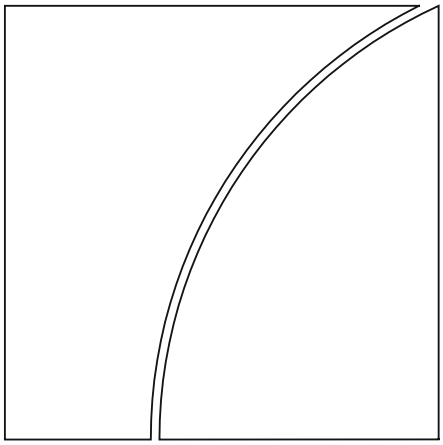
Comité de Supervisión Bancaria de Basilea



Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo

Enero de 2014

BANCO DE PAGOS INTERNACIONALES

Este documento ha sido redactado en inglés. En caso de duda, consúltese la versión inglesa.

Esta publicación también puede consultarse en la página web del BPI (www.bis.org).

ISBN 92-9131-530-3 (versión impresa)

ISBN 92-9197-530-3 (versión en línea)

Índice

Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo

I. Introducción

1. Consciente de los riesgos que asumen los bancos de ser utilizados, deliberadamente o no, en actividades delictivas, el Comité de Supervisión Bancaria de Basilea publica las presentes directrices sobre la forma en que los bancos deberán incluir el blanqueo de capitales (BC) y la financiación del terrorismo (FT) dentro de su gestión global del riesgo.

2. El Comité se comprometió hace tiempo a promover la aplicación de sólidas políticas y procedimientos de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo (PBC/FT), que son fundamentales para proteger la seguridad y solvencia de los bancos y la integridad del sistema financiero internacional. Tras un primer comunicado en 1988[1], el Comité ha publicado varios documentos secundando este compromiso. En septiembre de 2012, el Comité reiteró su postura publicando la versión revisada de los *Principios básicos para una supervisión bancaria eficaz*, cuyo Principio 29 está dedicado a la utilización abusiva de servicios financieros.

3. El Comité apoya la adopción de las normas emitidas por el Grupo de Acción Financiera Internacional (GAFI)[2]. En febrero de 2012, el GAFI publicó una versión revisada de *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (normas internacionales GAFI para combatir el blanqueo de capitales, la financiación del terrorismo y la proliferación de armas de destrucción masiva), a las cuales contribuyó el Comité[3]. Asimismo, en marzo de 2013, el GAFI publicó sus orientaciones sobre inclusión financiera (*Financial Inclusion Guidance*), que el Comité también ha tomado en consideración al redactar sus directrices. Con la publicación del presente documento, el Comité pretende coadyuvar a la aplicación nacional de las normas GAFI explorando áreas complementarias y aprovechando las capacidades de ambas organizaciones. Estas directrices incorporan tanto las normas GAFI como los Principios Básicos de Basilea aplicables a los bancos con operativa transfronteriza y se integran en el marco general de la supervisión bancaria. Así pues, estas directrices pretenden complementar y ser congruentes con los objetivos y metas de las normas GAFI, y en ningún caso deberán interpretarse como modificaciones de dichas normas, ya sea porque las refuercen o debiliten.

4. En ciertas partes de este documento, el Comité ha incluido referencias cruzadas a las normas GAFI para facilitar a los bancos el cumplimiento de los requisitos nacionales basados en la aplicación de

[1] Véase BCBS, *Prevention of criminal use of the banking system for the purpose of money-laundering*, diciembre de 1988, disponible en www.bis.org/publ/bcbsc137.pdf.

[2] El GAFI es un organismo intergubernamental que desarrolla normas internacionales y promueve políticas para proteger al sistema financiero internacional contra el blanqueo de capitales, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva. El GAFI define el blanqueo de capitales como el reciclado de fondos procedentes de actividades delictivas para ocultar su origen ilícito. El GAFI trabaja en estrecha colaboración con otras entidades involucradas en estos temas, en particular con sus miembros asociados y observadores. El Comité tiene estatus de observador en el GAFI.

[3] El Anexo 3 enumera algunas de las Recomendaciones más relevantes del GAFI que bancos y supervisores deberán cumplir cuando apliquen sus medidas PBC/FT. Ese listado no es exhaustivo, por lo que otras Recomendaciones del GAFI, incluidas las Notas Interpretativas, podrían ser pertinentes. La versión íntegra del documento está disponible en www.fatf-gafi.org/recommendations.

dichas normas. Sin embargo, dado que el objetivo del Comité no es la mera duplicación de las actuales normas GAFI, la inclusión de esas referencias cruzadas no es sistemática.

5. El compromiso del Comité con la lucha contra el blanqueo de capitales y la financiación del terrorismo está en plena consonancia con su mandato para «mejorar la regulación, la supervisión y las prácticas bancarias en todo el mundo con el fin de afianzar la estabilidad financiera»[4]. Una sólida gestión del riesgo BC/FT tiene especial relevancia para la seguridad y solvencia generales de los bancos y del sistema bancario, el principal objetivo de la supervisión bancaria, dado que:

- contribuye a proteger la reputación tanto de los bancos como de los sistemas bancarios nacionales al evitar y disuadir la utilización de entidades bancarias para blanquear fondos procedentes de actividades ilícitas o para captar o movilizar financiación en apoyo del terrorismo; y
- preserva la integridad del sistema financiero internacional, así como las actuaciones de los gobiernos para combatir la corrupción y la financiación del terrorismo.

6. La insuficiencia o ausencia de una sólida gestión del riesgo BC/FT plantea graves riesgos a los bancos, en especial riesgos de reputación, operacional, de cumplimiento y de concentración. Recientes acontecimientos, incluidas las robustas medidas adoptadas por los reguladores para hacer cumplir las normas y los correspondientes costes directos e indirectos en que han incurrido los bancos debido a su falta de diligencia en la aplicación de las adecuadas políticas, procedimientos y controles para la gestión del riesgo, han acentuado esos riesgos. Probablemente, estos costes y perjuicios podrían haberse evitado si los bancos hubieran aplicado unas eficaces políticas y procedimientos PBC/FT en función del riesgo.

7. Cabe señalar que todos estos riesgos están relacionados entre sí. Sin embargo, aparte de conllevar multas y sanciones impuestas por los reguladores, cualquiera de ellos podría ocasionar un considerable coste financiero para los bancos (por ejemplo, a raíz del cese de la financiación y de facilidades financieras en mercados mayoristas, las demandas interpuestas contra el banco, los gastos de investigación, la confiscación y embargo de activos, y los préstamos incobrables), así como la necesidad de dedicar tiempo de gestión y recursos operativos, que son limitados y valiosos, a resolver los problemas que surgen.

8. En consecuencia, este documento deberá leerse conjuntamente con una serie de documentos relacionados del Comité, incluidos los siguientes:

- *Principios básicos para una supervisión bancaria eficaz*, septiembre de 2012[5]
- *The internal audit function in banks*, junio de 2012[6]
- *Principles for the sound management of operational risk*, junio de 2011[7]
- *Principles for enhancing corporate governance*, octubre de 2010[8]

[4] Véase Comité de Supervisión Bancaria de Basilea, *Carta estatutaria*, enero de 2013, disponible en www.bis.org/bcbs/charter_es.pdf.

[5] Accesible en: www.bis.org/publ/bcbs230_es.pdf.

[6] Accesible en: www.bis.org/publ/bcbs223.pdf.

[7] Accesible en: www.bis.org/publ/bcbs195.pdf.

[8] Accesible en: www.bis.org/publ/bcbs176.pdf.

- *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*, mayo de 2009[9]
- *Compliance and the compliance function in banks,* abril de 2005[10]

9. Con el fin de racionalizar las publicaciones del Comité sobre directrices en materia de PBC/FT, este documento fusiona y sustituye a dos publicaciones previas del Comité sobre cuestiones relacionadas: *Debida diligencia con la clientela de los bancos*, (octubre de 2001) y *Gestión consolidada del riesgo KYC* (octubre de 2004). Al actualizar estos documentos, el Comité ha prestado asimismo una mayor atención a los riesgos asociados a la utilización de terceros por parte de los bancos para presentar negocios (véase Anexo 1) y a la prestación de servicios de corresponsalía bancaria (véase Anexo 2). Pese a su importancia y relevancia, otros ámbitos de riesgo específico abordados en documentos previos —como personas del medio político (PEP), banca privada y estructuras jurídicas singulares— no se desarrollan específicamente en estas directrices, por ser ya objeto de tratamiento en otras publicaciones del GAFI[11].

10. Con respecto al ámbito de aplicación, estas directrices deberán leerse conjuntamente con otras normas y orientaciones elaboradas por el Comité para promover la supervisión de grupos bancarios a escala consolidada[12]. Esto es particularmente relevante en el contexto de PBC/FT ya que los clientes con frecuencia tienen múltiples relaciones y/o cuentas con el mismo grupo bancario, pero en oficinas ubicadas en diferentes países.

11. Estas directrices resultan aplicables a todos los bancos. Algunos de los requisitos podrán requerir una adaptación a instituciones pequeñas o especializadas, para adecuarse a su tamaño o a sus modelos de negocio concretos. No obstante, tales ajustes desbordan el alcance de este documento orientativo.

12. Estas directrices se dirigen específicamente a bancos, grupos bancarios (partes II y III, respectivamente) y supervisores bancarios (parte IV). Como establece el Principio Básico 29, el Comité es consciente de la variedad de mecanismos nacionales existentes para garantizar el cumplimiento de LBC/FT, en particular el reparto de las funciones supervisoras entre supervisores bancarios y otras autoridades, como unidades de inteligencia financiera[13]. Así pues, a efectos de estas directrices, la referencia al «supervisor» puede extenderse a esas autoridades. En jurisdicciones donde la autoridad supervisora en materia LBC/FT es compartida, el supervisor bancario coopera con otras autoridades para procurar el cumplimiento de estas directrices.

13. Cabe señalar que en este documento no se tratan las normas GAFI que exigen a los países aplicar otras medidas en sus sectores financieros y en otros sectores no financieros específicos, o determinar las atribuciones y responsabilidades de las autoridades competentes.

9 Accesible en: www.bis.org/publ/bcbs154.pdf.

10 Accesible en: www.bis.org/publ/bcbs113.pdf.

11 Véase en particular, *FATF Guidance on Politically Exposed Persons* (Recomendaciones 12 y 22), disponible en http://www.fatf-gafi.org/fr/documents/documents/peps-r12-r22.html.

12 Véase, por ejemplo, el Principio 12 de los *Principios básicos para una supervisión bancaria eficaz*, septiembre de 2012.

13 Las unidades de inteligencia financiera se describen en la Recomendación 26 de las normas GAFI.

II. Elementos esenciales de una sólida gestión del riesgo BC/FT

14. Con arreglo a la actualización de los *Principios básicos para una supervisión bancaria eficaz* (2012), todos los bancos estarán obligados a «contar con políticas y procesos adecuados, incluidas estrictas reglas de debida diligencia con la clientela (CDD), para promover normas éticas y profesionales de alto nivel en el sector bancario e impedir que el banco sea utilizado, intencionalmente o no, con fines delictivos»[14]. Este requisito debe considerarse una parte concreta de la obligación general de los bancos de contar con sólidos programas de gestión del riesgo para tratar toda clase de riesgos, incluidos los riesgos BC y FT. En este contexto, disponer de «políticas y procesos adecuados» exige la aplicación de otras medidas adicionales a unas normas CDD eficaces. Estas medidas también deberán ser proporcionadas y estar en función del riesgo, e informadas por la propia evaluación que los bancos hacen de los riesgos BC/FT. Este documento presenta directrices sobre estas medidas. Además, cuando no existan orientaciones específicas en materia de PBC/FT, resultan aplicables o complementarias otras directrices (véase el párrafo 8 anterior).

1. Evaluación, comprensión, gestión y mitigación de riesgos

(a) Evaluación y comprensión de los riesgos

15. Una sólida gestión del riesgo[15] exige la identificación y el análisis de los riesgos BC/FT presentes en el banco y el diseño y la eficaz aplicación de políticas y procedimientos acordes con los riesgos identificados. Al realizar un análisis integral del riesgo para evaluar los riesgos BC/FT, el banco deberá considerar todos los factores de riesgo relevantes, inherentes y residuales, a escala nacional[16], sectorial, bancaria y de relación comercial, entre otras, para determinar su perfil de riesgo y el adecuado nivel de mitigación que se aplicará. Así pues, las políticas y procedimientos en materia de CDD, aceptación de clientes, identificación de clientes y seguimiento de relaciones comerciales y operaciones (productos y servicios ofrecidos) deberán tener en cuenta la evaluación del riesgo y el resultante perfil de riesgo del banco. El banco deberá disponer de mecanismos adecuados para documentar y notificar información sobre la evaluación del riesgo a las autoridades competentes, como los supervisores.

