Sin nombre
2.2. Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo del Comité de Basilea
AREA III
2. Enfoque basado en riesgos (contexto internacional)
2.2. Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo del Comité de Basilea
0

## 2.2. ADECUADA GESTIÓN DE LOS RIESGOS RELACIONADOS CON EL BLANQUEO DE CAPITALES Y LA FINANCIACIÓN DEL TERRORISMO DEL COMITÉ DE BASILEA[15]

### 1. Introducción

El Comité de Basilea publica las Directrices sobre la forma en que los bancos deben incluir el BC/FT dentro de su gestión global de riesgo. Dicho comité promueve la aplicación de políticas y procedimientos sólidos para la prevención del blanqueo de capitales PBC/FT, las cuales son fundamentales para proteger la seguridad y la solvencia de los bancos y la integridad del sistema financiero internacional.

Las directrices se dirigen específicamente a bancos, grupos y supervisores bancarios.

El Comité de Basilea contribuye a la adopción de las normas del GAFI; por tanto, las directrices incorporan tanto las normas del GAFI, así como los Principios Básicos de Basilea aplicables a los bancos con operativa transfronteriza y el margo general de la supervisión bancaria.[16]

Una sólida gestión del riesgo de BC/FT es relevante para la seguridad y solvencia de los bancos y del sistema bancario, el principal objetivo de la supervisión bancaria, dado que:

**a)** Contribuye a proteger la reputación de los bancos y de los sistemas bancarios nacionales, al evitar y disuadir su utilización para blanquear fondos movilizar recursos en apoyo al terrorismo, y

**b)** Preserva la integridad del sistema financiero internacional, así como las actuaciones de los gobiernos para combatir la corrupción y la financiación del terrorismo.

La insuficiencia o ausencia de una sólida gestión del riesgo de BC/FT implica riesgos a los bancos, principalmente de reputación, operacional, de cumplimiento y de concentración. Todos los riesgos están relacionados entre sí.

Las Directrices aplican a todos los bancos; sin embargo, algunos de los requisitos pueden requerir una adaptación por tamaño o especialización de la institución.

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

Todos los bancos están obligados a contar con políticas y procesos adecuados, incluidas las CDD –debida diligencia del cliente–, para promover normas éticas y profesionales de alto nivel e impedir que el banco sea utilizado con fines delictivos.

Los bancos están obligados a contar con sólidos programas de gestión de todo tipo de riesgos, incluidos los de BC/FT. Disponer de políticas y procesos adecuados exige la aplicación de otras medidas adicionales a las normas CDD, las cuales deben ser proporcionales y estar en función del riesgo. Las Directrices del Comité de Basilea señala sobre esas medidas.

**a)** Evaluación, comprensión, gestión y mitigación de los riesgos:

- Evaluación y comprensión de los riesgos:
  - La sólida gestión de riesgo exige la identificación y análisis de los riesgos BC/FT en el banco, así como el diseño y eficaz aplicación de las políticas y procedimientos acordes con los riesgos identificados.

    En el análisis integral de evaluación de los riesgos, el banco debe considerar todos los factores de riesgo relevantes, inherentes y residuales, a escala nacional, sectorial, bancaria y de relación comercial, a efecto de determinar su perfil de riesgo y el adecuado nivel de mitigación que se aplicará.

    Las políticas y procedimientos del CDD, aceptación de clientes, identificación de clientes y seguimiento de las relaciones comerciales, deben considerar la evaluación del riesgo y el perfil de riesgo del banco.
  - El banco debe desarrollar el conocimiento de los riesgos BC/FT inherentes a los clientes, productos, canales de distribución, servicios ofrecidos y jurisdicciones que las que los clientes realizan negocios. Este conocimiento debe basarse en datos contratos de operaciones y transacciones, fuentes internas, externas, evaluaciones del riesgo nacionales e informes sobre países elaborados por organismos internacionales.

