

Capítulo VI

Exigencias de las instituciones financieras

A. Identificación del cliente y debida diligencia

1. Alcance de la identificación del cliente y la debida diligencia
2. ¿Quién es un cliente?
3. Procedimientos de aceptación e identificación del cliente
4. Mantenimiento y vigilancia de cuentas de alto riesgo
5. Casos que necesitan mayor debida diligencia
6. Ampliación de la debida diligencia para incluir a los proveedores y otros
7. Medidas del sector de seguros
8. Medidas del sector de valores

B. Reportes sobre transacciones sospechosas

1. Transacciones sospechosas: Lo que esto supone
2. Disposiciones "para llegar a puerto seguro" con respecto a los reportes
3. Reportes del sector de seguros
4. Reportes del sector de valores

C. Exigencias sobre el mantenimiento de registros

1. Exigencias de las instituciones financieras sobre el mantenimiento de registros
2. Exigencias del sector de seguros sobre el mantenimiento de registros
3. Exigencias del sector de valores sobre el mantenimiento de registros

D. Reportes sobre transacciones de dinero en efectivo

1. Transacciones múltiples de dinero en efectivo
2. Movimientos transnacionales
3. Técnicas modernas de administración del dinero

E. Leyes de privacidad versus reportes y divulgación de información

F. Controles internos, cumplimiento, y auditoría

Es evidente que los blanqueadores de dinero y aquéllos que financian el terrorismo deben tener acceso a las instituciones financieras. Estas últimas proporcionan los medios para que dichos individuos transfieran fondos entre otras instituciones financieras, tanto a nivel nacional como internacional. Estas instituciones también facilitan los medios para convertir el dinero y pagar por los bienes utilizados en el proceso de lavado de dinero y financiamiento del terrorismo. Los tipos de instituciones financieras y sus capacidades varían mucho entre los diferentes países. Por lo tanto, es necesario que un país tome decisiones de principio sobre las exigencias de las instituciones financieras, basándose en las características únicas de dichas instituciones, los mercados financieros y la economía en general de ese país. Sin embargo, todas estas decisiones deberían tomarse con relación a las estándares internacionales.

A. Identificación del cliente y debida diligencia

Según las estándares internacionales establecidas por el Comité de Basilea de Supervisión Bancaria (Comité de Basilea)¹⁸⁰ y el Grupo de Acción Financiera sobre el Lavado de Dinero (GAFI),¹⁸¹ los países deben asegurarse de que sus instituciones financieras tengan métodos adecuados de identificación del cliente y debida diligencia. Dichos métodos se aplican tanto a los clientes particulares como empresariales de una institución financiera. Estos reglamentos o procedimientos aseguran que las instituciones financieras mantengan un conocimiento adecuado sobre sus clientes y las actividades financieras de estos últimos. Las exigencias de identificación del cliente también son conocidas como “Conozca a su cliente” (CSC),¹⁸² un término utilizado por el Comité de Basilea.¹⁸³

Las estándares CSC no sólo ayudan a las instituciones financieras a detectar, impedir, y prevenir el lavado de dinero y el financiamiento del terrorismo, también conceden beneficios concretos a la institución financiera, sus clientes respetuosos de la ley, y el sistema financiero en su totalidad. En particular, las estándares CSC

- promueven los buenos negocios, el buen gobierno, y la gestión de riesgos entre las instituciones financieras;
- ayudan a mantener la integridad del sistema financiero y permiten realizar esfuerzos de desarrollo en los mercados emergentes;
- reducen la frecuencia del fraude y otros delitos financieros; y

180. Comité de Basilea, Principios Basicos de Supervision Bancaria y Debida Diligencia para los Bancos, principio 15, en <http://www.bis.org/publ/bcbs30.pdf>

181. *Las Cuarenta Recomendaciones*, http://www1.oecd.org/fatf/40Recs_en.html y *Recomendaciones Especiales*, http://www1.oecd.org/fatf/SrecTF_en.htm *Las Cuarenta Recomendaciones* están incluidas en el Anexo IV y las *Recomendaciones Especiales* en el Anexo V de esta Guía de referencia.

182. Comité de Basilea, Principios Basicos de Supervision Bancaria, principio 15, el cual establece que: «Los supervisores bancarios deben asegurarse que los Bancos tengan políticas, prácticas y procedimientos adecuados, incluidas las reglas de « conozca a su cliente », que promueven estándares éticas y profesionales de alto nivel en el sector financiero y evitan que el Banco sea utilizado, voluntaria o involuntariamente por delincuentes ».