16. El banco deberá desarrollar un conocimiento minucioso de los riesgos BC/FT inherentes a su base de clientes, productos, canales de distribución y servicios ofrecidos (incluidos los productos en desarrollo o en fase de lanzamiento) y en las jurisdicciones en las que él o sus clientes realizan negocios. Este conocimiento deberá basarse en datos concretos de operaciones y transacciones y en otra información interna recogida por el banco, así como en fuentes de información externa, como evaluaciones del riesgo de ámbito nacional e informes sobre países elaborados por organismos internacionales. Las políticas y procedimientos en materia de aceptación de clientes, diligencia debida y seguimiento continuo deberán diseñarse y aplicarse para controlar adecuadamente esos riesgos inherentes identificados. Cualquier riesgo residual resultante deberá gestionarse en consonancia con el perfil de riesgo del banco establecido a partir de su evaluación del riesgo. Esta evaluación y conocimiento deberán poder demostrarse a petición del supervisor del banco y ser de su entera satisfacción.

[14] Véase el Principio 29 de los *Principios básicos para una supervisión bancaria eficaz*, septiembre de 2012.

[15] Véase, en particular, el Principio 15 de los *Principios básicos para una supervisión bancaria eficaz,* septiembre de 2012, así como el Principio 6 de los *Principles for enhancing corporate governance*, octubre de 2010.

[16] Cuando proceda, deberán tenerse en cuenta las evaluaciones del riesgo PBC/FT a escala supranacional.

(b) Mecanismos de gobierno adecuados

17. Una eficaz gestión del riesgo BC/FT exige unos mecanismos de gobierno adecuados, conforme se describe en las pertinentes publicaciones previas del Comité[17]. En particular, el requisito de que el Consejo de Administración apruebe y supervise las políticas en materia de riesgos, gestión del riesgo y cumplimiento es totalmente relevante en el contexto del riesgo BC/FT. El Consejo de Administración deberá comprender claramente los riesgos BC/FT. La información sobre la evaluación del riesgo BC/FT deberá comunicarse al Consejo de forma puntual y oportuna, completa, comprensible y precisa, a fin de capacitarlo para adoptar decisiones informadas.

18. El Consejo de Administración deberá asignar las competencias explícitas teniendo realmente en cuenta la estructura de gobierno del banco para garantizar la gestión eficaz de las políticas y procedimientos de la entidad. El Consejo de Administración y la alta dirección deberán nombrar un responsable ejecutivo de PBC/FT con la preparación adecuada para asumir las competencias generales de esa función y con la categoría y autoridad necesarias dentro del banco para que las cuestiones planteadas por este directivo reciban la necesaria atención del Consejo, la alta dirección y las líneas de negocio.

(c) Las tres líneas de defensa

19. Como regla general y en el contexto PBC/FT, las unidades de negocio (por ejemplo, las actividades de cara al público y en contacto directo con los clientes) constituyen la primera línea de defensa encargada de identificar, evaluar y controlar los riesgos de sus actividades. Estas unidades deberán conocer y aplicar las políticas y procedimientos y disponer de recursos suficientes para realizar eficazmente estas tareas. La segunda línea de defensa incluye al responsable ejecutivo de PBC/FT y a la función de cumplimiento de la normativa, así como también las de recursos humanos o tecnología. El departamento de auditoría interna constituye la tercera línea de defensa.

20. Como parte de **la primera línea de defensa**, las políticas y procedimientos deberán especificarse claramente por escrito y comunicarse a todo el personal. Deberán incluir una descripción clara de las obligaciones de los empleados y de las instrucciones que deben seguir, así como orientaciones para que la actividad del banco cumpla las regulaciones. Deberán existir procedimientos internos para detectar y notificar transacciones sospechosas.

21. El banco deberá disponer de políticas y procesos adecuados para seleccionar a su personal, presente y futuro, a fin de garantizar unos elevados principios éticos y profesionales. Todos los bancos deberán implantar programas de formación del personal de modo que sus empleados estén adecuadamente capacitados para aplicar las políticas y procedimientos PBC/FT de la entidad. El banco deberá adaptar la programación y contenido de la formación para el personal de las distintas secciones con arreglo a sus necesidades y al perfil de riesgo de la entidad. Las necesidades de formación variarán dependiendo de las funciones de los empleados y de las responsabilidades de los distintos puestos de trabajo, así como de la antigüedad en el banco. La organización y los materiales de los cursos de formación deberán adaptarse a la responsabilidad o función concreta de cada empleado con el fin de garantizar que éste cuenta con suficientes conocimientos e información para aplicar eficazmente las políticas y procedimientos PBC/FT del banco. Por estos mismos motivos, los nuevos empleados deberán recibir formación tan pronto como sea posible tras su contratación. Deberán impartirse cursos de actualización para garantizar que el personal recuerda sus obligaciones y que sus conocimientos y destrezas se mantienen al día. El alcance y frecuencia de esta formación deberán adaptarse a los factores

[17] Véanse, en particular, *The internal audit function in banks*, junio de 2012; *Principles for enhancing corporate governance*, octubre de 2010; *Compliance and the compliance function in banks*, abril de 2005.

de riesgo a los que los empleados se encuentren expuestos a tenor de sus responsabilidades y al nivel y naturaleza del riesgo presente en el banco.

22. Como parte de **la segunda línea de defensa**, el responsable ejecutivo de PBC/FT deberá hacerse responsable de un seguimiento continuo del cumplimiento de todas las obligaciones en materia de PBC/FT por parte del banco. Esto implica la verificación por muestreo del cumplimiento de la normativa y un examen de los informes de anomalías para alertar a la alta dirección o al Consejo de Administración si se considera que la dirección no está aplicando los procedimientos PBC/FT de forma responsable. El responsable ejecutivo de PBC/FT deberá ser el contacto para todas las cuestiones en esa materia de las autoridades internas y externas, incluidas las autoridades supervisoras o las unidades de inteligencia financiera (FIU).

23. Los intereses comerciales del banco no deberán oponerse en absoluto al eficaz desempeño de las atribuciones anteriormente mencionadas del responsable ejecutivo de PBC/FT. Con independencia del tamaño del banco o de su estructura directiva, deberán evitarse posibles conflictos de intereses. Así pues, para permitir juicios ecuánimes y facilitar un asesoramiento imparcial a la dirección, el responsable ejecutivo de PBC/FT no deberá, por ejemplo, asumir competencias en las líneas de negocio ni en el contexto de protección de datos o en la función de auditoría interna. Ante cualquier conflicto entre las líneas de negocio y las atribuciones del responsable ejecutivo de PBC/FT, deberán existir procedimientos que garanticen que las cuestiones de PBC/FT reciben una consideración objetiva al más alto nivel.

24. El responsable ejecutivo de PBC/FT también podrá desempeñar la función de director de riesgos, director de cumplimiento o equivalente. Este responsable deberá rendir cuentas directamente a la alta dirección o al Consejo. En caso de separación de tareas, la relación entre los directores previamente citados y sus respectivas funciones deberá definirse y conocerse con claridad.

25. Al responsable ejecutivo de PBC/FT también deberá atribuírsele la responsabilidad de notificar las transacciones sospechosas. Asimismo, deberá contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el régimen PBC/FT del banco. Para ello, deberá estar plenamente familiarizado con dicho régimen, sus requisitos legales y reglamentarios y los riesgos BC/FT derivados del negocio.

26. **La auditoría interna, la tercera línea de defensa,** desempeña una función importante al evaluar de forma independiente la gestión y los controles del riesgo, rindiendo cuentas al comité de auditoría del Consejo de Administración o un órgano de vigilancia similar mediante evaluaciones periódicas de la eficacia del cumplimiento de las políticas y procedimientos PBC/FT. El banco deberá implantar políticas para la realización de auditorías sobre (i) la adecuación de las políticas y procedimientos PBC/FT del banco para tratar los riesgos identificados; (ii) la eficacia de la aplicación de las políticas y procedimientos del banco por parte del personal; (iii) la eficacia de la vigilancia del cumplimiento y del control de calidad, incluyendo parámetros o criterios de alerta automática; y (iv) la eficacia de los programas de formación del personal relevante del banco. La alta dirección deberá garantizar que a las funciones de auditoría se les asigna personal experto en la materia y con la experiencia adecuada para realizar dichas auditorías. La dirección también deberá garantizar que el alcance y la metodología de las auditorías se adecuan al perfil de riesgo del banco y que la frecuencia de dichas auditorías depende asimismo del riesgo. Periódicamente, los auditores internos deberán realizar auditorías PBC/FT de todo el banco. Además, los auditores internos deberán mostrar iniciativa en el seguimiento de los resultados de su trabajo y sus recomendaciones[18]. Como regla general, los procesos utilizados en las auditorías deberán ser congruentes con el mandato general de la función de auditoría

[18] Véase BCBS, *The internal audit function in banks*, junio de 2012.

interna, estando sujetos a cualquier requisito preceptivo en materia auditora aplicable a las medidas PBC/FT.

27. En numerosos países, los **auditores externos** también desempeñan una importante función al evaluar los controles y procedimientos internos de los bancos en el curso de sus auditorías financieras, y al confirmar que cumplen las regulaciones y prácticas de supervisión en materia de PBC/FT. En los casos en que el banco utilice auditores externos para evaluar la eficacia de las políticas y procedimientos PBC/FT, deberá garantizar que el alcance de la auditoría se adecua a los riesgos del banco y que los auditores asignados a estas labores disponen de los conocimientos y experiencia necesarios. El banco también deberá garantizar que realiza un adecuado seguimiento de dichas labores.

(d) Adecuado sistema de seguimiento de transacciones

28. El banco deberá disponer de un sistema de seguimiento acorde con su tamaño, sus actividades y complejidad, así como con los riesgos presentes en la entidad. En la mayoría de los bancos, especialmente en aquéllos con actividad internacional, un seguimiento eficaz requerirá probablemente la automatización del proceso de seguimiento. Cuando el banco considere que un sistema de seguimiento basado en tecnologías de la información (TI) no es necesario en su situación concreta, deberá documentar su decisión y ser capaz de demostrar a su supervisor o a los auditores externos que dispone de una alternativa eficaz. Cuando se utilice un sistema TI, éste deberá incluir todas las cuentas de los clientes del banco y todas las transacciones en las que esos clientes sean ordenantes o beneficiarios. Este sistema deberá permitir al banco realizar un análisis de tendencias con los datos de transacciones e identificar relaciones comerciales y transacciones anómalas con el fin de prevenir BC o FT.

29. En particular, este sistema deberá ser capaz de ofrecer información fidedigna a la alta dirección sobre ciertos aspectos cruciales, incluidos cambios en el perfil de las transacciones realizadas por los clientes. Para elaborar el perfil del cliente, el banco deberá incorporar la información CDD actualizada, completa y fidedigna facilitada por el cliente. El sistema TI deberá permitir al banco, y al grupo cuando proceda, disponer de un repositorio centralizado de información (esto es, organizado por cliente, producto, entidades del grupo, transacciones realizadas durante un cierto intervalo de tiempo, etc.). Sin que se les exija disponer de un único archivo por cliente, los bancos deberán calificar a sus clientes en función del riesgo y gestionar alertas con toda la información relevante a su disposición. Un sistema de seguimiento TI deberá utilizar parámetros adecuados basados en la experiencia nacional e internacional sobre los métodos y la prevención de BC o FT. El banco podrá hacer uso de los parámetros estándar suministrados por el diseñador del sistema de seguimiento TI; sin embargo, los parámetros utilizados deberán reflejar y tener en cuenta la situación de riesgo específica del banco.

30. El sistema de seguimiento TI deberá permitir al banco determinar sus propios criterios para realizar seguimientos adicionales, elaborar informes de transacciones sospechosas (STR) o adoptar otras medidas para minimizar el riesgo. El responsable ejecutivo de PBC/FT deberá tener acceso al sistema TI y servirse de él en la medida en que sea relevante para su función (incluso si es gestionado o utilizado por otras líneas de negocio). Los parámetros del sistema TI deberán permitir la generación de alertas sobre transacciones anómalas, en cuyo caso también deberán someterse a ulterior evaluación por parte del responsable ejecutivo de PBC/FT. Cualquier criterio sobre riesgos utilizado en este contexto deberá estar en consonancia con la evaluación de riesgos del banco.

31. La auditoría interna también deberá evaluar el sistema TI para garantizar que es adecuado y que la primera y segunda líneas de defensa lo utilizan eficazmente.