    Las políticas y procedimientos de aceptación de clientes, diligencia debida y seguimiento, deberán diseñarse y aplicarse para controlar los riesgos inherentes identificados.

    Cualquier riesgo residual resultante debe gestionarse en consonancia con el perfil de riesgo determinado por el banco establecido en su evaluación de riesgos.
- Mecanismos de gobierno adecuados:
  - La eficaz gestión del riesgo BC/FT exige, por ejemplo: que el consejo de administración **(i)** apruebe y supervise las políticas en materia de riesgos, gestión y cumplimiento; **(ii)** comprenda los riesgos BC/FT**; (iii)** conozca la información sobre la evaluación de riesgos, para que adopte decisiones informadas; **(iv)** asigne competencias explícitas según la estructura, y **(v)** nombrar, en conjunto con la alta dirección, al responsable ejecutivo de PBC/FT con la preparación adecuada, categoría y autoridad para que sus decisiones reciban la atención del consejo, de la alta dirección y de las líneas de negocio.
- Tres líneas de defensa:
  - Primera línea de defensa: las unidades de negocio que tienen contacto directo con los clientes, encargadas de identificar, evaluar y controlar los riesgos de sus actividades.

    El personal debe conocer y aplicar las políticas y procedimientos, así como disponer de recursos suficientes, para cumplir eficazmente sus funciones.

    Las políticas y procedimientos se deben especificar y comunicar a todo el personal, describiendo las obligaciones de los empleados e instrucciones, además de estar orientadas a que el banco cumpla la regulación. Deben existir procedimientos para detectar y notificar transacciones sospechosas.

    El banco debe disponer de políticas y procesos adecuados para seleccionar al personal, con la finalidad de garantizar principios éticos y profesionales.

    El banco debe implementar programas de capacitación y actualización del personal, diseñados con base en las necesidades y el perfil de riesgo de la entidad, dependiendo de los cargos y funciones de los empleados, antigüedad. El alcance y frecuencia de los programas deben adaptarse a los factores de riesgos a los que los empleados están expuestos. Los programas deben incluir a los empleados de nuevo ingreso.
  - Segunda línea de defensa: el responsable de PBC/FT (en lo sucesivo, el “Ejecutivo” –oficial de cumplimiento–), a la función de cumplimiento, así como los recursos humanos y tecnológicos.

El responsable ejecutivo es responsable del seguimiento continuo de las obligaciones PBC/FT, lo que implica monitoreo de cumplimiento y examen de los informes de anomalías, para alertar al consejo de administración o alta dirección. Asimismo, es responsable de notificar las transacciones sospechosas.

El responsable Ejecutivo debe ser el contacto directo con las autoridades, incluidas las que supervisen y la UIF.

Los intereses comerciales del banco no deben oponerse al eficaz desempeño del Ejecutivo; deben evitarse los conflictos de interés, por lo que éste no deberá, por ejemplo asumir competencias en las líneas de negocio, protección de datos o auditoría interna.

Ante cualquier conflicto entre negocio y el Ejecutivo, deben existir procedimientos en los que las cuestiones PBC/FT reciban consideración objetiva al más alto nivel.

El Ejecutivo rinde cuentas a la alta dirección o al consejo de administración; debe contar con los recursos necesarios para ejercer su función.

- Tercera línea de defensa: auditoría interna, la cual evalúa en forma periódica e independiente la gestión y los controles del riesgo, rindiendo cuentas al comité de auditoría del consejo de administración.

  El banco debe implementar políticas para la realización de auditorías sobre: **(i)** la adecuación de las políticas y procedimientos para tratar los riesgos identificados; **(ii)** la eficacia de la aplicación de las políticas y procedimientos; **(iii)** la eficacia de la vigilancia del cumplimiento y del control de calidad; **(iv)** la eficacia de los programas de formación del personal relevante, y **(v)** evaluar el sistema de tecnologías de la información (TI).

