Manual de Inspección Antilavado de Dinero/Ley de Secreto Bancario

2010

ÍNDICE

Se indican por fecha las secciones del *Manual de Inspección BSA/AML* del FFIEC que han sido agregadas o modificadas de manera significativa respecto de la edición anterior.

INTRODUCCIÓN

Este *Manual de Inspección Antilavado de Dinero (AML)/Ley de Secreto Bancario (BSA)* del Consejo Federal de Inspección de Instituciones Financieras (FFIEC) constituye una guía para la realización de las inspecciones BSA/AML y las inspecciones a cargo de la Oficina de Control de Activos Extranjeros (OFAC, todas siglas en inglés). Un programa efectivo de cumplimiento BSA/AML exige una gestión de riesgos responsable, por lo tanto, el manual también proporciona una guía para identificar y controlar los riesgos asociados con el lavado de dinero y el financiamiento del terrorismo. El manual contiene un esquema general de las exigencias del programa de cumplimiento BSA/AML, los riesgos BSA/AML y las expectativas con respecto a la gestión de riesgos, las prácticas industriales responsables y los procedimientos de inspección. La creación de este manual contó con la colaboración de las agencias bancarias federales y estatales[1] y la Red de Lucha contra Delitos Financieros (FinCEN, por sus siglas en inglés), una división del Departamento del Tesoro de los Estados Unidos, para garantizar coherencia en la aplicación de las exigencias BSA/AML. Además, la OFAC asistió en el desarrollo de las secciones del manual relacionadas con los controles de la OFAC. Consulte los Apéndices A ("Normativa de la BSA"), B ("Directivas BSA/AML") y C ("Referencias BSA/AML") como guía.

Estructura del Manual

A fin de aplicar de manera eficaz los recursos y garantizar el cumplimiento de las exigencias de la BSA, la estructura del manual permite a los inspectores adaptar el campo de aplicación y procedimientos de inspección BSA/AML al perfil de riesgo específico de la organización bancaria. El manual está compuesto por las siguientes secciones:

- Introducción.
- Esquema general principal y procedimientos de inspección para analizar el programa de cumplimiento BSA/AML.
- Esquema general principal y procedimientos de inspección de las exigencias normativas y temas relacionados.
- Esquema general ampliado y procedimientos de inspección de programas consolidados y otros tipos de estructuras de programas de cumplimiento BSA/AML.

[1] El FFIEC se creó en Marzo de 1979 para establecer uniformidad en principios, normas y formularios de informes y para fomentar la regularidad en la supervisión de las instituciones financieras. El Consejo está compuesto por seis miembros con derecho a voto: La Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Administración Nacional de Cooperativas de Crédito, la Oficina del Interventor Monetario, la Oficina de Supervisión de Instituciones de Ahorro y el Comité de Coordinación Estatal. Las actividades del Consejo cuentan con el respaldo de grupos de tareas formados entre agencias y por un Comité de Coordinación Estatal asesor, compuesto por cinco representantes de agencias estatales, que supervisan las instituciones financieras.

- Esquema general ampliado y procedimientos de inspección de productos y servicios.
- Esquema general ampliado y procedimientos de inspección de personas y entidades.
- Apéndices.

Las secciones del esquema general principal y ampliado proporcionan una guía escrita e información básica sobre cada tema; a cada esquema general le siguen los procedimientos de inspección. Las secciones (principales) del "Esquema general principal y procedimientos de inspección para analizar el programa de cumplimiento BSA/AML" y del "Esquema general principal y procedimientos de inspección de las exigencias normativas y temas relacionados" sirven como plataforma para la inspección AML/BSA y, en su mayoría, tratan las exigencias legales y normativas del programa de cumplimiento BSA/AML. Las secciones "Establecimiento del campo de aplicación y planificación" y "Análisis de riesgos BSA/AML" ayudan al inspector a desarrollar un plan de inspección adecuado basado en el perfil de riesgo del banco. En algunos casos, un tema puede estar cubierto tanto en la sección principal como en la expandida (por ej., transferencias de fondos y actividades con bancos corresponsales extranjeros). En tales casos, el esquema general principal y los procedimientos de inspección se ocupan de las exigencias de la BSA, mientras que el esquema general ampliado y los procedimientos de inspección tratan sobre los riesgos AML de la actividad específica.