2. Política de aceptación de clientes

32. El banco deberá desarrollar y aplicar políticas y procedimientos claros de aceptación de clientes para identificar los tipos de clientes susceptibles de plantear un mayor riesgo de BC y FT conforme a la

evaluación de riesgos del banco[19]. Al evaluar el riesgo, el banco deberá tener en cuenta los factores pertinentes a la situación, como los antecedentes del cliente, su ocupación (incluido si ocupa un puesto relevante en el sector público o privado), sus fuentes de renta y riqueza, su país de origen y de residencia (cuando difieran), los productos utilizados, la naturaleza y finalidad de sus cuentas, las cuentas vinculadas, las actividades comerciales y otros indicadores de riesgo relacionados con el cliente, para determinar cuál es el nivel de riesgo total y las oportunas medidas a adoptar para gestionar esos riesgos.

33. Esas políticas y procedimientos deberán exigir una diligencia debida básica con todos los clientes y una diligencia debida proporcionada conforme varíe el nivel de riesgo asociado al cliente. En caso de situaciones probadas de bajo riesgo, podrán aceptarse medidas simplificadas, siempre que la legislación lo permita. Por ejemplo, la aplicación de procedimientos básicos para la apertura de cuentas podrá ser adecuada para un particular que prevea mantener pequeños saldos en cuenta y utilizar ésta para realizar operaciones rutinarias de banca minorista. Es importante que la política de aceptación de clientes no sea demasiado restrictiva para que no termine perjudicando el acceso del público en general a los servicios bancarios, especialmente de grupos financiera o socialmente desfavorecidos. La *Financial Inclusion Guidance*[20] del GAFI ofrece directrices útiles para diseñar procedimientos PBC/FT que no sean excesivamente restrictivos para personas financiera o socialmente desfavorecidas.

34. Cuando los riesgos sean más elevados, los bancos deberán adoptar medidas reforzadas para mitigar y gestionar esos riesgos. Una diligencia debida reforzada podrá ser esencial en el caso de un particular que planee mantener un importante saldo en cuenta y realice regularmente transferencias electrónicas transfronterizas o en el de una persona del medio político (PEP). En particular, esa diligencia debida reforzada es obligatoria en el caso de PEP extranjeras. Las decisiones de establecer o proseguir relaciones comerciales con clientes de alto riesgo exigirán la aplicación de medidas reforzadas de diligencia debida, como la aprobación de establecer o continuar esas relaciones, que deberá adoptar la alta dirección. La política de aceptación de clientes del banco también deberá definir las circunstancias en las cuales el banco no aceptará una nueva relación comercial o cancelará una relación ya existente.

3. Identificación, verificación y elaboración del perfil de riesgo de clientes y beneficiarios efectivos

35. A efectos de estas directrices, un cliente se define, con arreglo a la Recomendación 10 del GAFI, como cualquier persona[21] que entabla una relación comercial o realiza una transacción financiera ocasional con el banco. La diligencia debida con la clientela deberá aplicarse no sólo a los clientes, sino también a las personas que actúen por cuenta de aquéllos y de los beneficiarios efectivos[22]. Con arreglo a las normas GAFI, los bancos deberán identificar a los clientes y verificar su identidad[23].

19 Las normas GAFI también incluyen directrices útiles sobre la forma en que el banco podría aplicar eficazmente un enfoque en función del riesgo (véase, en particular, la Recomendación 1).

20 Véase FATF-GAFI, *Guidance on Anti-Money Laundering and Terrorist Financing and Financial Inclusion,* febrero de 2013, disponible en http://www.fatf-gafi.org/topics/financialinclusion/.

21 En este contexto, «persona» hace referencia a personas físicas o jurídicas o a estructuras jurídicas.

22 La expresión «beneficiario efectivo» se utiliza en este documento orientativo en consonancia con la definición y las aclaraciones incluidas en las normas GAFI. Como recordatorio, el GAFI define «beneficiario efectivo» como la(s) persona(s) física(s) que en último término posee(n) o controla(n) un cliente y/o la persona física en cuyo nombre se está realizando una transacción. También incluye a las personas que en último término ejercen un control efectivo sobre una persona o estructura jurídica.

23 Véase la nota interpretativa a la Recomendación 1 del GAFI. Este requisito resulta aplicable a menos que el país haya determinado, mediante una evaluación del riesgo, la existencia de tipos concretos de actividades (y clientes asociados a esas

36. El banco deberá implantar un procedimiento sistemático para identificar y verificar a sus clientes y, cuando proceda, a cualquier persona que actúe en nombre de aquéllos y de cualquier beneficiario efectivo. En general, el banco no deberá establecer una relación bancaria, ni realizar transacción alguna, hasta que la identidad del cliente haya sido satisfactoriamente establecida y verificada conforme a la Recomendación 10 del GAFI. En consonancia con el Principio Básico 29[24] y las normas GAFI, los procedimientos también deberán incluir la adopción de medidas razonables para verificar la identidad del beneficiario efectivo. El banco también deberá verificar que cualquier persona que actúe en nombre del cliente está autorizada para hacerlo, y deberá verificar la identidad de esa persona.

37. La identidad de clientes y beneficiarios efectivos, así como de las personas que actúen en nombre de aquéllos, deberá verificarse mediante documentos, datos o informaciones fiables e independientes. Cuando se recurra a documentos, el banco deberá tener presente que los mejores documentos para verificar la identidad son aquéllos más difíciles de obtener ilícitamente o falsificar. Cuando se recurra a otras fuentes de información distintas de documentos, el banco deberá cerciorarse de que los métodos (que podrán incluir la comprobación de referencias con otras instituciones financieras y la obtención de estados financieros) y las fuentes de información son adecuados y están en consonancia con las políticas y procedimientos del banco y con el perfil de riesgo del cliente. El banco podrá exigir a los clientes que cumplimenten una declaración por escrito sobre la identidad y los detalles del beneficiario efectivo, aunque no deberá recurrir únicamente a esas declaraciones. Al igual que en todos los elementos del proceso CDD, el banco también deberá considerar la naturaleza y nivel del riesgo planteado por un cliente cuando determine el alcance de las medidas de diligencia debida aplicables[25]. En ningún caso deberá el banco soslayar sus procedimientos de identificación y verificación de clientes solo porque el cliente no pueda presentarse a una entrevista (clientes no presentes); el banco también deberá tener en cuenta factores de riesgo como el motivo por el cual el cliente ha decidido abrir una cuenta lejos de su sede u oficina, especialmente en una jurisdicción extranjera. También sería importante tener en cuenta los riesgos relevantes asociados a clientes procedentes de jurisdicciones conocidas por sus deficiencias estratégicas en materia de PBC/FT y practicar una diligencia debida reforzada cuando así lo exijan el GAFI, otros organismos internacionales o las autoridades nacionales.

38. Si bien el proceso de identificación y verificación del cliente tiene lugar al comienzo de la relación o antes de realizarse una transacción bancaria ocasional, el banco deberá utilizar esa información para familiarizarse con el perfil y la conducta del cliente. La finalidad de la relación o de la transacción bancaria ocasional, el volumen de activos y el tamaño de las transacciones del cliente, así como la regularidad o duración de la relación, son ejemplos de información habitualmente recabada. Así pues, el banco deberá contar con políticas y procedimientos de diligencia debida con sus clientes que sean suficientes para elaborar perfiles de riesgo de clientes concretos o de determinadas categorías de clientes. La información recabada a estos efectos deberá venir determinada por el nivel de riesgo asociado al modelo de negocio y actividades del cliente, así como a los productos o servicios financieros demandados por éste. Estos perfiles de riesgo facilitarán la identificación de cualquier actividad en las cuentas que se desvíe de la actividad o conducta que sería considerada «normal» para un determinado cliente o categoría de clientes y que podría considerarse anómala, o incluso sospechosa. Los perfiles de riesgo de los clientes facilitarán al banco determinar posteriormente si el cliente o categoría de clientes plantea un alto riesgo y exige la aplicación de medidas y controles CDD reforzados. Los perfiles también

actividades) que podrán quedar eximidos debido al bajo riesgo probado de BC o FT, en consonancia con la nota interpretativa a la Recomendación 1.

[24] Véase Principio Básico 29, criterio esencial 5(b) de los *Principios básicos para una supervisión bancaria eficaz*, septiembre de 2012.

[25] Véase Banco Mundial, *Politically Exposed Persons, Preventive Measures for the Banking Sector,* 2010.

deberán reflejar el conocimiento que el banco tiene de la finalidad y naturaleza de la relación comercial o transacción bancaria ocasional, del volumen de actividad previsto, del tipo de transacciones y, en caso necesario, de las fuentes de fondos, renta o riqueza del cliente, así como de otras consideraciones análogas. Cualquier información significativa recabada sobre la actividad o conducta del cliente deberá utilizarse para actualizar la evaluación que realiza el banco del riesgo que presenta el cliente.

39. El banco deberá obtener los documentos de identificación del cliente, así como cualquier otra información y documentación recabada como resultado de la CDD practicada al cliente. Esa información podrá incluir copias o expedientes de documentos oficiales (como pasaportes, tarjetas de identidad, permisos de conducir), archivos de cuentas (por ejemplo, registros de transacciones financieras) y correspondencia comercial, incluidos los resultados de cualquier análisis realizado, como la evaluación del riesgo y las indagaciones efectuadas para averiguar los antecedentes y la finalidad de las relaciones y actividades.

40. El banco también deberá obtener toda la información necesaria para establecer a su entera satisfacción la identidad del cliente y la de cualquier persona que actúe en nombre de aquél y de los beneficiarios efectivos. Si bien el banco está obligado tanto a identificar a sus clientes como a verificar su identidad, la naturaleza y el alcance de la información requerida para la verificación dependerá de la evaluación del riesgo, incluidos el tipo de solicitante (persona física, empresa, etc.) y el volumen y uso previsto de la cuenta. Los requisitos específicos necesarios para comprobar la identidad de las personas físicas suelen establecerse en la legislación nacional. La verificación de la identidad de los clientes de alto riesgo exigirá la aplicación de procedimientos reforzados de diligencia debida. Si la relación es compleja, o el importe de la cuenta es sustancial, podrán resultar aconsejables medidas de identificación adicionales, que deberán determinarse en función del nivel de riesgo total.

41. Cuando el banco sea incapaz de completar las medidas CDD, no deberá abrir la cuenta, iniciar relaciones comerciales o realizar la transacción. No obstante, existen circunstancias en las que sería admisible completar la verificación tras establecer la relación comercial, porque resultaría esencial no interrumpir el curso normal de los negocios. En tales circunstancias, el banco deberá adoptar procedimientos adecuados de gestión del riesgo con respecto a las condiciones y limitaciones bajo las cuales el cliente podrá utilizar la relación bancaria antes de la verificación. En situaciones en que la cuenta haya sido abierta pero surjan problemas de verificación en el transcurso del establecimiento de la relación bancaria que no puedan ser resueltos, el banco deberá cerrar la cuenta o, si no, bloquear el acceso a ella. En cualquier caso, el banco deberá elaborar un STR en los casos en que existan problemas para completar las medidas CDD[26]. Además, cuando las comprobaciones CDD levanten sospechas u ofrezcan motivos razonables para sospechar que los activos o fondos del futuro cliente proceden de infracciones y delitos incluidos en supuestos de BC/FT, los bancos no deberán aceptar voluntariamente la apertura de cuentas a esos clientes. En dichas situaciones, los bancos deberán elaborar un STR, notificándolo a los autoridades competentes, y asegurarse de que el cliente no está informado, ni siquiera de forma indirecta, de que un STR ha sido, está siendo o será elaborado.

42. El banco deberá disponer de procedimientos y capacidad material para permitir a las actividades de cara al público y en contacto directo con los clientes identificar cualquier entidad o individuo designados (por ejemplo, terroristas, organizaciones terroristas) con arreglo a sus legislaciones nacionales y a las pertinentes Resoluciones del Consejo de Seguridad de las Naciones Unidas (RCSNU).

43. Si bien la realización de un depósito inicial mediante transferencia de fondos desde una cuenta a nombre del cliente en otro banco sujeto a las mismas normas CDD podría ofrecer cierta tranquilidad, aun así el banco deberá practicar su propia diligencia debida y considerar la posibilidad de que el

[26] Con sujeción a la legislación nacional sobre tratamiento de transacciones sospechosas.

anterior gerente de cuentas haya solicitado cancelar la cuenta por sospechar actividades ilícitas. Naturalmente, los clientes tienen derecho a cambiar de banco. Sin embargo, si un banco tiene motivos para pensar que otro banco ha negado servicios bancarios a un solicitante por sospechar actividades ilícitas del cliente, deberá considerar la clasificación de ese solicitante como de alto riesgo y aplicar procedimientos reforzados de diligencia debida al cliente y a la relación, elaborar un STR y/o no aceptar al cliente con arreglo a sus propios procedimientos y evaluaciones del riesgo.