  La alta dirección debe asegurarse de que las funciones de auditoría interna se le asignen a personal experto y con experiencia, así como que el alcance, la metodología y la frecuencia de las auditorías se adecuan al perfil del riesgo del banco. Lo mismo aplica para los auditores externos.

- Adecuado sistema de seguimiento de transacciones:
  - El banco debe disponer de un sistema de seguimiento acorde con su tamaño, actividades y complejidad, que incluya el perfil de riesgo BC/FT.

    Si un banco considera que no es necesario un seguimiento basado en las TI, debe documentar la resolución adoptada, así como demostrar al supervisor o al auditor externo que dispone de una alternativa eficaz.

    El sistema TI debe incluir todas las cuentas de los clientes y las transacciones; por lo que deberá permitir el análisis de las tendencias e identificar relaciones comerciales y transacciones anómalas para el BC/FT.
  - El sistema debe ofrecer información fidedigna a la alta dirección sobre temas cruciales, incluidos cambios en el perfil de los clientes.

    El sistema TI debe proporcionar al banco un repositorio centralizado de información –clientes; productos; transacciones–, para la clasificación de los clientes en función de su riesgo y gestionar alertas.

    Un sistema adecuado de TI utiliza parámetros basados en la experiencia nacional e internacional sobre los métodos y prevención BC/FT. Sin perjuicio de que el banco utilice los parámetros estándar del diseñador del sistema, este debe considerar la situación de riesgo específica del banco.
  - El sistema de seguimiento TI debe permitir al banco determinar sus criterios para seguimientos adicionales, elaborar informes de transacciones sospechosas o adoptar otras medidas para minimizar el riesgo.
  - Los parámetros del sistema TI deben permitir la generación de alertas sobre transacciones anómalas.

**b)** Política de aceptación de clientes:

- El banco debe desarrollar políticas y procedimientos de aceptación de clientes para identificar los susceptibles de representar un mayor riesgo BC/FT conforme a la evaluación de riesgos del banco. Dichas políticas y procedimientos permiten elaborar perfiles de riesgo de clientes o de categorías.
- Las políticas y procedimientos deben exigir una diligencia debida básica con todos los clientes y una diligencia debida proporcionada conforme varíe el nivel de riesgo asociado al cliente.
- La política de aceptación de cliente no debe ser restrictiva para que no perjudique el acceso del público en general a los servicios bancarios, en especial a los grupos financieros o socialmente desfavorecidos.
- La política de aceptación de clientes del banco debe determinar las circunstancias en las cuales el banco no aceptará una nueva relación comercial o cancelará una relación ya existente.
- Para determinar el nivel de riesgo del cliente se deben considerar: antecedentes del cliente, ocupación (incluido si ocupa puesto relevante en el sector público o privado), fuentes de riqueza, países de origen y de residencia (cuando difieran), productos utilizados, naturaleza y finalidad de las cuentas, cuentas vinculadas, actividades comerciales, y otros indicadores de riesgo.
- Se pueden aceptar medidas simplificadas de identificación del cliente, siempre que la legislación lo permita.
- Se deben adoptar medidas reforzadas cuando los riesgos de los clientes sean más elevados. Una diligencia debida reforzada aplica en el caso de saldos elevados en una cuenta, en el caso de que se realicen regularmente transferencias electrónicas transfronterizas, o en el caso de un PEP. Siempre se aplicarán medidas reforzadas tratándose de PEP extranjeros.

