos bancos pueden adoptar una postura cauta con respecto a la transferencia de información hacia sus sedes centrales, lo cual podría interferir en la gestión consolidada del riesgo *KYC*.

[4] En aquellos países en los que las inspecciones las realicen auditores externos, esta exención se aplicará a los auditores competentes a tal efecto.

25. Es primordial que todas las jurisdicciones en las que estén radicados bancos extranjeros se doten de un ordenamiento jurídico que permita transmitir la información necesaria para la gestión del riesgo *KYC* tanto a la oficina central o banco matriz como a los supervisores del país de origen. Igualmente, no deberán existir impedimentos a las inspecciones *in situ* de auditores de la sede central, de responsables de la gestión del riesgo, de agentes del cumplimiento o de supervisores del país de origen, ni tampoco restricciones a su capacidad de acceder a cualquier archivo de la oficina local, incluidos nombres de clientes y saldos en sus cuentas. Este acceso será el mismo tanto para filiales como sucursales. Si los obstáculos al intercambio de información resultaran insuperables y no hubiera alternativa posible, el supervisor de origen deberá informar al supervisor de destino de que el banco podría poner fin a su actividad por decisión propia o por requerimiento del supervisor de origen (véase el párrafo 69 de DDC).

26. Cuando el personal de la sede central del banco pueda acceder a información sobre clientes locales, no podrá prohibírsele que la transmita a la sede central. Dicha información deberá estar sujeta a la legislación sobre privacidad y privilegios del país de origen.

27. Bajo las condiciones antes mencionadas, el BCBS considera que no puede justificarse en modo alguno que la legislación local prohíba que una filial o sucursal transmita a su sede central o banco matriz información sobre sus clientes que esté destinada a la gestión del riesgo. Cuando la legislación en vigor restrinja la divulgación de información a terceros, es fundamental que la sede central o banco matriz quede fuera del ámbito que cubre la definición de “terceros”. Se insta a que aquellas jurisdicciones cuya legislación impida (o pueda interpretarse que impide) este tipo de intercambio de información eliminen dichas restricciones y proporcionen los canales de comunicación necesarios a tal efecto.

Grupos financieros mixtos

28. Muchos grupos bancarios también prestan en la actualidad servicios de contratación de valores y seguros. La debida diligencia con la clientela que debe seguir este tipo de entidades plantea cuestiones a las que pueden ser ajenos los grupos bancarios en sentido estricto. Así pues, estos grupos mixtos deberán contar con sistemas y procesos que les permitan recabar y compartir información sobre la identidad de sus clientes y la actividad de sus cuentas en todo el grupo, debiendo estar alerta ante clientes que utilicen sus servicios en distintos sectores, pues cualquier percance con un cliente en una parte del grupo podría acabar dañando la reputación del grupo en su conjunto.

29. Así como la variedad de actividades y las diferencias en las relaciones que mantiene cada institución con sus clientes justifican distintos requisitos *KYC* para cada sector, el grupo bancario deberá ser consciente de que, cuando venda productos y servicios a clientes de otros países a través de sus diferentes ramas de actividad, habrá de aplicar los requisitos *KYC* que correspondan a cada sector.