44. El banco no deberá abrir una cuenta ni realizar negocios con un cliente que insista en el anonimato o que proporcione un nombre a todas luces ficticio. Tampoco deberán funcionar las cuentas confidenciales numeradas[27] como cuentas anónimas, sino que deberán estar sujetas a los mismos procedimientos CDD que las demás cuentas de clientes, aun cuando los procedimientos los lleve a cabo personal escogido. Aunque una cuenta numerada puede ofrecer mayor confidencialidad al titular, la identidad de éste deberá ser verificada por el banco y conocida por un número suficiente de empleados para facilitar la práctica de una eficaz diligencia debida, especialmente si otros factores de riesgo indican que el cliente es de alto riesgo. El banco deberá garantizar que sus unidades internas de control, cumplimiento , auditoría y otras funciones de vigilancia, en particular el responsable ejecutivo de PBC/FT, así como los supervisores del banco, tienen pleno acceso a esta información si fuera necesario.

4. Seguimiento continuo

45. El seguimiento continuo constituye un aspecto esencial de una sólida y eficaz gestión del riesgo BC/FT. El banco solo puede gestionar eficazmente sus riesgos si conoce la actividad bancaria razonable y normal de sus clientes y puede de ese modo identificar transacciones intentadas y anómalas que trascienden los patrones habituales de la actividad bancaria. Sin este conocimiento, el banco probablemente no podrá cumplir con su obligación de identificar y notificar las transacciones sospechosas a las autoridades competentes. Deberá realizarse un seguimiento continuo de todas las relaciones comerciales y transacciones, aunque el alcance de este seguimiento deberá estar en función del riesgo identificado en la evaluación de riesgos realizada por el banco y en sus labores de CDD. El seguimiento de los clientes o transacciones de alto riesgo deberá reforzarse. El banco no solo deberá realizar un seguimiento de sus clientes y de las transacciones de éstos, sino también una vigilancia transversal de los productos o servicios con el fin de identificar y mitigar los patrones de riesgo emergentes.

46. Todos los bancos deberán disponer de sistemas para detectar transacciones o patrones de actividad anómalos o sospechosos. Al diseñar escenarios para identificar dichas actividades, el banco deberá considerar el perfil de riesgo del cliente elaborado a partir de la evaluación de riesgos de la entidad, la información recabada en sus labores de CDD y otra información procedente de agencias policiales y otras autoridades en su jurisdicción. Por ejemplo, el banco podría tener conocimiento de determinados sistemas o mecanismos utilizados para blanquear fondos procedentes de actividades delictivas que las autoridades pueden haber detectado dentro su jurisdicción. Como parte de este proceso de evaluación del riesgo, el banco habrá evaluado el riesgo de que la actividad asociada a esos sistemas o mecanismos pueda estar desarrollándose dentro del banco a través de una categoría de clientes, grupo de cuentas, patrón de transacciones o utilización de productos. Con ese conocimiento, el banco deberá diseñar y aplicar herramientas de seguimiento y controles adecuados para identificar esas actividades. Por ejemplo, esto podría concretarse en escenarios de alerta basados en sistemas de

[27] En el caso de una cuenta numerada, el banco conoce el nombre del cliente y del beneficiario efectivo, pero se sustituye por un número de cuenta o un código en la documentación posterior.

seguimiento informatizados o en el establecimiento de límites a una determinada clase o categoría de actividades.

47. Utilizando la información CDD, el banco deberá ser capaz de identificar transacciones que no tienen sentido económico aparente, que implican cuantiosos depósitos en efectivo o que no se corresponden con las transacciones normales y previstas del cliente.

48. El banco deberá aplicar políticas y procedimientos reforzados de diligencia debida a los clientes que haya identificado como de alto riesgo. Además de las políticas y procedimientos establecidos para aprobar la apertura de cuentas, el banco también deberá contar con políticas específicas sobre el alcance y la naturaleza de la necesaria CDD, la frecuencia del seguimiento continuo de cuentas y la actualización de la información CDD y de otros registros. La capacidad del banco para vigilar e identificar eficazmente las actividades sospechosas exigirá el acceso a perfiles y registros de clientes actualizados, completos y fidedignos.

49. El banco deberá asegurarse de que dispone de sistemas integrados de gestión de la información, proporcionados a su tamaño, estructura organizativa o complejidad, basados en criterios de importancia relativa y en los riesgos, que ofrezcan a las unidades de negocio (por ejemplo, los gerentes de relaciones) y a los responsables de riesgos y cumplimiento (incluido el personal de investigación) la oportuna información necesaria para identificar, analizar y realizar un seguimiento eficaz de las cuentas de clientes. Los sistemas utilizados y la información disponible deberán facilitar el seguimiento de esas relaciones con clientes por líneas de negocio e incluir toda la información disponible sobre esa relación con el cliente, incluyendo el historial de transacciones, documentación omitida en la apertura de cuentas y cambios significativos en la conducta o el perfil de negocio del cliente, así como transacciones anómalas efectuadas a través de una cuenta de cliente.

50. El banco deberá cotejar su(s) base(s) de datos de clientes cuando haya modificaciones en los listados de sanciones. El banco también deberá cotejar periódicamente su(s) base(s) de datos de clientes para detectar PEP extranjeras y otras cuentas de alto riesgo y practicarles una diligencia debida reforzada.

5. Gestión de la información

(a) Mantenimiento de registros

51. El banco deberá garantizar el registro de toda la información recabada en el contexto de CDD. Esto incluye (i) el registro de los documentos facilitados al banco al verificar la identidad del cliente o del beneficiario efectivo y ii) la transcripción en los propios sistemas TI del banco de la información CDD relevante contenida en dichos documentos u obtenida por otros medios.

52. El banco también deberá desarrollar y aplicar reglas claras sobre los registros que deben mantenerse para documentar la diligencia debida practicada a los clientes y a las transacciones individuales. Si fuera posible, estas reglas deberán tener en cuenta cualquier medida preceptiva en materia de privacidad. Deberán incluir una definición de los tipos de información y documentación que habrán de incluirse en los registros, así como del periodo de conservación de esos registros, que deberá ser al menos de cinco años desde el cese de la relación bancaria o transacción ocasional[28]. Aun cuando las cuentas estén canceladas, en caso de una investigación o litigio en curso, todos los registros deberán conservarse hasta el cierre del procedimiento. El mantenimiento de registros completos y actualizados resulta esencial para permitir al banco vigilar la relación con su cliente, comprender el negocio y

[28] Véase Principio 29, criterio esencial 5(f) de los *Principios básicos para una supervisión bancaria eficaz*, septiembre de 2012.

actividades recurrentes del cliente y, si fuera necesario, para aportar un registro de auditoría en caso de controversias, acciones legales o indagaciones o investigaciones que pudieran acarrear medidas reglamentarias o un proceso penal.

53. También deberán mantenerse registros adecuados que documenten el proceso de evaluación relacionado con el análisis y seguimiento continuo y con las conclusiones extraídas, de forma que permitan demostrar el cumplimiento de los requisitos CDD por parte del banco y su capacidad para gestionar el riesgo BC y FT.

(b) Actualización de la información

54. Solo si los bancos garantizan que los registros mantienen su fiabilidad, vigencia y relevancia periódica y de la actualización de la información CDD podrán otras autoridades competentes, agencias policiales o unidades de inteligencia financiera hacer un uso eficaz de esa información para desarrollar sus propias funciones en el contexto de PBC/FT. Además, mantener la información actualizada contribuirá a que el banco vigile eficazmente las actividades anómalas o sospechosas en la cuenta.

(c) Suministro de información a los supervisores

55. El banco deberá ser capaz de demostrar a sus supervisores, a requerimiento de éstos, la adecuación de sus sistemas de evaluación, gestión y mitigación de riesgos BC/FT; de su política de aceptación de clientes; de sus procedimientos y políticas sobre identificación y verificación de clientes; de sus procesos de seguimiento continuo y de sus procedimientos para notificar transacciones sospechosas, así como de todas las medidas adoptadas en el contexto de PBC/FT.

6. Notificación de transacciones sospechosas y bloqueo de activos

(a) Notificación de transacciones sospechosas

56. El seguimiento y análisis continuo de cuentas y transacciones permitirá a los bancos identificar actividades sospechosas, eliminar falsos positivos y notificar con rapidez transacciones auténticamente sospechosas. El proceso para identificar, investigar y notificar transacciones sospechosas a la FIU deberá especificarse claramente en las políticas y procedimientos del banco y comunicarse a todo el personal a través de programas periódicos de formación. Estas políticas y procedimientos deberán ofrecer a los empleados una descripción clara de sus obligaciones, así como instrucciones para el análisis, investigación y notificación de dichas actividades dentro del banco, al igual que directrices sobre la forma de cumplimentar esos informes.

57. También deberán existir procedimientos establecidos para evaluar si las obligaciones reglamentarias del banco con arreglo a los regímenes de notificación de actividades sospechosas detectadas exigen notificar la transacción a las agencias policiales o FIU y/o a las autoridades supervisoras competentes, si procede. Estos procedimientos también deberán reflejar el principio de confidencialidad, garantizar que la investigación se desarrolla con rapidez y que los informes contienen información relevante y se elaboran y notifican oportunamente. El responsable ejecutivo de PBC/FT deberá garantizar una notificación rápida cuando los fondos u otros activos sospechosos de proceder de actividades delictivas se mantengan en una cuenta.

58. Una vez que se sospecha de una cuenta o relación, además de notificar la actividad sospechosa, el banco deberá garantizar la adopción de medidas oportunas para mitigar adecuadamente el riesgo de que el banco sea utilizado en actividades delictivas. Estas medidas podrán incluir revisar la clasificación de riesgo del cliente o cuenta o de la relación en su totalidad. La adopción de medidas oportunas podría exigir trasladar el asunto en cuestión al nivel decisorio apropiado para determinar la forma de gestionar la relación, teniendo en cuenta cualquier otro factor relevante, como la cooperación con agencias policiales o la FIU.

(b) Bloqueo de activos

59. La financiación del terrorismo presenta similitudes con el blanqueo de capitales, pero también muestra singularidades que los bancos deberán tener en cuenta: los fondos utilizados para financiar actividades terroristas pueden proceder de actividades delictivas o de fuentes lícitas y la naturaleza de las fuentes de financiación puede variar según el tipo de organización terrorista. Además, cabe señalar que los importes de las transacciones asociadas a la financiación de terroristas pueden ser muy reducidos.

60. El banco deberá ser capaz de identificar y cumplir las decisiones de bloqueo de fondos adoptadas por la autoridad competente y bajo ningún motivo deberá mantener relaciones con entidades o individuos designados (por ejemplo, terroristas, organizaciones terroristas), en consonancia con las pertinentes legislaciones nacionales y RCSNU.

61. La CDD deberá permitir al banco detectar e identificar posibles transacciones FT, propiciando un conocimiento más preciso de sus clientes y de las transacciones que realizan. Al desarrollar sus políticas y procedimientos de aceptación de clientes, el banco deberá otorgar la debida importancia a los riesgos específicos de establecer o proseguir relaciones comerciales con entidades o individuos vinculados a grupos terroristas. Antes de establecer una relación comercial o realizar una transacción ocasional con nuevos clientes, el banco deberá comprobar si éstos figuran en listados de terroristas conocidos o presuntos publicados por las autoridades competentes (nacionales e internacionales). Del mismo modo, el seguimiento continuo deberá verificar que los actuales clientes no figuran en esos mismos listados.

62. Todos los bancos deberán contar con sistemas para detectar transacciones prohibidas (como transacciones con entidades designadas en las pertinentes RCSNU o en los listados de sanciones nacionales). La detección de terroristas no es una medida de diligencia debida sensible al riesgo, por lo que deberá realizarse independientemente del perfil de riesgo atribuido al cliente. Con el fin de detectar terroristas, el banco podrá adoptar sistemas de detección automática, pero deberá asegurarse de que esos sistemas son adecuados a sus fines. El banco deberá bloquear sin demora y sin previo aviso los fondos u otros activos de personas o entidades designadas, con arreglo a la legislación y regulación aplicables.

III. PBC/FT a escala de grupo y en un contexto transfronterizo

63. Cuando un banco opera en otras jurisdicciones, una sólida gestión del riesgo BC/FT implica tener en cuenta los requisitos legales del país de acogida. Dados los riesgos, cada grupo deberá desarrollar políticas y procedimientos PBC/FT a escala del grupo, con una aplicación y supervisión coherentes en todo el grupo. A su vez, las políticas y procedimientos en sucursales y filiales, aun cuando tengan en cuenta los patrones de negocio locales y los requisitos de la jurisdicción de acogida, deberán secundar y ser coherentes con las políticas y procedimientos generales para todo el grupo[29]. En los casos en que los requisitos de la jurisdicción de acogida sean más estrictos que los del grupo, la política del grupo deberá permitir a la sucursal o filial de que se trate adoptar y aplicar los requisitos locales de la jurisdicción de acogida.