183. La Debida Diligencia del Cliente para los Bancos, del Comité de Basilea, establece que: « Los supervisores a nivel mundial están cada vez más reconociendo la importancia de asegurarse que sus Bancos tengan controles y procedimientos adecuados, de manera que sepan con que clientes están tratando. Una Debida Diligencia adecuada con respecto a clientes existentes y nuevos es un elemento fundamental de estos controles ». <http://www.bis.org/publ/bcbs85.pdf>

Exigencias de las instituciones financieras

- protegen la reputación de la organización financiera contra los efectos perjudiciales de la relación con delincuentes.¹⁸⁴

1. Alcance de la identificación del cliente y la debida diligencia

Los métodos de identificación del cliente y debida diligencia utilizados por una institución financiera también deben aplicarse a sus sucursales y filiales de participación mayoritaria, tanto a nivel nacional como internacional, siempre y cuando no entren en conflicto con el derecho interno.¹⁸⁵ Cuando el derecho interno prohíbe su aplicación, se les debe notificar a las autoridades pertinentes en el país de origen que estos métodos no pueden ser utilizados por las instituciones de su país beneficiario. Los supervisores de los países beneficiarios deberían realizar esfuerzos para cambiar tales leyes y reglamentos en la jurisdicción local.¹⁸⁶ Cuando no hay restricciones legales en el país beneficiario y existen dos niveles diferentes de estándares reglamentarios entre el país de origen y el país beneficiario, debe aplicarse la estándares más importante o más amplia de las dos.¹⁸⁷

2. ¿Quién es un cliente?

El Comité de Basilea define a un cliente como:

- una persona o entidad que mantiene una cuenta en una institución financiera
- o en cuyo nombre se mantiene una cuenta (es decir, los beneficiarios);
- beneficiarios de transacciones realizadas por intermediarios profesionales (por ejemplo: agentes, contadores, abogados); y
- una persona o entidad vinculada con una transacción financiera que puede representar un riesgo importante para el banco.¹⁸⁸

184. Proviene de la Debida Diligencia del Cliente para los Bancos, del Comité de Basilea (disposición 9)

185. *Las Cuarenta Recomendaciones*, Rec. 20.

186. *Id.*

187. Debida Diligencia de los Clientes para los Bancos, del Comité de Basilea (disposición 66)

188. *Id.* (disposición 21)

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

Un aspecto crucial de la identificación del cliente es establecer si el cliente está actuando en su propio nombre o si hay un beneficiario de la cuenta que puede no estar identificado en los documentos mantenidos por la institución financiera. Si existe una razón para sospechar que el cliente está actuando en nombre de otra persona o entidad, deberían establecerse medidas adecuadas de debida diligencia.

La propiedad usufructuaria también es complicada en el caso de entidades jurídicas o sociedades anónimas donde existe propiedad escalonada. La propiedad escalonada comprende una sociedad anónima que posee o controla una o más empresas. En algunos casos, pueden haber varias sociedades anónimas, cada una de las cuales puede ser a su vez propiedad de otra sociedad anónima y, finalmente, ser propiedad o estar bajo el control de una sociedad matriz. Cuando las sociedades anónimas o entidades jurídicas están en juego, se deberían emplear medidas adecuadas de debida diligencia para determinar la identidad de la verdadera sociedad matriz o entidad de control.

3. Métodos de aceptación e identificación del cliente

Las instituciones financieras deberían desarrollar e imponer métodos claros de aceptación e identificación del cliente para los clientes mismos y para aquéllos que actúan en nombre de estos últimos.¹⁸⁹ Estos métodos deberían incluir la elaboración de perfiles de clientes de alto riesgo. Dichos perfiles podrían comprender indicadores de riesgo estándar, tales como los antecedentes personales, el país de origen, la ocupación de un cargo público o de alto perfil, las cuentas conexas y el tipo y la naturaleza de la actividad comercial.¹⁹⁰

Al diseñar políticas de aceptación de clientes, las instituciones financieras deben actuar con mucho cuidado para encontrar el equilibrio adecuado entre la prevención del riesgo con respecto a las actividades delictivas y la buena disposición para aceptar nuevos clientes. Por regla general, la rigidez de los estándares de aceptación debería estar acorde con el perfil de riesgo de un cliente potencial. Se recomienda firmemente que sólo la administración supe-

189. *Id.* (disposición 20)

190. *Id.*

rior tome decisiones sobre los clientes cuyos perfiles indican que representan un alto riesgo de estar implicado en actividades de lavado de dinero.¹⁹¹

Las instituciones financieras deberían diseñar sus políticas de aceptación del cliente de manera tal que no se excluyan a los desfavorecidos sociales. Estas políticas de aceptación del cliente no deberían de ninguna forma restringir el acceso del público en general a los servicios financieros.¹⁹² Esto es especialmente importante para los países que avanzan hacia una utilización más amplia de los instrumentos financieros, incluidos el uso de cheques, tarjetas de crédito o débito, mecanismos de pago electrónicos y otros, y el alejamiento de una economía basada en el dinero en efectivo.

Se deberían abrir las cuentas sólo luego de haber verificado de forma satisfactoria la identidad del nuevo cliente.¹⁹³ No se le debería permitir a ningún cliente abrir o mantener un cuenta utilizando un nombre anónimo o falso. Esta prohibición también se aplica a una cuenta numerada, si se tiene acceso a dicha cuenta mediante el uso de un número o código, una vez que la cuenta no requiere los procedimientos de identificación del cliente al utilizar la documentación oficial.¹⁹⁴ Las cuentas numeradas sólo son permitidas cuando se utilizan los mismos métodos de identificación del cliente y documentos justificativos (con mantenimiento de registros). Según estas estándares, las instituciones financieras deben comprobar y verificar el documento de identidad oficial de sus clientes. Los mejores documentos para verificar la identidad de los clientes potenciales o existentes son aquéllos que son más difíciles de reproducir.¹⁹⁵ En este sentido, los países deberían exigir el uso de documentos “oficiales” emitidos por las autoridades correspondientes, tales como un pasaporte, una licencia de conducir, un documento de identificación personal o un formulario de declaración de la renta.