Como mínimo, los inspectores deben utilizar los siguientes procedimientos de inspección incluidos en la sección "Esquema general principal y procedimientos de inspección para analizar el programa de cumplimiento BSA/AML" de este manual para asegurarse de que el banco cuente con un programa de cumplimiento BSA/AML idóneo según su perfil de riesgo:

- Establecimiento del campo de aplicación y planificación (consulte las páginas 20 a 22).
- Análisis de riesgos BSA/AML (consulte la página 34).
- Programa de cumplimiento BSA/AML (consulte las páginas 42 a 48).
- Desarrollo de conclusiones y finalización de la inspección (consulte las páginas 53 a 56).

Aunque los reglamentos de la OFAC no forman parte de la BSA, las secciones principales incluyen esquemas generales y procedimientos de inspección de las políticas, los procedimientos y los procesos de los bancos para garantizar el cumplimiento de las sanciones de la OFAC. Como parte de los procedimientos de establecimiento del campo de aplicación y planificación, los inspectores deben examinar el análisis de riesgos de la OFAC y las pruebas independientes del banco para determinar la profundidad del examen del programa de cumplimiento con la OFAC que se llevará a cabo durante la inspección. Consulte los procedimientos de inspección de la sección principal, "Oficina de control de activos extranjeros", en las páginas 176 a 178, como guía.

Las secciones ampliadas tratan sobre los rubros de actividades comerciales, productos, clientes o entidades específicos que podrían presentar desafíos y exposiciones únicos por los cuales los bancos deberían instituir políticas, procedimientos y procesos adecuados. Si no existieran los controles adecuados, estos rubros de actividades comerciales, productos,

clientes o entidades podrían originar riesgos BSA/AML. Además, la sección ampliada proporciona una guía sobre la gestión y las estructuras de programas de cumplimiento BSA/AML.

No todos los procedimientos de inspección principal y ampliada serán de probable aplicación a toda organización bancaria. Los procedimientos de inspección específicos que se deberán llevar a cabo dependerán del perfil de riesgo BSA/AML de la organización bancaria, la calidad y cantidad de pruebas independientes, los antecedentes de cumplimiento BSA/AML de la institución financiera y otros factores relevantes.

Antecedentes

En 1970, el Congreso de los Estados Unidos aprobó la Ley sobre Informes en Materia de Transacciones Extranjeras y en Moneda, comúnmente conocida como la "Ley de Secreto Bancario,"[2] que estableció las exigencias con respecto a la conservación y presentación de registros por parte de individuos particulares, bancos,[3] y otras instituciones financieras. La BSA fue diseñada para ayudar a identificar la fuente, el volumen y el movimiento de la moneda y otros instrumentos monetarios trasladados o transferidos a los Estados Unidos o hacia afuera de los Estados Unidos, o depositados en instituciones financieras. La ley buscó lograr ese objetivo exigiendo que los individuos particulares, bancos y otras instituciones financieras presenten declaraciones de transacción monetaria en el Departamento del Tesoro de los Estados Unidos (Tesoro de los Estados Unidos), identifiquen de manera adecuada las personas que lleven a cabo transacciones y cuenten con evidencia escrita conservando registros contables adecuados de las transacciones financieras. Estos registros contables permiten que las autoridades de aplicación pertinentes y las agencias regulatorias lleven a cabo investigaciones de violaciones penales, impositivas y normativas, si se requieren, y proporcionen evidencia útil para entablar una acción judicial en caso de lavado de dinero u otros delitos financieros.