**c)** Identificación, verificación y elaboración del perfil de riesgo de clientes y beneficiarios efectivos:

- El cliente es cualquier persona que entabla una relación comercial o realiza una transacción financiera ocasional con el banco. La CDD aplica también a las personas que actúen por cuenta de los clientes y a los beneficiarios efectivos (Recomendación 10 del GAFI),[17] por tanto, los bancos deben identificar a los clientes, incluyendo a cualquier persona que actúe a su nombre y al beneficiario activo.
- Para verificar la identidad del cliente se debe implementar un procedimiento sistemático, mediante documentos, datos o informaciones fiables e independientes. Cuando se recurra a fuentes distintas (comprobación de referencias con otras instituciones financieras y la obtención de estados financieros), debe cuidarse que ello sea consistente con las políticas y procedimientos del banco, así como el perfil del cliente. El banco no debe recurrir únicamente a las declaraciones de los clientes.
- Nunca se puede relevar el procedimiento de identificación y verificación.
- El banco no debe establecer una relación bancaria ni realizar transacción hasta que la identidad del cliente haya sido establecida y verificada (Recomendación 10 del GAFI). Si el banco no es capaz de completar las medidas CDD debe abstenerse de abrir la cuenta, iniciar relaciones comerciales o realizar transacciones. El banco no debe abrir cuentas con personas que insistan en el anonimato.
- Existen circunstancias en las que sería aceptable completar la verificación de identidad después de iniciada la relación, supuesto en el que el banco debe adoptar un procedimiento adecuado de gestión del riesgo; asimismo, en casos en que la cuenta haya sido abierta, pero surjan problemas de verificación en el transcurso de la relación comercial, que no pueden ser resueltos, el banco debe cerrar la cuenta o bloquear el acceso a la misma.
- Los bancos deben contar con políticas y procedimientos de CDD suficientes para elaborar perfiles de riesgo concretos o determinadas categorías de clientes; la información que se recabe debe estar

determinada por el nivel de riesgo asociado al modelo de negocio y actividades del cliente, los productos y servicios financieros demandados por el cliente.

- Los perfiles de riesgo permiten al banco determinar si el cliente o categoría de clientes tiene un alto riesgo y, en consecuencia, le son aplicables medidas y controles reforzados. Asimismo, los perfiles facilitan la identificación de cualquier actividad en las cuentas que se desvíe de la actividad normal y que podría considerarse anómala o, incluso, sospechosa.
- Los perfiles deben reflejar el conocimiento de la finalidad y naturaleza de la relación comercial o transacción ocasional, volumen previsto, tipo de transacción y la fuente de los fondos o riqueza.
- Lo bancos deben elaborar un reporte de operaciones sospechosas en los casos en que existan problemas para completar las medidas CDD, así como cuando las comprobaciones CDD levanten sospechas en cuanto a que los recursos del futuro cliente proceden de delitos BC/FT, supuesto en el que notificará a las autoridades y no permitirá que el cliente se informe de dicha situación.
- El banco debe disponer de procedimientos y recursos materiales para permitir que el personal que tiene contacto con los clientes, identifique cualquier entidad o individuo designado como terroristas u organizaciones terroristas.
- No obstante que los fondos de un cliente provengan de otro banco con las mismas normas CDD, aun así debe practicarse la debida diligencia. Si un banco tiene motivos para pensar que otro banco ha negado servicios bancarios al cliente por considerarlo como de alto riesgo, debe considerar a este cliente como de alto riesgo y aplicar procedimientos reforzados de debida diligencia, elaborar un reporte de operaciones sospechosas y/o no aceptar al cliente.
- Las cuentas confidenciales numeradas deben estar sujetas a los mismos procedimientos CDD que las demás cuentas de los clientes, aun cuando los procedimientos los lleve a cabo un personal especializado.
- El banco debe garantizar que las unidades internas de control, cumplimiento, auditoría y otras funciones de vigilancia, el Ejecutivo y los supervisores, tienen pleno acceso a la información.

