CAPÍTULO 1-14

PREVENCIÓN DEL LAVADO DE ACTIVO Y DEL FINANCIAMIENTO DEL TERRORISMO

I. CONSIDERACIONES GENERALES.

Las instituciones bancarias, por la naturaleza de sus funciones, pueden ser utilizadas para depositar y transferir fondos, cuyo objetivo sea intentar legitimar activos provenientes del narcotráfico o de otras operaciones ilícitas, o que sean utilizados, por ejemplo, para obtener materiales y/u otros elementos logísticos necesarios para el financiamiento del terrorismo.

Además, se debe tener en cuenta que tanto el lavado de activos como el financiamiento del terrorismo dan origen a riesgos de reputación, operativos y legales a que puede exponerse una entidad financiera, comprometiendo su estabilidad y viabilidad económica.

La debida diligencia en las transacciones y transferencias de fondos que diariamente ejecutan las instituciones bancarias por cuenta de sus clientes, hace necesario identificar aquellas que tienen un origen legítimo, de las que se pretenden realizar con la finalidad de encubrir negocios ilícitos o financiar acciones terroristas.

Con tal propósito, los bancos deben adoptar precauciones para tener un adecuado conocimiento de sus clientes, de las actividades que desarrollan y de las características más relevantes de las operaciones que éstos realizan. Asimismo, deben interiorizarse sobre los fundamentos en que se apoyan esas operaciones cuando no sean concordantes con el giro o profesión del cliente o, aun siéndolo, parezcan desmedidas o inusuales, sea por su monto, su frecuencia, o sus destinatarios, en el caso de transferencias de fondos.

Cabe mencionar que las directrices contra el lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva se han venido construyendo a partir de la adopción de una reglamentación internacional. Esta reglamentación que, en lo principal, es atingente al sector bancario, está plasmada en las recomendaciones del Grupo de Acción Financiera Internacional (GAFI), en los documentos del Comité de Supervisión Bancaria de Basilea y en las buenas prácticas de otros organismos internacionales.

A lo antes mencionado se suman las iniciativas de la Mesa Intersectorial sobre Prevención y Combate al Lavado de Activos y al Financiamiento del Terrorismo, creada mediante el Decreto N°1724 del Ministerio de Hacienda, publicado en el D.O el 19 de noviembre de 2015, que institucionaliza el Sistema Nacional Antilavado de Activos y contra el Financiamiento del Terrorismo y la Estrategia Nacional para la Prevención y Combate al Lavado de Activos y al Financiamiento del Terrorismo.

El marco jurídico chileno para las actividades desarrolladas por las entidades bajo la supervisión de esta Comisión está conformado por las disposiciones contenidas en la Ley General de Bancos y por instrucciones de este Organismo. No obstante, en materia de lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva, las entidades bancarias también deben cumplir con otras disposiciones de carácter general emanadas de leyes de la República, como es el caso de la Ley N°19.913 de fecha 18 de diciembre de 2003, que creó la Unidad de Análisis Financiero (UAF), organismo que en virtud del cumplimiento de su objetivo emite normativa a la cual los bancos deben ceñirse.

La citada ley N°19.913 establece que las personas naturales y las personas jurídicas que se indican están obligadas a reportar las operaciones sospechosas que adviertan en el ejercicio de sus actividades, entre las cuales están los bancos y otras entidades supervisadas por esta Comisión.

Asimismo, define por operación sospechosa, todo acto, operación o transacción que, de acuerdo con los usos y costumbres de la actividad de que se trate, resulte inusual o carente de justificación económica o jurídica aparente, sea que se realice en forma aislada o reiterada.

De acuerdo con dicha ley, los bancos están obligados a reportar operaciones sospechosas, a mantener registros especiales por el plazo mínimo de cinco años e informar a la Unidad de Análisis Financiero cuando esta lo requiera, de toda operación en efectivo superior al equivalente a 10.000 dólares de los Estados Unidos de América o su equivalente en pesos, según el valor del dólar observado el día en que se realizó la operación. Asimismo, deben informar todos los actos, transacciones u operaciones que se indican en el artículo 38 de la Ley N° 19.913, referidas a personas naturales o jurídicas que sean señaladas en los listados de las resoluciones del Consejo de Seguridad de Naciones Unidas.

En todo caso, cabe tener presente lo dispuesto en el artículo 154 de la Ley General de Bancos acerca de la reserva y secreto bancario y en el artículo 6° de la Ley N°19.913, sobre prohibición de informar al afectado o a terceras personas sobre la información enviada a la UAF u otros antecedentes al respecto.