[29] En este documento, el término «grupo» hace referencia a uno o más bancos incluidos en una organización, así como a las sucursales y filiales de esos bancos. En este documento, la expresión «oficina central» designa también al banco matriz o a la unidad en la cual se realiza la gestión del riesgo PBC/FT por líneas de negocio.

1. Proceso global para la gestión del riesgo de clientes

64. La gestión consolidada del riesgo implica establecer y administrar un proceso de coordinación y aplicación de políticas y procedimientos para todo el grupo, que establezca un punto de referencia sistemático e integral para gestionar los riesgos de las diferentes operaciones internacionales del banco. El diseño de las políticas y procedimientos no deberá perseguir únicamente el estricto cumplimiento de toda la legislación y regulación pertinentes, sino el objetivo más general de identificar, vigilar y mitigar los riesgos en todo el grupo. Deberá hacerse todo lo posible por garantizar que la capacidad del grupo para obtener y analizar información conforme a sus políticas y procedimientos globales no sufre menoscabo como resultado de modificaciones de las políticas o procedimientos locales que viniesen exigidas por requisitos legales locales. A este respecto, el banco deberá disponer de un robusto sistema de intercambio de información entre la oficina central y todas sus sucursales y filiales. Cuando los requisitos reglamentarios o legales mínimos de los países de origen y acogida difieran, las oficinas ubicadas en las jurisdicciones de acogida aplicarán las normas más estrictas.

65. Asimismo, conforme a las normas GAFI[30], si el país de acogida no permitiera la adecuada aplicación de esas normas, el responsable ejecutivo de PBC/FT deberá informar a los supervisores de origen. Deberán contemplarse medidas adicionales, incluida, cuando proceda, la cancelación de las operaciones del grupo financiero en el país de acogida.

66. El Comité reconoce que la aplicación de procedimientos PBC/FT en todo el grupo resulta más difícil que la de muchos otros procesos de gestión del riesgo, ya que algunas jurisdicciones continúan limitando la capacidad de los bancos para comunicar nombres y saldos de clientes a otros países. Para un seguimiento eficaz en todo el grupo y a efectos de la gestión del riesgo BC/FT, resulta fundamental que, sin perjuicio de las debidas salvaguardas jurídicas, los bancos estén autorizados a intercambiar información sobre sus clientes con sus oficinas centrales o banco matriz. Esto es aplicable tanto a sucursales como a filiales.

2. Evaluación y gestión del riesgo

67. El banco deberá tener un conocimiento exhaustivo de todos los riesgos asociados a sus clientes en todo el grupo, individualmente o por categorías, y deberá documentar y actualizar periódicamente esa información, en consonancia con el nivel y naturaleza del riesgo en el grupo. Al evaluar el riesgo asociado a un cliente, el banco deberá identificar todos los factores de riesgo relevantes, como la ubicación geográfica, los patrones de transacciones (declarados o puestos de manifiesto) y la utilización de productos y servicios bancarios, y establecer criterios para identificar a los clientes de alto riesgo. Estos criterios deberán aplicarse en todo el banco, sus filiales y sucursales y en las actividades subcontratadas (véase Anexo 1). Los clientes que planteen un alto riesgo de BC/FT para el banco deberán identificarse utilizando estos mismos criterios en todo el grupo. Las evaluaciones del riesgo asociado a los clientes deberán aplicarse del mismo modo en todo el grupo o, al menos, ser congruentes con la evaluación del riesgo a escala del grupo. Teniendo en cuenta las diferencias en los riesgos asociados a diferentes categorías de clientes, la política del grupo deberá reconocer que clientes incluidos en la misma categoría podrían plantear diferentes riesgos en distintas jurisdicciones. La información recabada en el proceso de evaluación deberá utilizarse posteriormente para determinar el nivel y naturaleza del riesgo total del grupo y facilitar el diseño de controles adecuados en el grupo para mitigar esos riesgos. Los factores mitigadores pueden incluir información adicional del cliente,

[30] Véase la nota interpretativa a la Recomendación 18 (Controles internos y sucursales y filiales en el extranjero) de las normas GAFI.

seguimientos más estrechos, actualizaciones más frecuentes de datos personales y visitas de personal del banco al domicilio del cliente.

68. El personal encargado del cumplimiento y la auditoría interna de los bancos, en particular el responsable ejecutivo de PBC/FT, o los auditores externos, deberán evaluar el cumplimiento de todos los aspectos de las políticas y procedimientos de su grupo, incluida la eficacia de las políticas CDD centralizadas y los requisitos para intercambiar información con otros miembros del grupo y responder a consultas de la oficina central. Los grupos bancarios con actividad internacional deberán garantizar que disponen de una sólida unidad de auditoría interna y una función de cumplimiento global, puesto que ambas constituyen los principales mecanismos para vigilar la aplicación general de la CDD global del banco y la eficacia de sus políticas y procedimientos de intercambio de información dentro del grupo. Al respecto, deberá existir un responsable ejecutivo de PBC/FT para todo el grupo que se responsabilizará del cumplimiento de todas las políticas, procedimientos y controles PBC/FT de ámbito nacional e internacional (véanse los párrafos 75 y 76).

3. Políticas y procedimientos PBC/FT a escala consolidada

69. El banco deberá garantizar que entiende el grado en que la legislación PBC/FT le permite recurrir a los procedimientos aplicados por otros bancos (por ejemplo, dentro del mismo grupo) cuando se está recomendando un negocio. El banco no deberá recurrir a presentadores que estén sujetos a normas menos estrictas que las que rigen sus propios procedimientos PBC/FT. En consecuencia, los bancos vigilarán y evaluarán las normas PBC/FT vigentes en la jurisdicción del banco que realiza la recomendación. El banco podrá recurrir a un presentador que forme parte del mismo grupo financiero y podrá sopesar conceder un mayor grado de fiabilidad a la información suministrada por este presentador, siempre que éste se encuentre sujeto a las mismas normas que el banco y que la aplicación de estos requisitos se supervise a escala del grupo. No obstante, el banco que adopte este enfoque deberá cerciorarse de que obtiene la información del cliente suministrada por el banco que lo recomienda (conforme se detalla en el Anexo 1), ya que podría exigirse remitir esta información a las FIU si se determinara que una transacción en la que participa el cliente recomendado es sospechosa.

70. La oficina central del grupo bancario deberá tener acceso a la información relevante con el fin de hacer cumplir las políticas y procedimientos PBC/FT del grupo. Cada oficina del grupo bancario deberá estar en disposición de cumplir las políticas y procedimientos PBC/FT y de accesibilidad mínimos aplicados por la oficina central y definidos con arreglo a las directrices del Comité.

71. Las políticas de aceptación de clientes, CDD y mantenimiento de registros deberán implementarse mediante la aplicación coherente de políticas y procedimientos en toda la organización, con los ajustes precisos para tener en cuenta las diferencias de riesgo por líneas de negocio o áreas geográficas de actividad. Además, se reconoce que puede ser necesario utilizar diferentes métodos de recopilación y conservación de la información en distintas jurisdicciones para adecuarse a los requisitos reglamentarios locales o a factores de riesgo relativo. No obstante, estos métodos deberán ser coherentes con las normas para todo el grupo anteriormente expuestas.

72. Independientemente de su ubicación, cada oficina deberá establecer y mantener políticas y procedimientos eficaces acordes con los riesgos presentes en la jurisdicción y en el banco. Este seguimiento local deberá complementarse con un robusto proceso de intercambio de información con la oficina central y, si procede, con otras sucursales y filiales en relación con las cuentas y actividades que puedan plantear un mayor riesgo.

73. A fin de gestionar eficazmente los riesgos BC y FT procedentes de tales cuentas, el banco deberá integrar esa información en función no solo del cliente, sino también de su conocimiento de los beneficiarios efectivos del cliente y de los fondos en cuestión. El banco deberá vigilar a escala consolidada las relaciones, saldos y actividades de importancia con clientes, con independencia de si las cuentas se mantienen dentro del balance, fuera del balance, como activos en administración o en

fideicomiso, e independientemente del lugar en que se mantengan. Las actuales normas GAFI incluyen también disposiciones más detalladas sobre la vigilancia de las funciones de cumplimiento, auditoría y/o PBC/FT del grupo por parte de las oficinas centrales de los bancos[31]. Además, habiéndose concebido estas directrices principalmente para bancos, podrían resultar de interés para conglomerados (que incluyen bancos).

74. Muchos grandes bancos con capacidad para ello centralizan ciertos sistemas de procesamiento y bases de datos para una gestión más eficaz o por motivos de eficiencia. Al aplicar este enfoque, el banco deberá documentar e integrar adecuadamente las funciones locales y centralizadas de seguimiento de transacciones/cuentas para garantizar que está en condiciones de vigilar patrones de posibles actividades sospechosas en todo el grupo y no solo a escala local o centralizada.

75. Los bancos con actividad nacional e internacional deberán nombrar un responsable ejecutivo de PBC/FT para todo el grupo (responsable de PBC/FT del grupo). El responsable de PBC/FT del grupo tiene la responsabilidad, como parte de la gestión global del riesgo, de crear, coordinar y evaluar a escala del grupo la aplicación de una única estrategia PBC/FT (que incluye políticas y procedimientos obligatorios y autorización para impartir órdenes a todas las sucursales, filiales y entidades subordinadas nacionales e internacionales).

76. La función del responsable de PBC/FT del grupo incluye el seguimiento continuo del cumplimiento de todos los requisitos PBC/FT, tanto nacionales como internacionales, en todo el grupo. Así pues, el responsable de PBC/FT del grupo deberá cerciorarse (incluso realizando visitas periódicas *in situ*) del cumplimiento de los requisitos PBC/FT en todo el grupo. En caso necesario, deberá estar facultado para impartir órdenes o adoptar las medidas oportunas en todo el grupo.

4. Intercambio de información dentro del grupo

77. Los bancos deberán vigilar la coordinación del intercambio de información. Las filiales y sucursales deberían estar obligadas a suministrar de forma proactiva a la oficina central información sobre clientes y actividades de alto riesgo que sea relevante a efectos de las normas globales PBC/FT y a responder de manera oportuna a las solicitudes de información sobre cuentas remitidas desde la oficina central o el banco matriz. Las normas del banco para el conjunto del grupo deberán incluir una descripción del proceso a seguir en todos los establecimientos para identificar, vigilar e investigar posibles circunstancias anómalas y notificar actividades sospechosas.

78. Las políticas y procedimientos del banco para todo el grupo deberán tener en cuenta las cuestiones y obligaciones relacionadas con la protección de datos a escala local y con la legislación y regulación en materia de privacidad. También deberán tener en cuenta los diferentes tipos de información que podrán compartirse dentro del grupo y los requisitos de almacenamiento, recuperación, intercambio/distribución y eliminación de esa información.

79. La función global de gestión del riesgo BC/FT del grupo deberá evaluar los posibles riesgos planteados por las actividades notificadas por sus sucursales y filiales y, cuando proceda, evaluar los riesgos en todo el grupo planteados por un determinado cliente o categoría de clientes. También deberá contar con políticas y procedimientos para comprobar si otras sucursales o filiales mantienen cuentas de un mismo cliente (incluidas las de partes vinculadas a ese cliente o pertenecientes a su mismo grupo). Asimismo, el banco deberá disponer de políticas y procedimientos globales en materia de relaciones de cuenta consideradas de alto riesgo o que hayan estado asociadas a actividades potencialmente

[31] Véase en particular la Recomendación 18 de las normas GAFI.

sospechosas, incluidos procedimientos de remisión a directivos de mayor jerarquía y directrices sobre restricciones a las actividades de las cuentas, incluido su cierre cuando proceda.

80. Además, el banco y sus sucursales y filiales deberán, con arreglo a sus respectivas legislaciones nacionales y a requerimiento de agencias policiales, autoridades supervisoras o FIU, cooperar ante solicitudes de información sobre clientes que aquéllas precisen en sus labores de lucha contra BC y FT. La oficina central del banco ha de poder exigir a todas sus sucursales y filiales el cotejo de sus archivos con determinados listados o solicitudes a fin de comprobar la presencia de individuos u organizaciones sospechosos de colaborar e instigar BC y FT y que notifiquen las coincidencias.

81. El banco deberá ser capaz de informar a sus supervisores, a requerimiento de éstos, sobre su proceso global de gestión del riesgo de clientes, su evaluación y gestión de los riesgos BC/FT, sus políticas y procedimientos PBC/FT a escala consolidada y sus sistemas de intercambio de información dentro del grupo.

5. Grupos financieros mixtos

82. Numerosos grupos bancarios realizan operaciones con valores y actividades de seguro. La aplicación de controles de gestión del riesgo BC/FT en los grupos financieros mixtos plantea cuestiones adicionales que podrían ser ajenas a las propias de las operaciones de captación de depósitos y concesión de préstamos. Los grupos mixtos deberán ser capaces de vigilar e intercambiar información sobre la identidad de los clientes y sobre sus transacciones y cuentas en el conjunto del grupo, y estar atentos a los clientes que utilicen sus servicios en diferentes sectores, según se describe en el párrafo 79 precedente.