En los casos en que un agente representa a un beneficiario (por ejemplo, a través de fideicomisos, apoderados, cuentas fiduciarias, sociedades anónimas, y otros intermediarios), las instituciones financieras necesitan tomar medidas razonables para verificar la identidad y naturaleza de las personas u

191. *Id.*

192. *Id.*

193. *Id.* (disposición 22)

194. *Las Cuarenta Recomendaciones*, Rec. 10, y la Debida Diligencia para los Bancos del Comité de Basilea (disposición 30)

195. Ver *Debida Diligencia para los Bancos del Comité de Basilea* (disposición 23)

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

organizaciones en cuyo nombre se está abriendo una cuenta o para quienes se está completando una transacción.¹⁹⁶ Las instituciones financieras deben verificar la legalidad de tales entidades reuniendo la siguiente información sobre los clientes potenciales:

- Nombre y forma jurídica de la organización del cliente;
- dirección;
- nombres de los directores;
- propietarios principales o beneficiarios;
- disposiciones que regulan el poder de obligar a la organización;
- agente(s) que actúan en nombre de la organización; y
- número de cuenta (si es pertinente).¹⁹⁷

En los casos de remesas de fondos, tales como las remesas de fondos, las instituciones financieras deberían incluir información exacta y significativa sobre la persona que origina la transferencia (nombre, dirección, y número de cuenta) y transmitir esta información a través de la cadena de pago junto con la transferencia de fondos.¹⁹⁸

Se debe confirmar la identidad de un cliente a través de métodos de debida diligencia en los casos en que se trata de un cliente eventual que ha sobrepasado el umbral determinado (ver la parte E de este capítulo), o cuando haya alguna duda sobre la verdadera identidad de ese cliente.¹⁹⁹ Lo mismo sucedería en el caso del cliente de una empresa.

La identificación del cliente es un proceso en curso que, por regla general, les exige a las instituciones financieras que mantengan registros actualizados de toda la información pertinente sobre los clientes. Los registros deben actualizarse, por ejemplo en el caso de transacciones importantes, cambios en las estándares con respecto a la documentación del cliente, cambios sustanciales en la operación de una cuenta, y si se comprueba que los registros existentes son insuficientes.²⁰⁰ Se exhorta a los

196. *Las Cuarenta Recomendaciones*, Rec.11

197. *Id.*, Rec. 10

198. Ver GAFI, Rec. Esp. VII

199. Ver Debita Diligencia para los Bancos del Comité de Basilea, Disposición 53, y GAFI, *Las Cuarenta Recomendaciones*, Rec.14

200. Debita Diligencia para los Bancos del Comité de Basilea, Disposición 24

Exigencias de las instituciones financieras

supervisores nacionales a que ayuden a las instituciones financieras a desarrollar sus propios métodos de aceptación e identificación del cliente.

4. Mantenimiento y supervisión de las cuentas de alto riesgo

Las instituciones financieras deberían evitar el mantenimiento de cuentas a través de instituciones financieras corresponsales ubicadas en jurisdicciones de alto riesgo que tienen una protección legal poco estricta contra el lavado de dinero y el financiamiento del terrorismo. El GAFI clasifica a ciertas jurisdicciones como “países y territorios no cooperantes” (PTNC).²⁰¹ Estas jurisdicciones representan para las instituciones financieras problemas específicos de alto riesgo.

Asimismo, deben evitarse las transacciones con ciertos tipos de “bancos ficticios”. En general, los bancos ficticios que hay que evitar son aquéllos que están dentro de una jurisdicción que no tiene ninguna presencia física en un grupo financiero regulado o ninguna afiliación con el mismo.²⁰²

Se exhorta a las instituciones financieras a que utilicen programas de software para ayudarlas en su gestión de la información.²⁰³ Dichos programas son útiles para recopilar, analizar, detectar, y comunicar datos que identifican a los clientes y las actividades de alto riesgo. Deberían detectar actividades extrañas o sospechosas.²⁰⁴ Estos programas cumplen una función clave en el descubrimiento de actividades potencialmente sospechosas en medio del gran número de transacciones legítimas que se realizan diariamente.