**d)** Seguimiento continuo:

- El banco solo puede gestionar sus riesgos BC/FT si conoce la actividad bancaria razonable y normal de sus clientes, y puede identificar transacciones intentadas y anómalas que trascienden su patrón habitual. Sin ese elemento el banco no puede cumplir con la obligación de identificar y notificar las transacciones sospechosas.
- El alcance del seguimiento debe estar en función del riesgo identificado en la evaluación de riesgos; asimismo, debe reforzarse el seguimiento de clientes o transacciones de alto riesgo.
- El banco también debe hacer un seguimiento transversal de los productos o servicios, con el fin de identificar y mitigar los patrones de riesgo emergentes.
- Todos los bancos deben disponer de sistemas para detectar transacciones anómalas o sospechosas; al diseñar escenarios para identificar esas actividades, el banco debe considerar el perfil de riesgo del cliente a partir de la evaluación de riesgos, la información recabada de CDD y otra información de agencias policiales y autoridades en su jurisdicción.
- Utilizando la información CDD, los bancos deben ser capaces de identificar transacciones que no tienen sentido.
- La capacidad del banco para vigilar e identificar eficazmente las actividades sospechosas, requiere el acceso de perfiles y registros actualizados de los clientes.
- Los sistemas integrados de gestión de información deben ser proporcionales al tamaño, estructura y complejidad, basados en riesgos, que ofrezcan a las unidades de negocio y a los responsables de riesgos o cumplimiento, información oportuna para identificar, analizar y realizar un seguimiento eficaz de las cuentas de los clientes.

- Los bancos deben cotejar los datos de los clientes cuando haya modificaciones en los listados de sanciones, para detectar PEP extranjeros y cuentas de alto riesgo, para practicar DD reforzada.

**e)** Gestión de la información:

- Mantenimiento de registros:
  - El banco debe garantizar el registro de toda la información recabada en el contexto del CDD.
  - Los registros deben cumplir con las reglas establecidas por el banco para estos efectos (las reglas deben tener en cuenta las medidas aplicables en materia de privacidad). Las reglas deben incluir el tipo de información que se debe registrar, el periodo de conservación no menor a cinco años.
  - Aun en el caso de cancelación de cuentas, investigación o litigios, los registros deben conservarse.
  - El mantenimiento y actualización de registros es fundamental para vigilar la relación con el cliente, comprender su negocio y actividades recurrentes y, en caso necesario, aportar un registro de auditoría en caso de acciones legales o investigaciones.
  - También deberá conservarse registro del proceso de evaluación del análisis y seguimiento continuo, de tal modo que permitan demostrar el cumplimiento de los requisitos CDD y su capacidad para gestionar el riesgo.
- Actualización de la información:
  - La garantía de que los registros mantienen fiabilidad, vigencia y actualización de la información CDD, otras autoridades, agencias policiales o las UIF, podrán hacer un uso eficaz para sus funciones; así como también, al banco, vigilar las actividades anómalas o sospechosas de la cuenta.
- Suministro de información a los supervisores:
  - El banco debe demostrar a los supervisores la adecuación de sus sistemas de evaluación, gestión y mitigación de riesgos; la política de aceptación de clientes; los procesos de seguimiento continuo y los procedimientos para notificar transacciones sospechosas, así como las medidas en el contexto de PBC/FT.

**f)** Notificación de transacciones sospechosas y bloqueo de activos:

- Notificación de transacciones sospechosas:
  - El seguimiento y análisis continuo de cuentas y transacciones permite a los bancos identificar operaciones sospechosas, eliminar falsos positivos y notificar con rapidez transacciones sospechosas. El proceso de identificación, investigación y notificación de transacciones sospechosas debe especificarse en las políticas y procedimientos y difundirse entre todo el personal.
  - También deben existir procedimientos para evaluar si la transacción debe notificarse a las agencias policiales, o supervisores.
  - Los procedimientos deberán incluir el principio de confidencialidad, que la investigación se desarrolla con rapidez, que los informes contienen información relevante y se elaboran y notifican oportunamente. El Ejecutivo PBC/FT deberá garantizar una notificación rápida cuando los fondos u otros activos sospechosos de proceder de actividades delictivas, se mantengan en una cuenta.
  - Además de notificar la actividad sospechosa, el banco deberá garantizar la adopción de medidas para mitigar el riesgo de que sea utilizado en actividades delictivas.
- Bloqueo de activos:

- El banco debe ser capaz de identificar y cumplir el bloqueo de fondos adoptado por la autoridad. No deberá mantener relación con entidades o individuos designados (terroristas, organizaciones terroristas).
- Antes de establecer una relación comercial o al realizar una transacción ocasional con clientes, el banco debe comprobar si estos figuran en listados de terroristas conocidos o presuntos. El seguimiento continuo permite verificar que los clientes actuales del banco no figuren en esos listados.
- Todos los bancos deben contar con sistemas para detectar transacciones prohibidas (transacciones con entidades designadas en las resoluciones del Consejo de Seguridad de la ONU o en los listados de sanciones nacionales).
- La detección de terroristas no es una medida de diligencia debida sensible al riesgo, por lo que debe realizarse independientemente del perfil de riesgo atribuido al cliente. Los bancos deben bloquear sin demora y previo aviso los fondos o activos de las personas designadas.

## 3. PBC/FT a escala de grupo[18] y en un contexto transfronterizo

- Cuando un banco opera en otras jurisdicciones, la sólida gestión del riesgo BC/FT implica tener en cuenta los requisitos legales del país en el que opera.
- Cada grupo debe desarrollar políticas y procedimientos PBC/FT a escala del grupo, con una aplicación y supervisión coherentes en todo el grupo; en ese sentido, las políticas y procedimientos en sucursales y filiales deben ser coherentes con las políticas y procedimientos generales para todo el grupo, sin que, en el caso de que los requisitos de la jurisdicción en donde opera sean más estrictos que los del grupo, se cumplan.

**a)** Proceso global para la gestión del riesgo de clientes:

- La gestión consolidada del riesgo implica establecer y determinar 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 objetivo general es identificar, vigilar y mitigar los riesgos en todo el grupo.
- Debe existir un sistema de intercambio de información entre la oficina central y todas las sucursales y filiales; los bancos deben estar autorizados a intercambiar información sobre sus clientes.
- En el caso de que un país no permita la adecuada aplicación de normas, el ejecutivo debe informar a los supervisores de origen y, en su caso, debe procederse a la cancelación de las operaciones del grupo financiero en el país que no permite el intercambio de información o aplicación de medidas.

**b)** Evaluación y gestión del riesgo:

- El banco debe conocer todos los riesgos asociados a los clientes (ubicación geográfica, patrones de transacciones, productos y servicios utilizados, clientes de alto riesgo) en todo el grupo, individualmente o por categorías. Esa información debe actualizarse periódicamente y en consistencia con el nivel y naturaleza del riesgo en el grupo.
- Los criterios de identificación de clientes de alto riesgo, deben ser los mismos para todo el grupo, así como las evaluaciones de riesgos asociadas.
- La información recabada en el proceso de evaluación debe utilizarse para determinar el nivel y naturaleza de riesgo total del grupo y facilitar el diseño de controles.

- La auditoría interna o externa, así como el Ejecutivo, deben evaluar el cumplimiento PBC/FT del grupo (incluido el intercambio de información).
- Los grupos bancarios internacionales deben garantizar que disponen de una sólida unidad de auditoría interna y función de cumplimiento global.
- Debe existir un Ejecutivo responsable del cumplimiento PBC/FT tanto en el ámbito nacional e internacional (responsable de PBC/FT del grupo).