83. Las diferencias en la naturaleza de las actividades y en los patrones de relaciones entre bancos y clientes en cada sector podrán requerir o justificar variaciones de los requisitos PBC/FT exigidos a cada sector. El grupo deberá estar atento a estas diferencias cuando se realicen ventas cruzadas de productos y servicios a los clientes desde distintas unidades de negocio, debiéndose aplicar los oportunos requisitos PBC/FT a los correspondientes sectores.

IV. El papel de los supervisores

84. Cabe esperar que los supervisores bancarios cumplan la Recomendación 26 del GAFI, que, entre otras cosas, indica lo siguiente: «En el caso de las instituciones financieras sujetas a los Principios Básicos, las medidas de regulación y supervisión que se aplican con fines de vigilancia prudencial, y que son también relevantes en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, deberían aplicarse de forma similar a los efectos de PBC/FT. Esto deberá incluir la aplicación de una supervisión consolidada a todo el grupo con fines de PBC/FT». El Comité prevé que los supervisores apliquen los *Principios básicos para una supervisión bancaria eficaz* a la gestión del riesgo BC/FT de los bancos en sintonía y colaboración con la supervisión general de los bancos que aquéllos realizan. Los supervisores tendrán la facultad de imponer una gama de sanciones eficaces, proporcionadas y disuasorias cuando los bancos incumplan sus requisitos PBC/FT.

85. Cabe esperar que los supervisores bancarios definan las expectativas supervisoras que guíen las políticas y procedimientos PBC/FT de los bancos. Los aspectos esenciales descritos en este documento deberán aportar a los supervisores directrices claras para acometer las tareas de diseño o mejora de las prácticas supervisoras nacionales. Se exhorta a los supervisores nacionales a que ofrezcan directrices que permitan a los bancos diseñar sus propias políticas y procedimientos de identificación de clientes. Por consiguiente, el Comité ha desarrollado en los Anexos 1 y 2 dos guías sobre aspectos concretos que los supervisores podrán utilizar con esa finalidad.

86. Los supervisores deberán adoptar un enfoque en función del riesgo para supervisar la gestión de los riesgos BC/FT de los bancos[32]. Este enfoque exige que los supervisores (i) desarrollen un conocimiento exhaustivo de los riesgos presentes en la jurisdicción y de su potencial impacto en las entidades supervisadas [33]; (ii) evaluar la suficiencia de la evaluación de riesgos del banco en función de la(s) evaluación(es) de riesgos nacional(es) de la jurisdicción[34]; (iii) evaluar los riesgos presentes en la entidad supervisada objetivo para conocer la naturaleza y el alcance de los riesgos en su base de clientes, productos y servicios y áreas geográficas en las que el banco y sus clientes realizan negocios; (iv) evaluar la suficiencia y eficacia de la aplicación de los controles (incluidas las medidas CDD) diseñados por el banco para cumplir sus obligaciones PBC/FT y la mitigación de riesgos; y (v) utilizar esta información para asignar recursos, dimensionar el examen, identificar la experiencia y destrezas de los supervisores necesarias para realizar un examen eficaz y asignar estos recursos con arreglo a los riesgos identificados.

87. Para garantizar un examen eficaz, es posible que las líneas de negocio o categorías de clientes de alto riesgo exijan conocimientos especializados y procedimientos adicionales. El perfil de riesgo del banco también deberá utilizarse para determinar la frecuencia y calendario del ciclo supervisor. De nuevo, los bancos cuya clientela presente perfiles de alto riesgo podrán requerir análisis más frecuentes que otros. Los supervisores también deberán verificar si los bancos han hecho un uso adecuado de su discrecionalidad al aplicar medidas PBC/FT enmarcadas en un enfoque en función del riesgo. También deberán evaluar los controles internos existentes y la forma en que los bancos determinan si cumplen las directrices supervisoras y reguladoras y las obligaciones exigidas. El proceso supervisor no solo deberá incluir un análisis de las políticas y procedimientos, sino también, en su caso, un examen de la documentación sobre clientes y del muestreo de cuentas y transacciones, informes internos y STR. Los supervisores estarán siempre autorizados a revisar toda la documentación relacionada con las transacciones efectuadas o las cuentas mantenidas en su jurisdicción, incluido cualquier análisis realizado por el banco para detectar transacciones anómalas o sospechosas.

88. Los supervisores tienen el deber de garantizar que los bancos aplican una sólida gestión del riesgo BC/FT, no solo para proteger su propia seguridad y solvencia, sino también la integridad del sistema bancario[35]. Los supervisores deberán dejar claro que adoptarán las medidas oportunas (que podrían ser severas y públicas si las circunstancias así lo justifican) contra los bancos y sus altos cargos que manifiestamente incumplan sus propios procedimientos internos y requisitos reglamentarios. Además, los supervisores (u otras autoridades nacionales competentes) estarán facultados para adoptar medidas correctivas adecuadas y garantizar que los bancos conocen y aplican medidas CDD reforzadas a las relaciones comerciales y transacciones cuando así lo exija el GAFI o a las vinculadas a jurisdicciones cuyas normas PBC/FT sean consideradas inadecuadas por el país. A este respecto, el GAFI y algunas autoridades nacionales han elaborado un listado de países y jurisdicciones considerados con deficiencias

[32] Los supervisores también deberán tener en cuenta el método de supervisión en función del riesgo descrito en la nota interpretativa 26 de las normas GAFI.

[33] A estos efectos, cabe esperar que los supervisores utilicen la evaluación de países descrita en la nota interpretativa a la Recomendación 1 de las normas GAFI.

[34] Incluida, cuando proceda, cualquier evaluación de riesgos supranacionales.

[35] Muchos supervisores también tienen el deber de informar de cualquier transacción sospechosa, anómala o ilegal detectada, por ejemplo, durante inspecciones *in situ*.

estratégicas en materia de PBC/FT o que incumplen normas internacionales sobre PBC/FT[36], debiendo incorporarse esta información a la gestión de riesgos BC/FT del banco.

89. Los supervisores también deberán considerar el proceso global de seguimiento y vigilancia por parte del banco del cumplimiento en sus sucursales y filiales, así como la capacidad del grupo para adaptarse a los requisitos reglamentarios locales y garantizar que cuando exista una discrepancia entre los requisitos locales y los del grupo, se aplicarán los más estrictos. Los supervisores también deberán garantizar que, en los casos en que la sucursal o filial del grupo no pueda aplicar la más estricta de las dos normas, se documentarán los motivos y las diferencias entre ambas y se aplicarán las oportunas medidas paliativas para mitigar los riesgos identificados como resultado de esas discrepancias.

90. En un contexto transfronterizo, los supervisores del país de origen[37] no deberán sufrir trabas durante las inspecciones *in situ* para verificar que el banco cumple las políticas y procedimientos PBC/FT en todo el grupo. Esta verificación podría exigir un examen de los archivos de clientes y un muestreo de cuentas o transacciones en la jurisdicción de acogida. Los supervisores del país de origen deberán tener acceso a información sobre las cuentas y transacciones de clientes individuales extraídas en el muestreo y sobre los riesgos nacionales e internacionales asociados a esos clientes, en la medida en que sea necesario para realizar una correcta evaluación de la aplicación de las normas CDD y una valoración de las prácticas de gestión del riesgo. Este uso de información con fines supervisores legítimos, salvaguardado por cláusulas de confidencialidad aplicables a los supervisores, no deberá verse entorpecido por la legislación local sobre secreto bancario o protección de datos. Aunque los supervisores y/u otras autoridades del país de acogida mantengan la responsabilidad de hacer cumplir los requisitos PBC/FT locales (lo que incluiría una evaluación de la idoneidad de los procedimientos), los supervisores del país de acogida deberán garantizar su plena cooperación y apoyo a los supervisores del país de origen, quienes podrían necesitar evaluar la forma en que el banco vigila el cumplimiento de las políticas y procesos PBC/FT en todo el grupo.

91. La función del auditor (externo o interno) del grupo es particularmente importante para evaluar la eficacia de las políticas y procedimientos PBC/FT. Los supervisores del país de origen deberán garantizar la existencia de una política adecuada, en función del riesgo, y de una asignación de recursos adecuados en consonancia con el alcance y la frecuencia de la auditoría de los procedimientos PBC/FT del grupo. Asimismo, deberán garantizar que los auditores tienen pleno acceso a todos los informes relevantes durante el proceso de auditoría.

92. Los supervisores deberán garantizar que la información sobre los clientes y transacciones de los bancos está sujeta a los mismos criterios de confidencialidad aplicables al amplio conjunto de información sobre las actividades de los bancos intercambiada entre los supervisores.

[36] Por ejemplo, podrán identificarse públicamente esas jurisdicciones a través de:

- La *Public Statement* (o declaración pública) del GAFI, que identifica:
  - (i) jurisdicciones con deficiencias estratégicas en materia de PBC/FT y a las cuales se aplican medidas correctivas;
  - (ii) jurisdicciones con deficiencias estratégicas en materia de PBC/FT que no han realizado suficientes progresos para subsanar las deficiencias o no se han comprometido a seguir un plan de actuación desarrollado con el GAFI para paliarlas.
- El GAFI publica un documento, *Improving Global AML/CFT Compliance: On-going Process*, que identifica jurisdicciones con deficiencias estratégicas en materia de PBC/FT que han demostrado un elevado grado de compromiso político para subsanarlas mediante la aplicación de un plan de actuación desarrollado en colaboración con el GAFI.

[37] En los países donde el proceso de inspección lo realicen auditores externos, este tratamiento eximente también deberá aplicarse a los auditores competentes.

93. Resulta esencial que todas las jurisdicciones que acojan bancos extranjeros ofrezcan un marco jurídico adecuado para facilitar la transmisión de información necesaria con fines de gestión del riesgo de clientes a la oficina central o banco matriz y a los supervisores del país de origen. Del mismo modo, no deberán existir impedimentos a las visitas *in situ* a las filiales y sucursales en la jurisdicción de acogida por parte de auditores, gerentes de riesgos, responsables de cumplimiento (incluido el responsable ejecutivo PBC/FT o el responsable PBC/FT del grupo) de la oficina central de la jurisdicción de origen, o de los supervisores del país de origen, ni restricciones a su capacidad para acceder a todos los registros del banco en la jurisdicción de acogida, incluidos nombres de clientes y saldos en sus cuentas. Este acceso será el mismo tanto para sucursales como para filiales. Si las trabas al intercambio de información resultaran insuperables, y no hubiese arreglo alternativo satisfactorio, los supervisores de origen deberán informar al supervisor de acogida de que el banco podría quedar sujeto a actuaciones supervisoras adicionales, como el refuerzo de las medidas supervisoras sobre el grupo, incluida, en su caso, la exigencia al grupo matriz del cierre de sus operaciones en la jurisdicción de acogida.

94. Cuando se permita el acceso de personal de la oficina central de un banco a información sobre clientes locales, no deberá impedírsele que la transmita a la oficina central. Esa información deberá estar sujeta a las oportunas salvaguardas sobre confidencialidad y utilización y podrá estar sometida a la legislación aplicable sobre privacidad y privilegios en el país de origen.

95. El Comité cree que no existen razones que justifiquen una legislación que impida la transmisión de información de clientes desde una sucursal o filial bancaria de acogida hacia su oficina central o banco matriz en la jurisdicción de origen con fines de gestión del riesgo, incluidos los riesgos BC y FT. Si la legislación en la jurisdicción de acogida restringiese la divulgación de esa información a «terceros», es fundamental que la oficina central o banco matriz y los supervisores bancarios de la jurisdicción de origen quedasen claramente excluidos de la definición de terceros. Se insta a las jurisdicciones con legislaciones que impidan, o pueda interpretarse que impiden, ese intercambio de información con fines de gestión del riesgo BC/FT a levantar esas restricciones y a proporcionar canales de comunicación específicos adecuados a tal efecto.

Anexo 1

Utilización de otro banco, institución financiera o tercero para practicar la diligencia debida a clientes

I. Introducción

1. En algunos países, se permite a los bancos utilizar otros bancos, instituciones financieras u otras entidades para practicar la diligencia debida a clientes (CDD). Estos mecanismos pueden adoptar diversas formas pero, en esencia, suelen conllevar alguna de las dos situaciones siguientes:

Recurso a terceros

2. En algunos países se permite a los bancos recurrir a la CDD practicada por otras instituciones financieras o determinadas empresas o profesiones no financieras que, a su vez, se encuentran supervisados o vigilados a efectos de PBC/FT[38]. En estas situaciones, el tercero tendrá normalmente una relación comercial previa con el cliente y los bancos podrían quedar eximidos de aplicar sus propias medidas CDD al inicio de la relación. Las normas GAFI[39] permiten dicho recurso para estas cuestiones:

(a) Identificar al cliente y verificar su identidad utilizando documentos, datos o informaciones fiables e independientes.