La Ley de Control del Lavado de Dinero de 1986 intensificó la eficacia de la BSA al agregar las secciones interrelacionadas 8(s) y 21 de la Ley Federal de Seguro de Depósitos (FDIA) y la sección 206(q) de la Ley Federal de Cooperativas de Crédito (FCUA, todas siglas en inglés), cuyas secciones son aplicables de la misma manera a los bancos constituidos por cualquier estatuto.[4] La Ley de Control del Lavado de Dinero de 1986 imposibilita que se eludan las exigencias de la BSA al imponer la responsabilidad penal a toda persona o institución financiera que participe deliberadamente en el lavado de dinero, o que estructure transacciones para evitar declararlas. La ley de 1986 exigía

[2] 31 USC (Código de los Estados Unidos) 5311 *et seq*., 12 USC 1829(b) y 1951-1959. Consulte también 12 USC 1818(s) (instituciones de depósito con seguro federal) y 12 USC 1786(q) (cooperativas de crédito con seguro federal).

[3] Según la BSA, de acuerdo con lo aplicado por 31 CFR 103.11, el término "banco" incluye a todo agente, agencia, sucursal u oficina en los Estados Unidos de bancos comerciales, asociaciones de ahorro y préstamo, instituciones de ahorro, cooperativas de crédito y bancos extranjeros. En todo el manual, el término "banco" se usa genéricamente para hacer referencia a la institución financiera que se está inspeccionando.

[4] 12 USC 1818(s), 1829(b) y 1786(q), respectivamente.

que los bancos establecieran y realizaran procedimientos diseñados razonablemente para asegurar y supervisar el cumplimiento de las exigencias de la BSA con respecto a la conservación y presentación de los registros. Como resultado, el 27 Enero de 1987, todas las agencias bancarias federales emitieron reglamentos esencialmente similares que exigían que los bancos desarrollaran programas para el cumplimiento de la BSA.

La Ley Annunzio-Wylie contra el Lavado de Dinero de 1992 agravó las sanciones por violaciones de la BSA y el papel del Tesoro de los Estados Unidos. Dos años después, el Congreso de los Estados Unidos aprobó la Ley de Supresión del Lavado de Dinero de 1994 (MLSA, por sus siglas en inglés) que consideró con más detenimiento el papel del Tesoro de los Estados Unidos en la batalla contra el lavado de dinero.

En Abril de 1996, se desarrolló un Informe de actividades sospechosas (SAR, por sus siglas en inglés) para ser utilizado por todas las organizaciones bancarias de los Estados Unidos. Se exige que toda organización bancaria presente un SAR siempre que sospeche o tenga conocimiento de una violación delictiva de la ley federal o detecte una transacción sospechosa relacionada con actividades de lavado de dinero o con una violación de la BSA.

Como respuesta a los ataques terroristas del 11 de Septiembre de 2001, el Congreso de los Estados Unidos aprobó la Ley para Unir y Fortalecer a Norteamérica Mediante la Provisión de Herramientas Adecuadas Requeridas para Interceptar y Obstruir el Terrorismo (Ley PATRIOTA de los EE. UU.) de 2001. El título III de la Ley PATRIOTA de los EE. UU. corresponde a la Ley de Supresión del Lavado de Dinero Internacional y Lucha contra la Financiación del Terrorismo de 2001. La Ley PATRIOTA de los EE. UU. es sin duda la ley AML más importante promulgada por el Congreso de los Estados Unidos desde la BSA. Entre otras cosas, la Ley PATRIOTA de los EE. UU. penalizó la financiación del terrorismo y amplió el marco de la BSA al fortalecer los procedimientos de identificación de clientes; prohibir a las instituciones financieras negociar con bancos fantasmas extranjeros; exigir a las instituciones financieras llevar a cabo procedimientos de debida diligencia y, en algunos casos, procedimientos de debida diligencia especial en las cuentas de bancos corresponsales extranjeros y bancos privados; y mejorar el intercambio de información entre las instituciones financieras y el Gobierno de los Estados Unidos. La Ley PATRIOTA de los EE. UU. y su reglamento de ejecución también:

- Extendieron las exigencias del programa AML a todas las entidades financieras.[5] Consulte el Apéndice D ("Definición legal de institución financiera") para obtener más información.
- Aumentaron las sanciones civiles y penales por lavado de dinero.