Las disposiciones señaladas en este Capítulo son las mínimas que deben observar los bancos para la adopción de un sistema sobre prevención del lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva, y su cumplimiento forma parte de la evaluación que lleva a cabo este Organismo sobre la gestión integral de riesgos, sin perjuicio de las sanciones que puede imponer en caso de incumplimiento, de acuerdo con lo dispuesto en el artículo 19 de la Ley General de Bancos.

En el contexto del compromiso de cooperación entre Chile y Estados Unidos de Norteamérica para combatir la evasión tributaria de sus nacionales, las autoridades de ambos países firmaron un Acuerdo Intergubernamental (IGA) al amparo del Tratado para evitar la Doble Tributación, de 4 de febrero de 2010, con el objeto de establecer la forma de cumplimiento de la Foreign Account Tax Compliance Act (FATCA) por parte de los bancos y otras entidades financieras obligadas a reportar por esta ley.

El cumplimiento de la ley FATCA involucra que los bancos deben registrarse ante el U.S. Internal Revenue Service (IRS) y reportarle anualmente la información relativa a las "US Accounts" requerida para fines de tributación en Norteamérica.

Lo anterior obliga a los bancos a efectuar un due dilligence para identificar y reportar las "US accounts" en los términos descritos en el IGA, y contar con procesos operativos y tecnológicos adecuados para el cumplimiento del Acuerdo.

Para los efectos de este Capítulo, son clientes todas las personas naturales y jurídicas con las cuales la entidad establece o mantiene una relación de origen legal o contractual, como consecuencia de la prestación de un servicio o contratación de un producto, ofrecido en el marco de las actividades propias de su giro y de conformidad a las disposiciones legales y reglamentarias. Esta relación puede ser ocasional o habitual.

II. SISTEMA DE PREVENCIÓN DE LAVADO DE ACTIVOS, FINANCIAMIENTO DEL TERRORISMO Y LA NO PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA.

1. Condiciones generales de un sistema para la prevención del lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva.

Un sistema de prevención de lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva está fundado en el concepto de "conozca a su cliente".

Los principales componentes de este sistema dicen relación con la existencia de un marco de políticas y procedimientos, la presencia de un Oficial de Cumplimiento, la creación de un comité de prevención, la existencia de herramientas para la detección, monitoreo y reporte de operaciones inusuales, la definición de políticas relacionadas con selección de personal y capacitación, la existencia de un código de conducta interno y de una función de auditoría independiente.

El Directorio deberá aprobar el sistema de prevención de lavado de acti¬vos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva, con todos los componentes señalados precedentemente. El sistema deberá ser acorde al volumen y complejidad de las operaciones de la entidad, incluidas sus filiales y sociedades de apoyo al giro cuando corresponda, y de la presencia internacional que pudiera tener. A su vez, deberá recibir información periódica sobre las operaciones analizadas, las acciones realizadas sobre ellas, aquellas informadas a la Unidad de Análisis Financiero y también sobre el cumplimiento de las políticas y procedimientos internos.

Si el banco tiene sucursales o filiales en el exterior, el Directorio deberá velar porque las leyes y regulaciones del país anfitrión permitan cumplir adecuadamente las exigencias establecidas en este Capítulo. En el caso que ello no sea posible, deberá informarlo a esta Comisión, junto con las medidas que se adopten para mitigar dicha situación.

2. Debida Diligencia y Conocimiento del Cliente.

2.1 Elementos centrales de una debida diligencia y conocimiento del cliente

Es obligación no delegable del banco identificar y conocer a sus clientes y realizar una debida diligencia sobre ellos, considerando lo establecido en la Circular N°59 de la UAF, que modificó el Título III de su Circular N°49. Dicha norma contempla una serie de medidas fundamentales, las cuales deben ser abordadas desde una perspectiva prudencial, vale decir, que se configure como un mecanismo de gestión eficaz de los riesgos a los cuales está expuesta una entidad y no sólo sea una herramienta orientada a la prevención formal.

Las medidas que definen el proceso de Debida Diligencia y Conocimiento del Cliente (DDC) se pueden sintetizar en las acciones:

(a) Identificar al cliente y verificar su identidad utilizando para ello documentos, datos o información confiable, de fuentes independientes.