(b) Identificar al beneficiario efectivo y adoptar medidas razonables para verificar su identidad, de forma que la institución financiera quede satisfecha de que conoce quién es el beneficiario efectivo. En el caso de personas y estructuras jurídicas, las instituciones financieras deberán entender la estructura de propiedad y control del cliente.

(c) Entender la finalidad y naturaleza prevista de la relación comercial y, cuando proceda, obtener información sobre ella.

Las normas GAFI exigen además que la institución financiera que recurra a un tercero obtenga inmediatamente la información necesaria sobre estas tres medidas CDD.

3. Algunos países limitan de diversas formas ese recurso; por ejemplo, circunscribiéndolo a instituciones financieras, permitiéndolo solo en el caso de relaciones previas de terceros (y prohibiendo las cadenas de recurso) o no permitiendo el recurso a entidades extranjeras.

Subcontratación/agencia

4. Los bancos podrán utilizar terceros, mediante vínculo contractual, para cumplir determinadas partes de sus obligaciones CDD, frecuentemente a través de una relación de subcontratación/agencia (es decir, la entidad subcontratada aplica las medidas CDD en nombre del banco que delega). Suele haber

[38] Véase la Recomendación 17 de las normas GAFI y su nota interpretativa.

[39] Véanse la Recomendación 17 y la Recomendación 10 sobre CDD de las normas GAFI.

menos restricciones sobre quién puede actuar como agente de un banco, pero habitualmente es a cambio de la existencia de procedimientos y registros obligatorios.

5. Tanto en el caso de recurso a terceros como en el de subcontratación, los bancos podrán limitar el tamaño, ámbito o naturaleza de los tipos de transacciones cuando utilicen terceros. En todos los casos, los supervisores deberán tener puntual acceso a la información sobre clientes cuando así lo soliciten. Aunque estas dos categorías parecen similares o relacionadas, existen notables diferencias entre ellas y los bancos deberán cerciorarse de que entienden esas diferencias y las reflejan en sus políticas y procedimientos.

II. Recurso a terceros

6. Los bancos deberán disponer de políticas y procedimientos claros con respecto a si y cuándo es aceptable y prudente recurrir a otro banco o institución financiera. Dicho recurso en modo alguno libera al banco de la responsabilidad de disponer de adecuadas políticas y procedimientos CDD y de otros requisitos PBC/FT con respecto a los clientes, como el conocimiento de su actividad prevista, si son de alto riesgo o si las transacciones son sospechosas.

7. Cuando dependan de otro banco o institución financiera para practicar ciertos aspectos de la CDD, los bancos deberán evaluar la razonabilidad de ese recurso. Además de garantizar la existencia de capacidad legal para formalizar el recurso, los criterios relevantes para su evaluación incluyen:

(a) La entidad bancaria, institución financiera u otra entidad (según permita la legislación nacional) a la que se recurra deberá estar sometida a una regulación y supervisión tan exhaustiva como el banco, utilizar requisitos comparables para la identificación de consumidores durante la apertura de cuentas y tener una relación previa con el cliente que abre una cuenta en el banco. Alternativamente, la legislación nacional podrá exigir el uso de medidas o controles paliativos, en los casos en que estas normas no se cumplan.

(b) El banco y la otra entidad deberán formalizar por escrito un convenio o acuerdo reconociendo el recurso del banco a los procesos CDD de la otra institución financiera.

(c) Los procedimientos y políticas del banco deberán documentar ese recurso y establecer adecuados controles y procedimientos de evaluación de dicha relación.

(d) Podrá exigirse a los terceros que certifiquen al banco que han aplicado su programa PBC y que practican una CDD sustancialmente equivalente a la del banco o coherente con las obligaciones de éste.

(e) El banco deberá tener debidamente en cuenta informaciones públicas desfavorables sobre el tercero, como estar sometido a medidas coercitivas por causa de deficiencias o violaciones en materia de PBC.

(f) El banco deberá identificar y mitigar cualquier riesgo adicional que plantee recurrir a una multitud de terceros (una cadena de recursos) en vez de mantener una relación directa con una sola entidad.

(g) La evaluación de riesgos del banco deberá identificar el recurso a terceros como un factor potencial de riesgo.

(h) El banco deberá examinar periódicamente a la otra entidad para cerciorarse de que ésta continúa practicando CDD de una forma tan exhaustiva como el banco. A estos efectos, el banco deberá obtener toda la información y documentación CDD del banco, institución financiera o entidad a la que recurra y evaluar la diligencia debida practicada, incluido su cotejo con bases de datos locales para garantizar el cumplimiento de los requisitos reglamentarios locales.

(i) Los bancos deberán contemplar el cese de su recurso a entidades que no practiquen una adecuada CDD a sus clientes o incumplan requisitos y expectativas.

8. Los bancos con filiales o sucursales fuera de la jurisdicción de origen utilizan frecuentemente el grupo financiero para presentar sus clientes a otras partes del grupo. En países que permiten este recurso transfronterizo a filiales, las instituciones financieras que confíen la identificación de clientes a otras partes del grupo deberán cerciorarse de la vigencia de los criterios de evaluación precedentes. Las normas GAFI[40] permiten a los países excluir el riesgo país de esta evaluación si la institución financiera está sujeta a las normas PBC/FT de todo el grupo y supervisada a escala del grupo por su supervisor financiero.

III. Subcontratación/agencia

9. Los bancos podrán aplicar directamente procedimientos de identificación y otros procesos CDD o designar a uno o más terceros para que apliquen esas medidas en su nombre, a veces mediante una relación de agencia. Aunque las funciones de cumplimiento de PBC/FT pueden ser desarrolladas por terceros, la responsabilidad de satisfacer los requisitos CDD y PBC/FT continúa recayendo en el banco. El grado en que se utilizan terceros suele depender del modelo de negocio del banco; normalmente, los bancos que operan por teléfono o internet o que tienen pocas sucursales físicas suelen utilizar terceros en mayor medida. Los bancos podrán utilizar terceros para ampliar su base de clientes o mejorar la asistencia prestada a éstos y el acceso general a sus servicios.

10. Los bancos que decidan utilizar terceros deberán asegurarse de la existencia de un acuerdo por escrito que establezca las obligaciones PBC/FT del banco y la forma en que el tercero las ejecutará. En algunos países, la relación entre bancos y terceros está regulada.

11. Como se señaló anteriormente, es importante que los bancos entiendan la diferencia entre utilizar un tercero como agente y recurrir a los procesos de identificación de clientes y CDD de otro banco. Con arreglo a la legislación sobre agente y principal, el agente suele ser una prolongación legal del banco. Cuando el cliente o potencial cliente de un banco trata con un agente del banco, legalmente está tratando con el propio banco. Por tanto, el tercero estará obligado a aplicar las políticas y requisitos del banco con respecto a la identificación y verificación y a la CDD.

12. En la práctica, los terceros utilizados por los bancos deberán disponer de destrezas, conocimientos y formación necesarios para aplicar las medidas de identificación de clientes y CDD del banco. En algunos casos, cuando los modelos de negocio de los terceros se basan en prestar sus servicios a varios bancos, aquéllos suelen desarrollar importantes destrezas internas propias. Sin embargo, los terceros no siempre están sujetos a obligaciones PBC/FT, aunque muchos suelen estarlo. Sea o no éste el caso, el tercero siempre está en disposición de aplicar los requisitos de identificación y CDD de su principal (que, a su vez, deben satisfacer los requerimientos legales).

13. Los intermediarios en depósitos minoristas, agentes hipotecarios y abogados son algunos ejemplos de terceros utilizados habitualmente por los bancos para cumplir las obligaciones de identificación de clientes. La mitigación del riesgo BC/FT puede verse comprometida cuando los bancos no se aseguran de que los terceros aplican los requisitos de identificación de clientes y CDD aplicables.

14. Como se señaló, deberá existir un convenio o acuerdo por escrito que documente las responsabilidades del tercero y que deberá incluir lo siguiente:

[40] Véase la Recomendación 17 de las normas GAFI.

(a) exigencia de la aplicación de los requisitos de identificación de clientes y CDD del banco (incluidas indagaciones sobre la fuente de fondos y riqueza, cuando proceda);

(b) garantía de que, cuando el cliente esté presente en persona en el momento en que se practique la identificación de clientes y/o las medidas CDD, el tercero aplica procedimientos de identificación de clientes que incluyen la inspección de los documentos de identificación originales cuando la regulación o el banco así lo requieran;

(c) garantía de que, cuando el cliente no esté presente en el momento de verificar su identidad, el tercero aplica todos los requisitos de identificación de clientes no presentes preceptivos o estipulados por el banco que resulten aplicables; y

(d) garantía de que el tercero mantiene la confidencialidad sobre la información de clientes.

15. Los bancos también deberán:

(a) garantizar que si el tercero es responsable de determinar y/o identificar al beneficiario efectivo o a una PEP, estas responsabilidades se encuentran documentadas;

(b) garantizar que el tercero proporciona al banco información sobre la identificación de clientes en los plazos establecidos;

(c) examinar o auditar periódicamente, de manera sistemática, la calidad de la información sobre clientes recopilada y documentada por el tercero para garantizar que continúa cumpliendo los requisitos del banco; e

(d) identificar claramente los casos que el banco consideraría incumplimiento de sus obligaciones contractuales por parte del tercero y establecer un proceso de adopción de medidas oportunas, como revocar la relación en respuesta a fallos identificados.

16. El banco deberá obtener oportuna y puntualmente del tercero toda la información relevante y cerciorarse de que la información es completa y se mantiene actualizada en los registros de clientes del banco.

17. Los contratos con terceros deberán revisarse y actualizarse según proceda para garantizar que continúan recogiendo con exactitud las atribuciones de los terceros y reflejando cualquier actualización de sus funciones.

Anexo 2

Corresponsalía bancaria

I. Consideraciones generales sobre banca corresponsal

1. Conforme al Glosario del GAFI, «la banca corresponsal consiste en la provisión de servicios bancarios por un banco (el «banco corresponsal») a otro banco (el «banco correspondiente»)».

2. Las cuentas corresponsales, utilizadas en todo el mundo, permiten a los bancos correspondientes realizar negocios y prestar servicios[41] que no pueden ofrecer directamente (por falta de una red internacional). Las cuentas corresponsales que requieren especial atención son las relacionadas con la prestación de servicios en jurisdicciones en las que los bancos correspondientes no tienen presencia física.

3. El banco corresponsal procesa/ejecuta transacciones para los clientes del banco correspondiente. El banco corresponsal no tiene por lo general relaciones comerciales directas con los clientes del banco correspondiente, que pueden ser particulares, sociedades o empresas de servicios financieros. El cliente del banco corresponsal es el banco correspondiente.

4. Dada la estructura de esta actividad y la limitada información disponible sobre la naturaleza o finalidad de las transacciones subyacentes, los bancos corresponsales pueden verse expuestos a determinados riesgos vinculados al blanqueo de capitales y la financiación del terrorismo (riesgos BC/FT).

II. Evaluación del riesgo BC/FT de la banca corresponsal: recogida de información

5. Los bancos que realicen actividades de banca corresponsal deberán practicar una adecuada evaluación de los riesgos BC/FT asociados a esas actividades y, consiguientemente, aplicar las oportunas medidas de diligencia debida a clientes (CDD).

6. Los bancos corresponsales deberán recabar información suficiente, al inicio de su relación y de forma continuada después, sobre sus bancos correspondientes a fin de conocer cabalmente la naturaleza de su negocio y poder evaluar en todo momento correctamente los riesgos BC/FT

7. Entre los factores que deberán considerar los bancos corresponsales se incluyen:

(a) la jurisdicción donde se ubica el banco correspondiente;

(b) el grupo al que pertenece el banco correspondiente y las jurisdicciones en las que puedan ubicarse las filiales y sucursales del grupo;

[41] Tales como «gestión de tesorería (por ejemplo, cuentas que devengan intereses en una serie de divisas), transferencias internacionales, compensación de cheques, cuentas de transferencia de pagos en otras plazas y servicios en moneda extranjera», según recoge el Glosario del GAFI.

(c) información sobre la gestión y propiedad del banco correspondiente (especialmente la presencia de beneficiarios efectivos o PEP), su reputación[42], principales actividades comerciales, clientes y establecimientos;

(d) la finalidad de los servicios prestados al banco correspondiente;

(e) el negocio del banco, incluidos sus mercados objetivo y base de clientes;

(f) la situación y calidad de la regulación y supervisión bancaria en el país del banco correspondiente (especialmente la legislación y regulación sobre PBC/FT);

(g) las políticas y procedimientos de prevención y detección del blanqueo de capitales del banco correspondiente, incluida una descripción de la CDD practicada por éste a sus clientes;

(h) la capacidad de conocer la identidad de cualquier tercero facultado para utilizar los servicios de corresponsalía bancaria;

(i) la posible utilización de la cuenta por otros bancos correspondientes dentro de una relación de banca corresponsal «anidada»[43].