**c)** Políticas y procedimientos PBC/FT a escala consolidada:

- El banco no debe recurrir a normas menos estrictas que las que rigen sus propios procedimientos PBC/FT; podrá sopesarse conceder un mayor grado de fiabilidad a la información suministrada en la otra jurisdicción siempre que se sujete a las mismas normas que el banco y que la aplicación de los requisitos se supervise a escala del grupo.
- La oficina central del grupo debe tener acceso a la información relevante para hacer cumplir las políticas y procedimientos PBC/FT del grupo.
- Las políticas de aceptación de clientes, CDD y mantenimiento de registros deben implementarse en forma coherente en toda la organización, con los ajustes necesarios según las diferencias de riesgo por líneas de negocio o áreas geográficas.
- Los métodos de recopilación de información, si bien pueden ser distintos para adecuarse a los requisitos locales o a factores de riesgo, deben ser coherentes con las normas para todo el grupo.
- Cada oficina deberá establecer y mantener políticas y procedimientos acordes con los riesgos en la jurisdicción y en el banco.
- El banco deberá vigilar a escala consolidada las relaciones, saldos y actividades de importancia con clientes.
- Al aplicar la centralización de sistemas de procesamiento y bases de datos global, el banco debe documentar e integrar adecuadamente las funciones locales y centralizadas de seguimiento de transacciones/cuentas, para vigilar patrones de posibles actividades sospechosas en todo el grupo y no solo a escala local o centralizada.
- Corresponde al responsable de PBC/FT del grupo crear, coordinar y evaluar a escala del grupo la aplicación de una única estrategia PBC/FT; dar seguimiento continuo al cumplimiento de todos los requisitos PBC/FT, tanto nacionales como internacionales; cerciorarse del cumplimiento, así como ordenar las medidas oportunas en todo el grupo.

**d)** Intercambio de información dentro del grupo:

- Las filiales y sucursales deben suministrar a la oficina central la información sobre clientes y actividades de alto riesgo, que sea relevante para las normas globales PBC/FT, así como responder a las solicitudes de información sobre cuentas.
- Las normas del banco para el grupo deben incluir una descripción del proceso a seguir en todos los establecimientos para identificar, vigilar e investigar posibles circunstancias anómalas y notificar operaciones sospechosas, incluyendo las obligaciones en materia de protección de datos y privacidad, así como los diferentes tipos de información que se pueden compartir y los requisitos de almacenamiento, recuperación, intercambio/distribución y eliminación de esa información.
- La función global de gestión del riesgo BC/FT del grupo debe evaluar los posibles riesgos 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; asimismo, deben contar con políticas y procedimientos para comprobar si otras sucursales o filiales mantienen cuentas de un mismo cliente.

- El banco debe contar con políticas y procedimientos globales tratándose de cuentas de alto riesgo o que hayan estado asociadas a actividades potencialmente sospechosas.
- El banco y sus sucursales y filiales deben cooperar ante solicitudes de información sobre clientes por parte de las autoridades.
- La función global de gestión del riesgo BC/FT del grupo es evaluar los posibles riesgos establecidos 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. Se debe 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).
- A requerimiento de los supervisores, el banco debe informar sobre su proceso global de gestión del riesgo de clientes, la evaluación y gestión de los riesgos BC/FT, las políticas y procedimientos PBC/FT a escala consolidada y sus sistemas de intercambio de información dentro del grupo.

**e)** Grupos financieros mixtos:

- Los grupos mixtos deben ser capaces de vigilar e intercambiar información sobre la identidad de los clientes y sobre sus transacciones y cuentas en el conjunto del grupo, así como estar atentos a los clientes que utilicen sus servicios en diferentes sectores.
- Se debe evaluar los posibles riesgos establecidos por las actividades de los sectores y, cuando proceda, evaluar los riesgos en todo el grupo planteados por un determinado cliente o categoría de clientes.
- Las diferencias en la naturaleza de las actividades y en los patrones de relaciones entre bancos y clientes en cada sector podrán requerir variaciones de los requisitos PBC/FT; por lo que el grupo debe estar atento a esas diferencias cuando se realicen ventas cruzadas de productos y servicios a los clientes desde distintas unidades de negocio.