Además, las instituciones financieras deberían mejorar sus capacidades de vigilancia para adaptarse a las diversas cuentas internacionales, que algunas veces son medios conocidos para el abuso indirecto del sistema a nivel transnacional. Las instituciones financieras deberían dar cuenta de este potencial de abuso sumando y vigilando los saldos y actividades importantes en las cuentas “sobre una base mundial consolidada”.²⁰⁵

201. Para obtener una lista completa de los países y territorios « no cooperantes » del GAFI, ver http://www1.oecd.org/fatf/NCCT_en.htm

202. Ver Debida Diligencia para los Bancos del Comité de Basilea, Disposición 51

203. *Id.* (disposiciones 53-54)

204. *Id.*

205. *Id.*, (disposición16)

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

5. Casos que necesitan mayor debida diligencia

Por regla general, la debida diligencia debería estar acorde con el nivel de riesgo percibido de una cuenta.²⁰⁶ Los clientes y las cuentas de alto riesgo deberían ser examinados más a fondo. Se debería emplear una mayor debida diligencia en los casos mencionados a continuación:²⁰⁷

- operaciones que de alguna forma se sospecha que están relacionadas con el terrorismo u organizaciones que respaldan o ayudan al terrorismo;
- remesas de fondos que no proporcionan la información completa sobre el autor de la transferencia (nombre, dirección, y número de cuenta);
- nueva tecnología que permita el anonimato de los clientes o las operaciones;
- ejemplos de operaciones complejas, extensas, o extrañas sin ningún propósito económico o legal aparente;
- actividad de cuentas en jurisdicciones conocidas por tener una legislación poco estricta sobre el lavado de dinero y el financiamiento del terrorismo;
- ciudadanos extranjeros que mantienen cuentas en otro Estado soberano sin haber dado una razón clara;
- cuando una institución financiera cree que otra institución financiera le ha negado sus servicios a un cliente potencial;
- envíos comerciales a través de los servicios de la banca corresponsal (es decir, remesas de fondos electrónicas y uso de cuentas corresponsales por terceros);
- operaciones bancarias y clientes de alto riesgo, especialmente los individuos expuestos a la política y sus afiliados; y
- clientes que no se presentan ellos mismos en las entrevistas u operaciones cara a cara (por ejemplo, operaciones bancarias electrónicas via Internet o presentación de terceros).

206. *Id.*, (disposición 6)

207. *Recomendaciones Especiales*, Recs. Esp. IV y VII; *Las Cuarenta Recomendaciones*, Recs. 9, 13, 14 y 21; y *Debida Diligencia para los Bancos del Comité de Basilea* (disposiciones 23, 29, 35-36, 44, 46 y 52). Esta lista es un ejemplo y no muestra en detalle todas las circunstancias que requieren un aumento de la debida diligencia.

Exigencias de las instituciones financieras

Se deberían tomar medidas para atenuar el nivel más elevado de riesgo planteado por dichos casos. Esto significa obtener más información sobre el cliente, la cuenta, la institución, la operación, o la jurisdicción implicada. Es un estándares, por ejemplo, que las instituciones financieras exijan mayor información sobre los clientes que no se presentan en entrevistas cara a cara. Estas operaciones poco convencionales pueden ser aclaradas una vez que se proporcione la información adicional.²⁰⁸ El cliente puede brindar dicha información en forma de documentos certificados, otros formularios de identificación, un contacto independiente y verificable con el cliente, envíos de terceras partes o instituciones que cumplen con las estándares CSC, o el primer pago de un cliente bajo su nombre en otro banco que acata estándares semejantes.²⁰⁹

Si el cliente no puede brindar información suficiente para abordar las preocupaciones de una institución financiera sobre la debida diligencia, o si la sospecha persiste, las instituciones deberían retener el poder de no aceptar al cliente. En este sentido, se debe tener cuidado al establecer las razones específicas para negar los servicios, de manera que las instituciones no estén sujetas a una posible responsabilidad legal. Sin embargo, la autoridad para negar los servicios por falta de información adecuada sobre la identificación del cliente debería ser una opción disponible para las instituciones.

6. Ampliación de la debida diligencia para incluir a los abastecedores y otros.

La estructura de la cadena de abastecimiento de muchas empresas se ha vuelto cada vez más compleja e interrelacionada con el desarrollo del comercio mundial. Por lo tanto, muchas instituciones financieras se han dado cuenta que es necesario ejercer una mayor diligencia con respecto a los proveedores, abastecedores y agentes de organizaciones, así como en relación a los empleados y bancos corresponsales de las instituciones financieras. El supervisor nacional de cada país debería considerar poner en práctica políticas que incluyan estas tendencias de la debida diligencia.

208. Debida Diligencia para los Bancos del Comité de Basilea (disposición 48)

209. *Id.*

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

7. Medidas del sector de seguros

La Asociación Internacional de Supervisores de Seguros (AISS) mantiene sus propias estándares de identificación del cliente y debida diligencia. La industria de seguros debe observar estas estándares, además de otras estándares pertinentes que se presentan a continuación. Las estándares de la AISS recomiendan que las compañías de seguros:

- establezcan de una manera que “consideren razonable” que cada parte pertinente para la aplicación de los seguros existe realmente. En el caso de muchos temas (por ejemplo: pólizas de seguro de vida colectivo y planes de pensiones), puede ser suficiente usar un grupo limitado, tales como los principales accionistas o los directores más importantes;
- verifiquen todos los mandantes subyacentes, así como su relación con los asegurados. Los mandantes, y no los asegurados, deberían ser interrogados con respecto a la naturaleza de la relación;
- prohíban cuentas anónimas y ficticias;
- verifiquen las reclamaciones, comisiones, y cualquier otra suma de dinero entregada a los no asegurados (por ejemplo: asociaciones, compañías);
- aumenten la debida diligencia cuando los flujos financieros o los esquemas de las operaciones de los asegurados cambien de manera significativa, inesperada, o inexplicada;
- aumenten la debida diligencia con respecto a la compra y venta de pólizas dotalas usadas y la utilización de pólizas relacionadas a una sola unidad; y
- vigilen el reaseguro o la retrocesión con regularidad, para asegurar los pagos a las empresas reaseguradoras de *buena fe*, a tarifas justificadas por el nivel de riesgo.²¹⁰

210. Ver AISS, notas de orientación sobre el antilavado de dinero, <http://www.iaisweb.org/framesets/pas.html>

8. Medidas del sector de valores

La Organización Internacional de Comisiones de Valores (OICV) no ha establecido exigencias particulares sobre la identificación del cliente o la debida diligencia para las sociedades de valores, los corredores, o las entidades de inversión colectiva. Aunque la OICV no ha instaurado tales exigencias específicas, los requisitos de identificación del cliente de *Las Cuarenta Recomendaciones* (tal como se describe con mayor detalle en la Metodología) se aplican al sector de valores.

B. Reportes sobre transacciones sospechosas

“Se les debe exigir a los empleados que denuncien los comportamientos sospechosos o extraños a un superior o la seguridad interna.”²¹¹ En otras palabras, las instituciones financieras tienen la obligación, según este mandato internacional, de reportar las transacciones sospechosas. “Además, de les debe exigir a los bancos que denuncien las actividades sospechosas y los casos importantes de fraude a los supervisores, [y] los supervisores deben asegurarse que se ha alertado a las autoridades competentes.”²¹² Las instituciones que reporten actividades sospechosas no deberían en ningún caso avisar a sus clientes que su comportamiento ha sido reportado como sospechoso a las autoridades.²¹³ Desde ese momento en adelante, es decir, a partir de la reporte, las instituciones financieras deben acatar completamente las instrucciones de las autoridades gubernamentales.²¹⁴

1. Transacciones sospechosas: Lo que esto supone

Las transacciones sospechosas contienen ciertas características amplias generales, entre las cuales se incluyen, obviamente, las transacciones que

211. *Id.*

212. Principios Básicos del Comité de Basilea, principio 15, descripción 31

213. *Las Cuarenta Recomendaciones*, Rec. 17

214. *Id.*, Rec. 18

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

parten de esquemas estándares de actividad de una cuenta. Cualquier transacción compleja o excepcionalmente importante, además de cualquier esquema de transacción extraño, sin la presencia de un propósito económico, comercial o legal aparente, es sospechosa y, por lo tanto, merece una mayor investigación por parte de la institución financiera y, si es necesario, por parte de las autoridades competentes.²¹⁵ Para ayudar a las instituciones financieras a detectar las transacciones sospechosas, dichas instituciones deberían establecer límites sensibles a los riesgos para vigilar categorías o tipos particulares de cuentas. Los casos específicos de actividades sospechosas (por ejemplo, un alto movimiento de cuentas incompatible con la cantidad de dinero que queda como saldo) son útiles para las instituciones financieras individuales y los supervisores deberían de alguna manera darles estos ejemplos.²¹⁶

Las instituciones financieras y sus empleados deberían estar siempre alertas con respecto a las transacciones sospechosas. Aunque los ejemplos siguientes indican la presencia de transacciones sospechosas, la lista no es exhaustiva:

- Indicios generales:
 - Fondos retirados inmediatamente después de haber sido abonados en una cuenta.
 - Una cuenta sin movimiento que de pronto se vuelve activa sin ninguna razón admisible.
 - El alto valor del capital de un cliente no es compatible con la información sobre el cliente mismo ni sobre sus negocios.
 - Un cliente proporciona información falsa o adulterada, o se niega a transmitir al banco la información requerida.
 - La forma en que se hace una transacción implica un propósito ilegal, es ilógica desde el punto de vista económico, o no identificable.

215. *Id.*, Rec. 14

216. *Id.*, Rec. 28. Ver también Debida Diligencia para los Bancos del Comité de Basilea (disposición 53).

Exigencias de las instituciones financieras

- Indicios con respecto a las transacciones de dinero en efectivo
 - Depósitos frecuentes de dinero en efectivo incompatibles con la información sobre el cliente o sus negocios.
 - Depósitos de dinero en efectivo inmediatamente seguidos de la emisión de cheques o remesas hacia cuentas abiertas en otros bancos ubicados en el mismo país o en el exterior.
 - Retiros frecuentes de dinero en efectivo sin ningún vínculo evidente con los negocios del cliente.
 - Intercambio frecuente de billetes de gran valor por billetes de valor más pequeño, o por otra moneda.
 - Cobros de cheques, incluidos los cheques de viajero, por grandes cantidades.
 - Transacciones frecuentes de dinero en efectivo por montos justo por debajo del nivel donde se exige la identificación o reporte por parte de la institución financiera.
- Indicios con respecto a las transacciones de las cuentas a plazo
 - El cierre de una cuenta seguido de la apertura de cuentas nuevas bajo el mismo nombre o por miembros de la familia del cliente.
 - Compra de acciones mobiliarias con fondos que han sido transferidos del exterior o inmediatamente después de haber depositado dinero en efectivo en la cuenta.
 - Estructuras ilógicas (varias cuentas, remesas frecuentes entre cuentas, etc.).
 - Concesión de garantías (empeños, fianzas) sin ninguna razón aparente.
 - Remesas en favor de otros bancos sin ninguna indicación sobre el beneficiario.
 - Rembolso inesperado, sin ninguna razón convincente, de un préstamo en mora.
 - Depósito de cheques de montos importantes incompatibles con la información sobre el cliente o sus negocios.