8. La información sobre políticas y procedimientos PBC/FT podrá basarse en un cuestionario cumplimentado por el banco correspondiente o en información de dominio público facilitada por éste (como información financiera o información preceptiva a efectos supervisores).

III. Requisitos de diligencia debida con clientes

9. Si los bancos corresponsales no aplicasen un adecuado nivel de diligencia debida a sus relaciones de corresponsalía bancaria, podrían incurrir en mantenimiento y/o transmisión de capitales vinculados a actividades ilícitas.

10. Todas las relaciones de corresponsalía bancaria deberán someterse a un adecuado nivel de CDD. Los bancos no deberán considerar el proceso CDD como un «ejercicio de recogida de papel», sino como una evaluación real del riesgo BC. La recogida de información deberá concluir, si es necesario, con la celebración de reuniones con la dirección y el responsable de cumplimiento del banco correspondiente local, así como con su regulador/supervisor, unidades de inteligencia financiera y otras agencias públicas competentes.

11. La información CDD también deberá revisarse y actualizarse periódicamente, con arreglo al enfoque en función del riesgo. Esta información deberá utilizarse para actualizar el proceso de evaluación de riesgos del banco.

[42] La reputación podrá incluir medidas/sanciones civiles, administrativas o penales (multas, amonestaciones, etc.) dictadas por un tribunal o autoridad supervisora.

[43] La banca corresponsal anidada hace referencia a la utilización de una relación de banca corresponsal por parte de una serie de bancos correspondientes mediante sus relaciones con el banco directamente correspondiente para realizar transacciones y acceder a otros servicios financieros.

IV. Aceptación de clientes

12. La decisión de establecer (o continuar) una relación de corresponsalía bancaria deberá ser aprobada por la alta dirección del banco corresponsal.

13. La información podrá proceder de informes de evaluación mutua y declaraciones del GAFI sobre jurisdicciones identificadas por éste como sujetas a medidas correctivas o con deficiencias estratégicas PBC/FT. Los informes de evaluación mutua de organismos regionales análogos al GAFI también podrán aportar dicha información. Los bancos también podrán utilizar cualquier información de dominio público procedente de las autoridades nacionales competentes. Deberá tenerse en cuenta el hecho de que un país esté sujeto a medidas restrictivas, especialmente si existen prohibiciones a la prestación de servicios de banca corresponsal. Los bancos corresponsales deberán prestar especial atención cuando establezcan o mantengan relaciones con bancos correspondientes ubicados en jurisdicciones con normas PBC/FT deficientes o identificadas como «no dispuestas a cooperar» en la lucha contra el blanqueo de capitales y la financiación del terrorismo.

14. Los bancos corresponsales deberían negarse a establecer o continuar una relación de banca corresponsal con un banco constituido en una jurisdicción en la que éste no tenga presencia física y que no forme parte de un grupo financiero regulado (es decir, bancos simulados).

V. Seguimiento continuo

15. El banco corresponsal deberá implantar políticas y procedimientos adecuados que le permitan detectar cualquier actividad incongruente con la finalidad de los servicios prestados al banco correspondiente o contraria a los compromisos que puedan haber pactado el corresponsal y el correspondiente.

16. Si el banco corresponsal decidiera permitir a terceros el uso directo de cuentas de corresponsalía para negocios propios de éstos (por ejemplo, cuentas de transferencia de pagos en otras plazas), deberá intensificar el seguimiento de estas actividades con arreglo a sus riesgos específicos. El banco corresponsal deberá verificar que el banco correspondiente ha practicado una adecuada CCD a los clientes con acceso directo a las cuentas del banco corresponsal y que el banco correspondiente está capacitado para ofrecer información CDD relevante a solicitud del banco corresponsal.

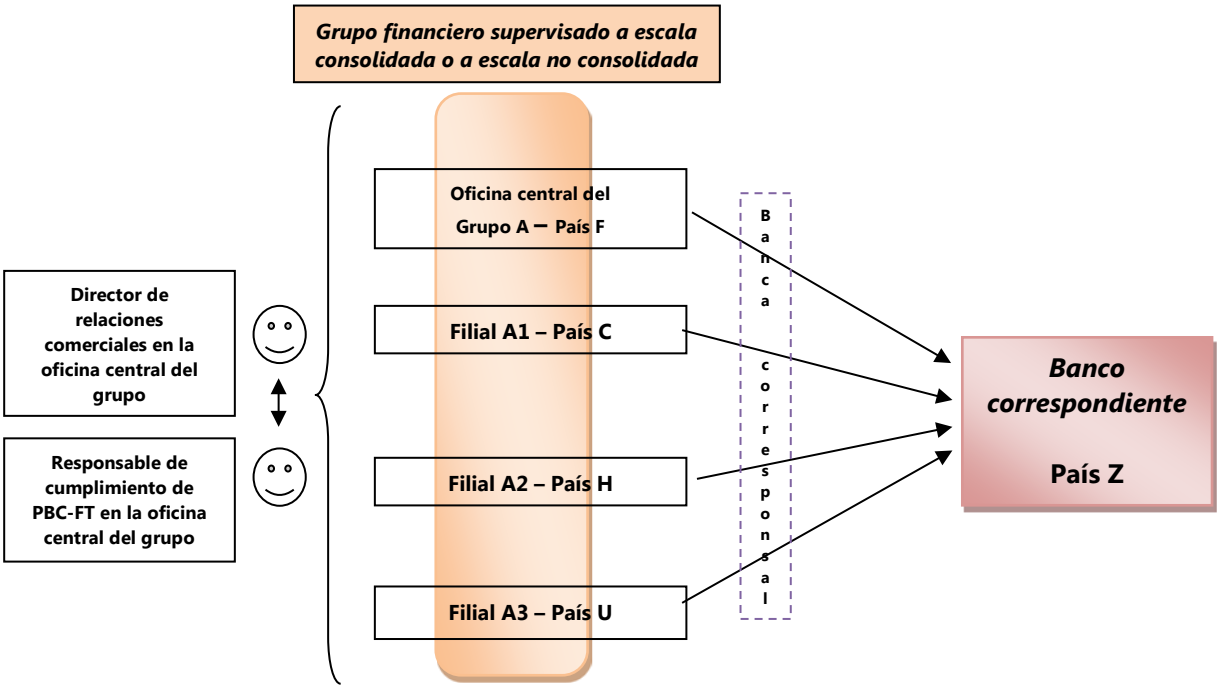
17. La alta dirección deberá ser periódicamente informada de las relaciones de corresponsalía bancaria de alto riesgo y del seguimiento a que están sometidas.

VI. Consideraciones a escala de grupo y transfronterizas

18. Si el banco correspondiente mantiene relaciones de corresponsalía bancaria con varias entidades pertenecientes al mismo grupo[44] (caso 1), la oficina central del grupo deberá prestar especial atención a que las evaluaciones de riesgos realizadas por las diferentes entidades del grupo sean congruentes con la política de evaluación de riesgos para todo el grupo. La oficina central del grupo deberá coordinar el seguimiento de la relación con el banco correspondiente, particularmente en el caso

[44] Cada entidad presta un servicio de banca corresponsal en su país de acogida.

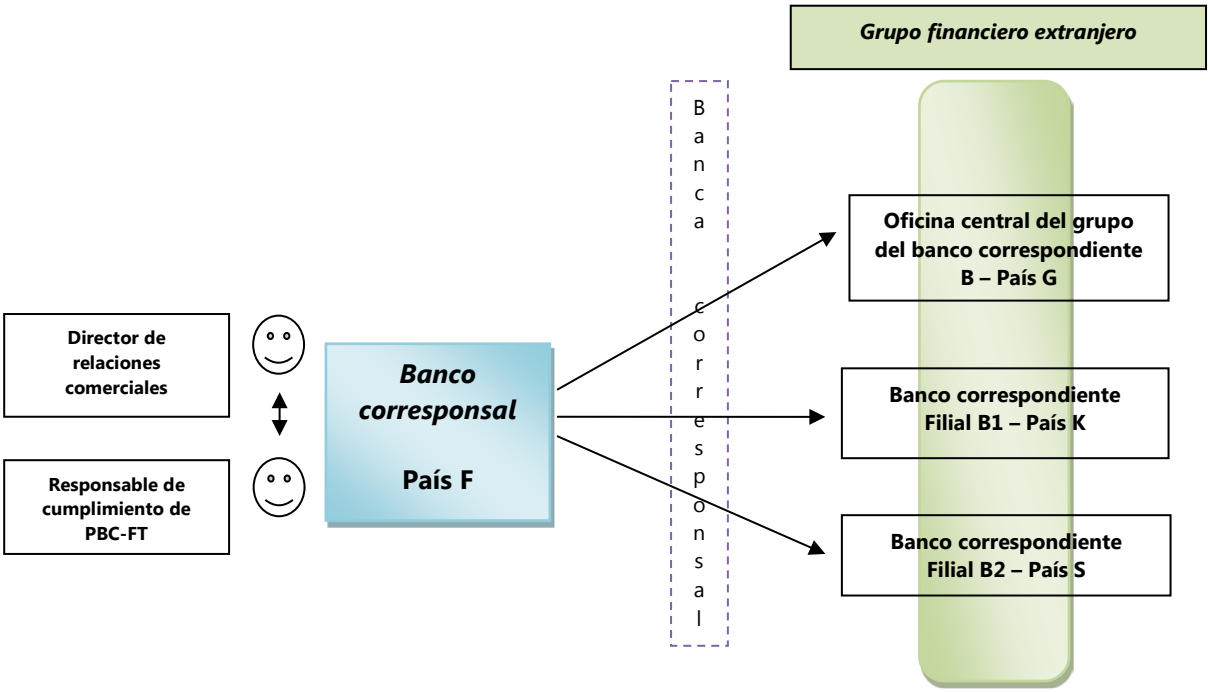
de una relación de alto riesgo, y cerciorarse de la existencia de mecanismos adecuados de intercambio de información dentro del grupo.



Caso 1

19. Si el banco corresponsal mantiene relaciones comerciales con varias entidades pertenecientes al mismo grupo pero ubicadas en diferentes países de acogida (caso 2), el banco corresponsal deberá tener en cuenta el hecho de que esas entidades pertenecen al mismo grupo. Aun así, el banco corresponsal deberá también evaluar los riesgos BC/FT planteados por cada relación comercial.

Caso 2



VII. Gestión del riesgo

20. El banco deberá aplicar procedimientos específicos para gestionar las relaciones de corresponsalía bancaria. Las relaciones comerciales deberán formalizarse mediante acuerdos por escrito que definan con claridad las funciones y responsabilidades de los socios bancarios.

21. La alta dirección también deberá conocer las competencias y funciones de los diferentes servicios (líneas de negocio, responsables de cumplimiento (incluido el responsable ejecutivo de PBC/FT y el responsable de PBC/FT del grupo), auditoría, etc.) dentro del banco con respecto a las actividades de banca corresponsal.

22. Las funciones de auditoría interna y cumplimiento del banco [45] tienen importantes responsabilidades en materia de evaluación y certificación del cumplimiento de los procedimientos relacionados con las actividades de banca corresponsal. Los controles internos deberán incluir las medidas de identificación de los bancos correspondientes, la recogida de información, el proceso de evaluación del riesgo BC/FT y el seguimiento continuo de las relaciones de corresponsalía bancaria.

[45] Véanse *The internal audit function in banks*, junio de 2012, y el Principio 26 sobre control interno y auditoría en los *Principios básicos para una supervisión bancaria eficaz*, septiembre de 2012.

Anexo 3

Listado de Recomendaciones relevantes del GAFI

Nuevas Recomendaciones del GAFI (incluidas sus notas interpretativas)
• R. 1: Evaluación del riesgo y aplicación de un enfoque en función del riesgo
• R. 2: Cooperación nacional y coordinación
• R. 9: Legislación sobre el secreto profesional de las instituciones financieras
• R. 10: Debida diligencia con clientes
• R. 11: Mantenimiento de registros
• R. 12: Personas Políticamente Expuestas (PEP)
• R. 13: Corresponsalía bancaria
• R. 15: Nuevas tecnologías
• R. 16: Transferencias electrónicas
• R. 17: Recurso a terceros
• R. 18: Controles internos, y sucursales y filiales en el extranjero
• R. 20: Notificación de transacciones sospechosas
• R. 26: Regulación y supervisión de instituciones financieras
• R. 40: Cooperación internacional