

CAPITULO 1-14 (Bancos)

MATERIA:

PREVENCION DEL LAVADO DE ACTIVOS 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.

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, aún 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 y financiamiento del terrorismo 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) y en el documento de debida diligencia con la clientela de los bancos, del Comité de Supervisión Bancaria de Basilea. También debe considerarse en ese sentido el trabajo desarrollado por la Asociación de Bancos e Instituciones Financieras de Chile A.G., materializado en el "Manual para la prevención del blanqueo de capitales".

El marco jurídico chileno para las actividades desarrolladas por las entidades bajo la supervisión de esta Superintendencia, está conformado por las disposiciones contenidas en la Ley General de Bancos y por instrucciones de este Organismo. No obstante, 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).

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 Superintendencia.

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 de 450 unidades de fomento en cualquier moneda.

En todo caso, cabe tener presente lo dispuesto en el artículo 154 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 y financiamiento del terrorismo y su cumplimiento forma parte de la evaluación que lleva a cabo este Organismo sobre la gestión integral de riesgos.

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 y Financiamiento del Terrorismo.

1.- Condiciones generales de un sistema para la prevención del lavado de activos.

Un sistema de prevención de lavado de activos 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 activos y financiamiento del terrorismo, 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.

2.- Conocimiento del cliente.

Es obligación del banco identificar y conocer a sus clientes. Esto debe abordarse desde una perspectiva prudencial, vale decir, que no sólo sea una herramienta orientada a la prevención, sino que también un mecanismo de gestión eficaz de los riesgos a los cuales está expuesta una entidad.

El 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, los que deberán tener en cuenta, entre otros factores, los antecedentes del cliente; perfiles de actividad; 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. Si se trata de una persona de influencia a nivel internacional, 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.

Cabe agregar que para personas jurídicas, deberá demostrarse la existencia de la sociedad, mediante copias legalizadas de las escrituras e inscripciones correspondientes, la identificación de los propietarios de la empresa -accionistas o socios- y de las personas que componen su nivel directivo y los cargos que ocupan, de acuerdo al tipo de sociedad de que se trate. Asimismo, deberán identificarse sus representantes legales, las actividades que desarrolla la empresa, su dirección y números telefónicos.

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 lo futuro.

Para los casos de operaciones no habituales o cuando se trate de clientes ocasionales o expuestos políticamente a nivel internacional, 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.

Especial atención se deberá tener en el caso de transferencias de fondos en cuanto a identificar al ordenante y al beneficiario.

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 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.

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 y financiamiento del terrorismo.

Dichas políticas y procedimientos son la base para establecer y poner en práctica un adecuado sistema de prevención de lavado de activos y financiamiento del terrorismo.

Los elementos esenciales que deben contemplar las políticas, corresponden, a lo menos, al 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.

El manual debe permanecer actualizado, es decir, debe incluir los nuevos productos y servicios que ofrezcan. 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. Para los clientes que estén dentro de la categoría de políticamente expuestos a nivel internacional 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.

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) tomar conocimiento de los controles implementados para detectar operaciones de lavado de activos y financiamiento del terrorismo; y, iii) documentar las respectivas responsabilidades de cada institución, cuando sea del caso.

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 y Financiamiento del Terrorismo.

El banco deberá informar a esta Superintendencia el nombre, cargo y dependencia del Oficial de Cumplimiento, información que deberá mantenerse actualizada.

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 y Financiamiento del Terrorismo.

Dependiendo de su tamaño, la institución deberá constituir un Comité de Prevención de Lavado de Activos y Financiamiento del Terrorismo. 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.

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 y financiamiento del terrorismo 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 Superintendencia.

La suficiencia y la eficacia de las políticas y procedimientos sobre prevención de lavado de activos y financiamiento del terrorismo adoptados por las instituciones, son parte del proceso de supervisión, evaluación y clasificación por gestión de que trata el Capítulo 1-13 de esta Recopilación.

IV.- Disposición Transitoria.

Para efectos de cumplir con el número 2 del título II. de este Capítulo, en cuanto a mantener actualizados los antecedentes de los clientes existentes a la fecha de la comunicación de esta norma, las entidades bancarias tendrán un plazo de un año para requerir la información correspondiente, sin perjuicio de solicitarlos cuando el cliente realice alguna transacción o demande la prestación de servicio sin haber actualizado previamente esa información.