(b) Identificar al beneficiario final y tomar todas las medidas razonables necesarias para verificar su identidad, de manera tal que el banco esté convencido de que conoce quién es éste, en concordancia con las disposiciones establecidas en la Circular N°57 de la UAF, o aquella que la reemplace. Para el caso de personas y otras estructuras jurídicas, esto debe incluir que el banco entienda la estructura de titularidad y de control del cliente, identificando a la o las personas naturales que ejercen el control efectivo en la toma de decisiones de dichas entidades.

(c) Entender y obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial.

(d) Realizar una debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación, para que aquellas que se realicen sean consistentes con el conocimiento que tiene el banco sobre el cliente, su actividad comercial y el perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos.

La debida diligencia y conocimiento del cliente comienza desde el momento en que, con motivo de una operación, éste se vincula con la entidad bancaria. Por lo tanto, el banco requiere la elaboración de políticas y procedimientos de aceptación e identificación de clientes, y verificación de información, los que deberán tener en cuenta, entre otros factores, los antecedentes del cliente; perfil de riesgo; monto y origen de los fondos involucrados; el país de origen de éstos y si dicho país cumple con los estándares mínimos de aceptación exigidos; y sus relaciones societarias u otros indicadores de riesgo. Para el caso de los clientes que son personas o estructuras jurídicas, los bancos deben entender plenamente la naturaleza del negocio y su estructura accionaria y de control. Si se trata de una persona expuesta políticamente o pasa a esa condición durante el transcurso de la relación comercial, deberá contar con la aprobación de la alta administración.

Para una adecuada identificación de los clientes que no mantengan una cuenta corriente con la institución, pero que habitual u ocasionalmente realicen operaciones con el banco, se recomienda al menos aplicar las exigencias establecidas al respecto en el Capítulo 2-2 de esta Recopilación. No obstante, considerando la naturaleza, características y nivel de riesgo de los productos y servicios que contraten con éste, podrán omitirse ciertos requisitos como, por ejemplo, la exigencia de una fotografía del cliente y la impresión digital. Las políticas deberán referirse a los procedimientos que deben aplicarse en estos casos.

Asimismo, los bancos deberán considerar las instrucciones impartidas en la citada Circular N°59 de la UAF, para la implementación de los distintos parámetros de una DDC, las que podrán ser reforzadas o simplificadas, en función del riesgo de los clientes, productos, servicios u otros.

Con la información obtenida, se deberán elaborar perfiles de clientes, que permitan determinar en forma aproximada, el volumen y tipo de operaciones que harán éstos en el futuro.

Para los casos de operaciones no habituales o cuando se trate de clientes ocasionales o expuestos políticamente, el banco deberá exigir una declaración sobre el origen de los fondos, cuando corresponda a una operación que supere el umbral menor entre el definido por la Ley N°19.913 y el reglamentado internamente. Esa declaración deberá acompañarse con documentación que la sustente.

2.2 Personas políticamente expuestas

Se entenderá como personas expuestas políticamente (PEP), a los chilenos o extranjeros que desempeñen o hayan desempeñado funciones públicas destacadas en algún país, Chile inclusive, a lo menos hasta un año de finalizado el ejercicio de las mismas. Se incluyen en esta categoría los jefes de estado o de un gobierno, políticos de alta jerarquía (entre ellos, a los miembros de mesas direc¬tivas de partidos políticos), funcionarios gubernamentales, judiciales o militares de alta jerarquía, altos ejecutivos de empresas estatales, así como sus cónyuges, sus parientes hasta el segundo grado de consanguinidad y las personas naturales con las que hayan celebrado un pacto de actuación conjunta mediante el cual tengan poder de voto suficiente para influir en sociedades constituidas en Chile.

De acuerdo con lo anterior, se entiende que en Chile a lo menos deberán estar calificados como PEP, sin que este enunciado sea taxativo:

- Presidente de la República, senadores, diputados y alcaldes.
- Ministros de la Corte Suprema y de las Cortes de Apelaciones.
- Ministros de Estado, subsecretarios, intendentes, gobernadores, secretarios regionales ministeriales, embajadores, jefes superiores de servicios tanto centralizados como descentralizados y el directivo superior inmediato que deba subrogar a cada uno de ellos.
- Comandantes en Jefe de las Fuerzas Armadas, General Director de Carabineros, Director General de Investigaciones y el superior inmediato que deba subrogar a cada uno de ellos.