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

2. Disposiciones “para llegar a puerto seguro” con respecto a los reportes

Las leyes “para llegar a puerto seguro” ayudan a incitar a las instituciones financieras a que denuncien todas las transacciones sospechosas. Dichas leyes protegen a las instituciones financieras y los empleados contra la responsabilidad penal y civil cuando reporten de buena fe transacciones sospechosas a las autoridades competentes. Estas disposiciones legales deberían dar protección a las instituciones financieras, y a sus empleados o representantes, contra juicios por cualquier supuesta violación de las leyes de confidencialidad o secreto, siempre y cuando la reporte sobre la transacción sospechosa haya sido hecha de buena fe (es decir, no fue hecha de forma superficial ni maliciosa).²¹⁷

3. Reportes del sector de seguros

La AISS ha establecido su propio conjunto de estándares con respecto a la reporte de transacciones sospechosas. La industria de seguros debe acatar estas estándares, además de las estándares pertinentes que se presentan a continuación. Las compañías de seguro deberían reportar las actividades sospechosas a la unidad de inteligencia financiera o a otra autoridad nacional centralizada. Los siguientes son casos de transacciones sospechosas, relacionados con un sector específico, que merecen una investigación adicional:

- Cancelación temprana de una póliza de seguros, de forma inusitada o desfavorable;
- Utilización poco común de un intermediario durante algunas transacciones o actividades financieras habituales (por ejemplo: el pago de reclamaciones o una comisión alta a un intermediario inhabitual);
- Método de pago a estándares; y
- Transacciones que comprometen a jurisdicciones con instrumentos reguladores poco estrictos con respecto al lavado de dinero y/o el financiamiento del terrorismo.²¹⁸

217. *Las Cuarenta Recomendaciones*, Rec. 16

218. Ver Notas de Orientación sobre el Antilavado de dinero de la AISS

Exigencias de las instituciones financieras

4. Reportes del sector de valores

La OICV no ha establecido exigencias específicas con respecto a los reportes de actividades sospechosas para las sociedades de valores, los corredores, o las entidades de inversión colectiva. Aunque la OICV no ha implantado requisitos específicos o adicionales en esta área, las exigencias sobre reportes de actividades sospechosas que aparecen en *Las Cuarenta Recomendaciones* se aplican al sector de valores.

C. Exigencias sobre el mantenimiento de registros

1. Exigencias de las instituciones financieras sobre el mantenimiento de registros

Las instituciones financieras deberían mantener los registros sobre la identidad del cliente y las transacciones por un plazo mínimo de cinco años, luego del cierre de una cuenta.²¹⁹ Se les podría exigir a las instituciones que mantengan registros por más de cinco años, si así lo requieren los reguladores. El contenido de los registros debería ponerse inmediatamente a disposición de las autoridades cuando éstas lo soliciten y, más adelante, ser suficiente para permitir que se entablen acciones judiciales contra las actividades delictivas.²²⁰

El mantenimiento de registros es importante tanto para prevenir como para detectar alguna intención de lavado de dinero o financiamiento del terrorismo. Si un cliente potencial sabe que se mantienen registros, es poco probable que dicho cliente trate de usar la institución para estos fines ilegales. Mantener registros también es útil para detectar a las personas implicadas y además proporciona pistas a nivel financiero para ayudar a las autoridades competentes a perseguir a estas personas.

Cuando se registra la transacción de un cliente, se debería incluir la siguiente información:

219. *Las Cuarenta Recomendaciones*, Rec. 12.

220. Id.

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

- nombre del cliente y/o del beneficiario;
- dirección;
- fecha y naturaleza de la transacción;
- tipo y cantidad de dinero comprendidos en la transacción;
- tipo de cuenta y la identificación del número de cuenta; y
- otra información pertinente que la institución financiera registra generalmente.²²¹

2. Exigencias del sector de seguros sobre el mantenimiento de registros

La AISS mantiene su propio conjunto de exigencias sobre el mantenimiento de registros. Las compañías de seguro deben acatar estas exigencias, además de las estándares correspondientes que se encuentran en *Las Cuarenta Recomendaciones*. La compañía de seguros también debe obtener la siguiente información (si es pertinente) al registrar la transacción del cliente:

- Locación finalizada
- evaluación financiera sobre el cliente;
- análisis de las necesidades del cliente;
- detalles sobre los métodos de pago;
- descripción de los beneficios;
- copia de la documentación utilizada para verificar la identidad del cliente;
- registros de post-venta relacionados con el contrato hasta su plazo de vencimiento; y
- detalles sobre el proceso de vencimiento y la liquidación de reclamaciones (incluida la “documentación sobre el pago”).²²²

Los supervisores de las instituciones financieras deben verificar que todos los representantes de las compañías de seguros sean titulares de una licencia, según la ley de seguros y jurisdicción correspondientes²²³ Los

²²¹. *Id.*

²²². Ver Notas de Orientación sobre el Antilavado de Dinero de la AISS

²²³. *Id.*

Exigencias de las instituciones financieras

representantes pueden guardar documentos en nombre de una compañía de seguros, pero la totalidad de los registros permanece en la compañía de seguros en su calidad de proveedora de productos.²²⁴ En tales casos, se necesita hacer una división clara de responsabilidades entre la compañía de seguros y sus representantes.²²⁵

3. Exigencias del sector de valores sobre el mantenimiento de registros

El OICV ha establecido su propio conjunto de exigencias sobre el mantenimiento de registros, que las sociedades de valores deben respetar, además de acatar las estándares generales pertinentes que se enumeran más abajo. El OICV exige que la autoridad nacional centralizada sobre el delito financiero u otra autoridad competente se asegure de que los intermediarios mantengan los registros necesarios para demostrar que observan las estándares establecidas.²²⁶ Estos registros deben ser legibles, comprensibles y detallados, y deben incluir todas las operaciones que comprendan los bienes y las transacciones de inversión colectiva.²²⁷

D. Reportes sobre transacciones de dinero en efectivo

Los países deberían considerar los beneficios que podrían obtener al exigir que se denuncien todas las transacciones de dinero en efectivo que sobrepasen un valor umbral determinado.²²⁸ Es obligatorio, sin embargo, que un país tenga ese tipo de requisito. Las reportes sobre transacciones de dinero en efectivo tienen consecuencias significativas con respecto a los recursos y la privacidad que los países necesitan tener en cuenta al considerar el asunto. Cada país o jurisdicción establece su propio umbral de reportes,

224. *Id.*

225. *Id.*

226. Ver OICV, *Principles for the Supervision of Operators of Collective Investment Schemes* (CIS, Septiembre 1997), disponible en http://www.iosco.org/docs-public/1997_principles_for_the_supervision.html

227. *Id.*

228. *Las Cuarenta Recomendaciones*, Rec. 23

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

basándose en su propia situación. Por ejemplo, Estados Unidos exige que las instituciones financieras registren y denuncien a las autoridades competentes todas las transacciones que comprendan dinero o instrumentos al portador superiores a \$10.000.²²⁹ Dichos umbrales pueden ser establecidos por ley, o mediante reglamentación bajo la autoridad del organismo de supervisión correspondiente del buen gobierno. Según la situación de un país, dichos requisitos también pueden aplicarse a ciertos negocios, tales como los casinos, los anticuarios, o los concesionarios de automóviles, o cuando se pagan compras de un valor importante con dinero en efectivo.

Las autoridades competentes deben tener mucho cuidado al determinar el nivel umbral de un país. Éste debe ser suficientemente alto como para detectar transacciones insignificantes pero también tan bajo como para detectar transacciones potencialmente relacionadas con el delito financiero. Además, los países podrían añadir excepciones a las exigencias sobre las reportes en el caso de transacciones donde las reportes son onerosas para el sistema y no sirven mucho para asegurar el cumplimiento de la ley. Asimismo, algunas entidades presentan un bajo riesgo de estar implicadas en el lavado de dinero y, por lo tanto, pueden reunir las condiciones para ser incluidas dentro de estas excepciones. Entre estas entidades, se incluyen los buen gobiernos, ciertas instituciones financieras o empresas que lógicamente se supone están libres de la corrupción, y clientes que realizan transacciones frecuentes y de grandes sumas de dinero, debido a la naturaleza de sus negocios. Dichas excepciones deberían ser revisadas regularmente para determinar si todavía son adecuadas. Esto debe hacerse como regla general y en el caso de algunas entidades, bajo circunstancias específicas.

1. Transacciones múltiples de dinero en efectivo

Las exigencias con respecto a las reportes sobre transacciones de dinero en efectivo también se aplican a las transacciones múltiples realizadas en un solo día, una práctica llamada “smurfing.” Si el monto consolidado de la transacción sobrepasa el nivel umbral de reportes establecido, las

229. Ver, por ejemplo Ley del Secreto Bancario de Los Estados Unidos (1970).

instituciones financieras deben reportar toda la serie de transacciones.²³⁰ Esta protección contra el « smurfing » (por el cual muchas transacciones individuales que comprenden múltiples cuentas en una institución financiera logran llevarse a cabo justo por debajo del nivel umbral de reportes de un país) es un elemento fundamental de los esfuerzos para prevenir el lavado de dinero y el financiamiento del terrorismo. Los delincuentes y los terroristas, obviamente, recurren a sus propias medidas para evitar ser detectados por los programas de software. Esta es la razón por la cual es absolutamente importante que las autoridades competentes empleen un análisis proactivo para detectar las actividades delictivas y de financiamiento del terrorismo.