## **4.** El papel de los supervisores

- El Comité de Basilea prevé que los supervisores apliquen los principios básicos para una supervisión bancaria eficaz a la gestión del riesgo BC/FT de los bancos, en consistencia con la supervisión general de los bancos.
- Los supervisores deben definir las expectativas que guíen las políticas y procedimientos PBC/FT de los bancos; en ese sentido, el Comité de Basilea aporta directrices para la mejora de las prácticas supervisoras.
- Los supervisores deben adoptar un enfoque en función del riesgo, lo que exige:

  **(i)** Conocer los riesgos en la jurisdicción y de su potencial impacto en las entidades supervisadas.

  **(ii)** Evaluar la suficiencia de la evaluación de riesgos del banco.

  **(iii)** Evaluar los riesgos en la entidad supervisada para conocer su naturaleza y el alcance en su base de clientes, productos y servicios, así como áreas geográficas en las que el banco y clientes realizan negocios.

  **(iv)** Evaluar la aplicación de los controles y la mitigación de riesgos.

  **(v)** Utilizar la información para asignar recursos e identificar capacidades requeridas.
- El perfil de riesgo del banco deberá utilizarse para determinar la frecuencia y calendario del ciclo supervisor.
- Los supervisores deben verificar si los bancos han hecho un uso adecuado de su discrecionalidad al aplicar medidas PBC/FT en el EBR; evaluar los controles internos; analizar las políticas y

procedimientos y la documentación sobre clientes, informes internos y un reporte de operaciones sospechosas; revisar la documentación relacionada con las transacciones y revisar el análisis realizado por el banco para detectar transacciones anómalas o sospechosas.

- Los supervisores deben garantizar que los bancos aplican una sólida gestión del riesgo BC/FT para proteger su propia seguridad y solvencia y la del sistema bancario, así como que aplican medidas CDD reforzadas a las relaciones comerciales y transacciones cuando así lo exija el GAFI, o en los casos en que las jurisdicciones cuyas normas PBC/FT sean consideradas inadecuadas.
- En caso de incumplimiento, los supervisores deben adoptar las medidas ante incumplimientos (tanto a la institución como a los funcionarios), aplicar medidas correctivas.
- Los supervisores deben considerar el proceso global de seguimiento y vigilancia por parte del banco del cumplimiento en sus sucursales y filiales, así como su capacidad para adaptarse a los requisitos y garantizar que cuando exista una discrepancia, se apliquen los más estrictos. En aquellos casos en que la sucursal o filial del grupo no pueda aplicar la más estricta de las normas, deben documentarse los motivos y se apliquen medidas paliativas para mitigar los riesgos por las discrepancias.
- En un contexto transfronterizo, los supervisores del país de origen no deben tener limitación (incluso de acceso a todo tipo de información) para las inspecciones para verificar que el banco cumple las políticas y procedimientos PBC/FT en todo el grupo.
- En el uso de la información, los supervisores deben garantizar la confidencialidad debida.
- Los supervisores del país de que se trate deben garantizar su cooperación y apoyo a los supervisores del país de origen.
- Los supervisores del país de origen deben garantizar la existencia de una política adecuada y asignación de recursos en función del riesgo, en consistencia con el alcance y la frecuencia de la auditoría de los procedimientos PBC/FT del grupo; asimismo, deben garantizar que los auditores tienen acceso a todos los informes durante el proceso de auditoría.
- No debe haber ningún tipo de restricción en las jurisdicciones para facilitar la transmisión de información, o para las visitas, ni en la capacidad para acceder a todos los registros del banco, incluidos nombres de clientes y saldos en sus cuentas. Si existieran obstáculos, y no hubiese arreglo satisfactorio, los supervisores de origen deberán informar al supervisor del país receptor que el banco podría quedar sujeto a actuaciones adicionales, incluida la exigencia al grupo matriz del cierre de sus operaciones en la jurisdicción que presenta obstáculos.
- Debe permitirse también la transmisión de información sobre los clientes locales a la oficina central (como se ha indicado, guardando confidencialidad, privacidad y privilegios).

El Comité de Basilea indica que no existen razones que justifiquen una legislación que impida la transmisión de información de clientes desde una sucursal o filial bancaria de un país a la oficina central o banco matriz en la jurisdicción de origen.