- Directores y ejecutivos principales de empresas estatales, según lo definido en la Ley N°18.045.
- Directores de sociedades anónimas nombrados por el Estado o sus organismos.
- Miembros de las directivas de los partidos políticos.
- Fiscal Nacional del Ministerio Público y Fiscales Regionales.
- Contralor General de la República.
- Consejeros del Banco Central de Chile.
- Presidente y Consejeros del Consejo de Defensa del Estado.
- Ministros del Tribunal Constitucional.
- Ministros del Tribunal de la Libre Competencia.
- Integrantes titulares y suplentes del Tribunal de Contratación Pública.
- Miembros del Consejo de Alta Dirección Pública.

Los elementos mínimos que las instituciones deben considerar para la relación con PEP se encuentran contenidos en el Capítulo 1-16 de la RAN.

2.3 Beneficiario final

La definición de beneficiario final para efectos de este Capítulo deberá considerar aquella establecida en la Circular N°57 de la UAF, al igual que las correspondientes instrucciones sobre las obligaciones de identificación, verificación y registro de datos de estos para personas y estructuras jurídicas que en ella se señalan, así como también considerar las evaluaciones de riesgo sectoriales que indique la UAF.

Cabe agregar que para personas y estructuras jurídicas, incluidas las organizaciones sin fines de lucro (OSFL), deberá demostrarse la existencia de la sociedad o entidad, según sea el caso, mediante copias de las escrituras e inscripciones correspondientes, la identificación de los propietarios o fundadores de la empresa o institución -accionistas o socios- y de las personas que componen su nivel directivo y los cargos que ocupan, de acuerdo al tipo de entidad de que se trate, incluidas aquellas personas que pueden disponer de sus recursos. Asimismo, deberán identificarse sus representantes legales, las actividades que desarrolla la entidad, su dirección, números telefónicos y demás información de contacto.

2.4 Transferencias electrónicas de fondos

Especial atención se deberá tener en el caso de transferencias de fondos en cuanto a identificar al ordenante y al beneficiario. Para dichos efectos, se deben considerar instrucciones de la Circular N°59 de la UAF, que modificó el Título V de su Circular N°49, así como las directrices sobre su aplicación que dicho servicio imparta en el marco de un enfoque basado en riesgos, en concordancia con lo dispuesto en el inciso segundo del artículo 2° de la Ley N°19.913; además de las instrucciones generales sobre identificación y respaldo de tales operaciones, contenidas en el Capítulo 1-7 de esta Recopilación.

2.5 Banca Corresponsal

Por su importancia requiere especial atención la banca corresponsal. En efecto, en lo que se refiere a las relaciones de corresponsalía y otras con la banca transnacional, las instituciones financieras, entre otros factores, además de aplicar las medidas sobre conocimiento de sus clientes ya señaladas, deberán: i) reunir información suficiente sobre los bancos con los cuales mantengan cualquier tipo de relación que les permita comprender cabalmente la naturaleza de los negocios que éstos desarrollan y verificar la reputación y la calidad de su supervisión; ii) evaluar las políticas y procedimientos aplicados para detectar operaciones de lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva; iii) documentar las respectivas responsabilidades de cada institución, cuando sea del caso; y, iv) obtener la aprobación de la alta gerencia antes de establecer nuevas relaciones corresponsales.

En todo caso, los bancos no deberán establecer relaciones comerciales o efectuar operaciones con bancos denominados como pantallas o ficticios.

2.6 Mantención de registros

La entidad financiera deberá mantener actualizados los antecedentes de sus clientes en el curso de su relación comercial, de modo de asegurarse que los datos de identificación y financieros estén siempre al día. Lo anterior, con el objeto de que les permita asegurar que las operaciones que realizan esos clientes son coherentes con la actividad, sus negocios y su perfil de riesgo.

La institución debe prevenir al cliente de su obligación de actualizar, a lo menos anualmente, los datos que varíen, según el producto o servicio de que se trate, suministrando los antecedentes correspondientes. Asimismo, esta deberá verificar y asegurarse, por los medios que estime más adecuados, que la información sobre la identificación entregada por los clientes corresponda a la realidad. Si existieren dudas sobre su veracidad o el cliente impidiere su adecuada identificación, el banco deberá evaluar el término de la relación comercial y emitir un reporte de operación sospechosa a la Unidad de Análisis Financiero.

En concordancia con lo dispuesto en el artículo 5° de la Ley N°19.913, la información de estos registros debe mantenerse por un plazo mínimo de 5 años. En este sentido, para aquellas operaciones ocasionales o de personas que ya no son clientes del banco, dicho periodo debe contarse desde la última operación registrada o la fecha de término de la relación contractual, según corresponda.