Por supuesto, una transacción también puede ser reportada como una transacción sospechosa que no pasa la prueba de umbrales o transacciones múltiples. Por ejemplo, un solo depósito de \$9,900 puede considerarse sospechoso, bajo diversas circunstancias, cuando el nivel umbral de reportes de un país es de \$10,000, porque indica una estructura de transacciones realizada por un cliente para eludir las exigencias sobre las reportes.

2. Movimientos transnacionales

Los blanqueadores de dinero se dedican a hacer remesas transnacionales de dinero en efectivo, instrumentos negociables al portador y bienes de gran valor, como un sistema para blanquear fondos. Es importante que los países establezcan un mecanismo para detectar cuándo dichas remesas son utilizadas con fines de lavado de dinero o financiamiento del terrorismo.

Los ministros de finanzas y los funcionarios de aduana deberían pensar en establecer un límite mínimo con respecto a las reportes sobre los movimientos de dinero, otros instrumentos negociables, y bienes de gran valor (es decir, metales preciosos o gemas). El movimiento extraño o sospechoso de tales bienes, su punto de origen y su destino deberían reportarse al servicio de aduanas del país o a otras autoridades correspondientes.²³¹

230. Debida Diligencia del Cliente para los Bancos del Comité de Basilea (disposición 16)

231. *Las Cuarenta Recomendaciones*, Rec. 22

Guía de Referencia para la lucha contra el lavado de dinero y el financiamiento del terrorismo

3. Técnicas modernas de administración del dinero

Las capacidades de supervisión de las instituciones financieras y los funcionarios públicos se han beneficiado de un menor empleo de las remesas de dinero en efectivo y divisas y un mayor uso de los cheques, las tarjetas de crédito, los depósitos directos, y el registro de valores en el libro mayor. Estas transacciones dejan una huella escrita que es útil cuando se sospecha que ha habido una infracción y les permite a las autoridades competentes llevar a cabo las investigaciones. El éxito de las investigaciones depende de un mantenimiento de registros exacto y completo. Por este motivo, se recomienda mucho el uso de estos métodos modernos de administración del dinero y transferencia de pagos.²³²

E. Leyes de privacidad *versus* reportes y divulgación de información

Las reportes sobre algún tipo de información, por ejemplo, con respecto a las transacciones sospechosas y las transacciones de dinero en efectivo, o la divulgación de registros hechas por parte de una institución financiera a una autoridad competente, comprenden necesariamente datos que, por regla general, se tratan de manera confidencial, bajo las leyes de privacidad y secreto bancario de un país. Al exigir la reporte o divulgación de tales datos para fines ALD y LFT, un país debe incluir las excepciones correspondientes en sus leyes de privacidad o, de lo contrario, autorizar específicamente la reporte y divulgación con esos fines limitados. El GAFI aconseja que las leyes de privacidad de la institución financiera sean redactadas de manera que no impidan la aplicación de ninguna de sus recomendaciones.²³³

F. Controles internos, cumplimiento, y auditoría

Los países deberían exigirles a todas las instituciones financieras cubiertas por sus leyes ALD y LFT que establezcan y mantengan políticas y

232. *Id.*, Rec. 24

233. *Las Cuarenta Recomendaciones*, Rec. 2.

procedimientos internos para evitar que sus instituciones sean utilizadas para fines de lavado de dinero y financiamiento del terrorismo.²³⁴ Las políticas y procedimientos internos pueden variar de una institución a la otra y entre los diversos tipos de instituciones, sin embargo, todos deberían considerar el tamaño, el alcance, y la naturaleza de las operaciones de la institución.

Los procedimientos internos comprenden un adiestramiento permanente que mantenga a los empleados informados y al día sobre los avances con respecto al ALD y la LFT. La capacitación ofrecida a los empleados debe (1) describir la naturaleza y los procesos de lavado de dinero y financiamiento del terrorismo; (2) explicar las leyes ALD/LFT y las exigencias reglamentarias; y (3) explicar las políticas y los sistemas de una institución con respecto a las exigencias de los reportes sobre actividades sospechosas, haciendo hincapié en la identificación del cliente, la debida diligencia y las exigencias de los reportes.

Además, las instituciones financieras deberían investigar a los postulantes a un empleo para verificar si tienen la intención de usar sus instituciones para blanquear el dinero y/o financiar el terrorismo.²³⁵

La tercera política interna que se recomienda es que cada institución financiera nombre a un funcionario, a nivel administrativo, que garantice el cumplimiento de las leyes ALD/LFT.²³⁶ Dicho funcionario ayuda a asegurarse que se dedique la atención administrativa adecuada a los esfuerzos de cumplimiento de la institución.

La cuarta política interna que se aconseja establecer es una función de auditoría. Esta función debería ser independiente de la función administrativa de cumplimiento, con el fin de poner a prueba y asegurarse de la aceptabilidad de la función de cumplimiento, en términos generales.²³⁷

234. *Id.*

235. *Id.*, Recs. 19 y 26

236. *Id.*

237. *Id.*