3. Manual de políticas y procedimientos.

Las instituciones financieras deben contar con un manual que establezca las políticas y procedimientos que deben aplicar para evitar verse envueltas o servir de medio para la facilitación o realización de operaciones de lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva.

Dichas políticas y procedimientos son la base para establecer y poner en práctica un adecuado sistema de prevención y detección de lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva.

Los elementos esenciales que deben contemplar las políticas, corresponden, a lo menos, a la debida diligencia y conocimiento de su cliente, desarrollo de adecuados métodos de vigilancia y relaciones con la banca corresponsal. Además, deben estar claramente identificados los roles y responsabilidades que le corresponden a todo el personal del banco, de forma que su cumplimiento pueda ser objeto de revisión.

De igual forma, las políticas de prevención y detección que establezcan los bancos deben diferenciar claramente los delitos de lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva (LA/FT/ADM), dado que existen diferencias importantes entre ambos, razón por la cual deben tomar las precauciones necesarias para que ambos puedan estar debidamente identificados.

En particular para el caso del financiamiento del terrorismo y la no proliferación de armas de destrucción masiva, los sistemas preventivos de las entidades deben tener como objetivo detectar los actos, operaciones o transacciones sospechosas de proveer fondos con la finalidad de ser utilizados en la comisión de cualquiera de los delitos terroristas incluidos en la ley 18.314, así como los que resulten sospechosos de ser solicitados o recaudados para estos mismos fines, además de aquellas operaciones en que actúen personas naturales o jurídicas que sean señaladas en los listados de las resoluciones del Consejo de Seguridad de Naciones Unidas. Dichos listados se encuentran disponibles en la web de la UAF y las entidades deben considerar la permanente revisión y monitoreo de ellas, de manera de poder reportar de inmediato una operación sospechosa cada vez que se detecte a una persona, empresa o entidad que esté mencionada en alguna de ellas.

Asimismo, se deben considerar los tipos OSFL que presenten mayores riesgos de abuso con fines de LA/FT/ADM, de acuerdo con las evaluaciones de riesgo sectoriales que indique la UAF, así como los criterios adicionales que defina cada institución.

El manual debe permanecer actualizado, es decir, debe incluir los nuevos productos y servicios que ofrezcan. En estos últimos se deben evaluar los riesgos previo a su lanzamiento, así como las nuevas tecnologías en que se sustenta su oferta, considerando el uso de los desarrollos tecnológicos que permiten también poner a disposición de los clientes productos y servicios preexistentes, además de considerar las nuevas disposiciones que la UAF establezca para los sujetos obligados. Asimismo, deben contemplarse pautas relativas al análisis que debe hacerse de las transacciones que realicen sus clientes, particularmente cuando ellas no coincidan con la actividad o giro conocido de éstos, sea por su monto, frecuencia, destinatarios, remitentes, etc.

Por otra parte, para el caso de detección de operaciones que merezcan sospechas, deben establecerse procedimientos específicos que consideren el discreto manejo y recopilación de los antecedentes y las etapas y plazos que se deben seguir para informar tales operaciones a quien corresponda.

El manual también deberá contener procedimientos para el adecuado seguimiento de sus clientes, los que deben ser diferenciados en función del nivel de riesgo de estos. En este ámbito, también se deben considerar las relaciones comerciales y transacciones con personas naturales o jurídicas de o en países que apliquen de manera insuficiente las recomendaciones del GAFI. Para los clientes que estén dentro de la categoría de políticamente expuestos o para personas que, de acuerdo con su perfil, pudieran estar expuestas a ser utilizadas para el lavado de activos, corresponderá desarrollar un sistema especial de seguimiento de sus operaciones.

4. Oficial de Cumplimiento.

El Oficial de Cumplimiento deberá ser un funcionario de confianza, independiente de las áreas tomadoras de riesgo, operativa y de auditoría interna; tener un nivel gerencial, cuya función y responsabilidad principal será mantener una coordinación interna respecto de la vigilancia de las operaciones de los clientes con la entidad y sus filiales, la observancia de las instrucciones del manual de procedimientos, el conocimiento de los casos sospechosos y su comunicación al Comité de Prevención de Lavado de Activos, Financiamiento del Terrorismo y la No Proliferación de Armas de Destrucción Masiva.

El banco podrá incluir en las funciones del Oficial de Cumplimiento, las relativas a las labores que impone la ley FATCA.

De acuerdo al tamaño y naturaleza de la entidad, el Oficial de Cumplimiento deberá contar con recursos humanos y tecnológicos adecuados.

5. Comité de Prevención de Lavado de Activos, Financiamiento del Terrorismo y la No Proliferación de Armas de Destrucción Masiva.

Dependiendo de su tamaño, la institución deberá constituir un Comité de Prevención de Lavado de Activos, Financiamiento del Terrorismo y la No Proliferación de Armas de Destrucción Masiva. Es deseable que este Comité esté integrado por a lo menos un director (no exigible para sucursal de entidad extranjera), el gerente general, a lo menos un gerente de área, el fiscal y el Oficial de Cumplimiento.

Entre sus funciones estará la de planificar y coordinar las actividades de cumplimiento de las políticas y procedimientos sobre las materias definidas por la entidad, relacionadas con aquellas de que trata este Capítulo. Además, deberá tomar conocimiento de la labor desarrollada y operaciones analizadas por el oficial de cumplimiento, como también, de decidir sobre mejoras a las medidas de control que éste proponga. Las funciones del Comité podrán incluir las tareas concernientes a la ley FATCA.

6. Herramientas para la detección, monitoreo y reporte de operaciones inusuales.

Las entidades deben contar con las herramientas tecnológicas adecuadas, que le permitan desarrollar sistemas de alertas, con el propósito de identificar y detectar operaciones inusuales. Dichos instrumentos deberán ser capaces de monitorear todas las transacciones realizadas por sus clientes a través de los diversos productos, prestando especial atención a aquellas que se efectúen con dinero en efectivo. Los parámetros de detección de operaciones inusuales considerarán en su aplicación el riesgo de clientes y/o productos.

Asimismo, deberán desarrollar y proveer a las instancias encargadas de ejecutar los servicios a los clientes, de una lista de "señales de alerta", que les sirvan para detectar operaciones inusuales o conocer operaciones sobre las cuales deben tener especial prudencia.

En este sentido, constituye una señal importante que debe ser comunicada a la unidad interna responsable cuando la entidad rechace una operación de un cliente o de un potencial cliente, producto de haber observado movimientos inusuales u otras características de sospecha que merecieron tal rechazo.

Las operaciones inusuales identificadas a través de estos sistemas de alerta implementados, ya sean de naturaleza computacional o producto del monitoreo de las áreas encargadas de ejecutar los servicios a los clientes, deberán ser reportadas a la unidad responsable de la evaluación de dichas operaciones. Cuando la identificación provenga de sistemas manuales, deberá contemplarse para el reporte a la unidad correspondiente el uso de un formulario especialmente diseñado. Todos los análisis efectuados de estas operaciones deben quedar debidamente documentados.

Identificada una operación sospechosa, la que ha sido definida en el Título I de este Capítulo, el banco está obligado a reportar dicha operación a la Unidad de Análisis Financiero.

7. Selección de personal, programas de capacitación y código de conducta interno.

Los bancos deben contar con políticas y normas de selección de personal y de conducta de éste en relación con clientes, con el objeto de prevenir la ocurrencia de operaciones de lavado de activos y financiamiento del terrorismo.

Asimismo, deben disponer de reglas de conducta contenidas en un código, que orienten la actuación de cada uno de sus funcionarios para el adecuado desarrollo del sistema de prevención adoptado, y prevenir y resolver conflictos de intereses que pudieran surgir con sus clientes.

La institución debe desarrollar programas de capacitación e instrucción permanentes a sus empleados, sobre las normas vigentes en materia de prevención de lavado de activos y financiamiento del terrorismo, sus políticas, los sistemas y los procedimientos en uso establecidos al respecto, como también, adiestramiento en cuanto a modalidades, técnicas o procedimientos utilizados en estas actividades.

Estos programas deberán comprender a todo el personal del banco, incluido el de sus filiales y sociedades de apoyo al giro cuando corresponda, y deberán ser periódicos y diferenciados según se trate de personal nuevo, de la función de cumplimiento, del área de operaciones o que atiende público en forma directa.

8. Auditoría interna.

El sistema de prevención de lavado de activos, financiamiento del terrorismo y la no proliferación de armas de destrucción masiva. implementado es responsabilidad de cada entidad y debe ser periódicamente evaluado por la auditoría interna de la institución, sobre la base de procedimientos definidos por la entidad, aprobados por la alta administración y de aceptación general.

III. EVALUACIÓN DE ESTA COMISION.

La evaluación de las temáticas contempladas en este Capítulo es parte del proceso de supervisión, evaluación y clasificación por gestión, de que trata el Capítulo 1-13 de esta Recopilación.

****