[5] La Ley PATRIOTA de los EE. UU. amplió la exigencia del programa AML a todas las instituciones financieras, según se define dicho término en 31 USC 5312(a)(2). Sin embargo, a partir de la publicación de este manual, tan sólo ciertos tipos de instituciones financieras están sujetas a las normas definitivas que implementan las exigencias del programa AML del 31 USC 5318(h)(1), según lo establecido por la Ley PATRIOTA de los EE. UU. Las instituciones financieras que no están sujetas actualmente a una norma definitiva del programa AML están temporalmente exentas de las exigencias establecidas en la Ley PATRIOTA de los EE. UU. en cuanto a la creación de un programa AML, según se estipula en 31 CFR 103.170.

- Otorgaron autoridad al Secretario del Tesoro de los Estados Unidos para imponer "medidas especiales" a jurisdicciones, instituciones o transacciones que revistan "interés principal en cuanto al lavado de dinero".

- Facilitaron el acceso a los registros y exigieron a los bancos que respondan a las solicitudes normativas de información en un plazo de 120 horas.

- Exigieron que las agencias bancarias federales tengan en cuenta el registro AML de los bancos en el control de las fusiones y adquisiciones de bancos y otras aplicaciones relativas a combinaciones comerciales.

El Papel de las Agencias Gubernamentales con Respecto a la BSA

Algunas agencias gubernamentales desempeñan un papel clave en la ejecución de los reglamentos de la BSA, la elaboración de guías para las inspecciones, el control del cumplimiento de la BSA y la aplicación de la BSA. Estas agencias son el Tesoro de los Estados Unidos, la FinCEN y las agencias bancarias federales (Junta de Gobernadores del Sistema de Reserva Federal, Corporación Federal de Seguro de Depósitos, Administración Nacional de Cooperativas de Crédito, Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro). A escala internacional existen varias entidades gubernamentales multilaterales que apoyan la lucha contra el lavado de dinero y la financiación del terrorismo. Consulte el Apéndice E ("Organizaciones internacionales") para obtener información adicional.

Departamento del Tesoro de los Estados Unidos

La BSA autoriza al Secretario del Tesoro a exigir a las instituciones financieras que establezcan programas AML, presenten ciertos informes y mantengan ciertos registros contables de las transacciones. Algunas disposiciones de la BSA se han ampliado para cubrir no sólo a las instituciones de depósito tradicionales, tales como bancos, asociaciones de ahorro y cooperativas de crédito, sino también a instituciones financieras no bancarias, como negocios de servicios monetarios, casinos, agentes bursatiles, comisionistas del mercado de futuros financieros, fondos comunes de inversión, compañías de seguros y operadores de sistemas de tarjetas de crédito.

FinCEN

La FinCEN, una división del Departamento del Tesoro de Estados Unidos, es la entidad delegada para administrar la BSA. En esta calidad, la FinCEN expide reglamentos y guías interpretativas, brinda más alcance a las industrias reguladas, apoya las funciones de inspección que llevan a cabo las agencias bancarias federales, y ejerce acciones civiles cuando ello se justifica. La FinCEN se vale de las agencias bancarias federales para inspeccionar el cumplimiento de la BSA de los bancos que estén dentro de sus jurisdicciones. Otras obligaciones importantes de la FinCEN incluyen brindar a las autoridades de aplicación pertinentes apoyo en casos de investigación, identificar e

informar sobre tendencias y patrones que presenten los delitos financieros, y promover la cooperación internacional con todas sus contrapartes en todo el mundo.

Agencias Bancarias Federales

Las agencias bancarias federales tienen la responsabilidad de supervisar las diferentes entidades bancarias que operan en los Estados Unidos, incluidas las sucursales en el extranjero de bancos estadounidenses. Las agencias bancarias federales se encargan del establecimiento de estatutos (a través de la Administración Nacional de Cooperativas de Crédito, la Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro), los seguros (a través de la Corporación Federal de Seguro de Depósitos y la Administración Nacional de Cooperativas de Crédito) y la regulación y supervisión de los bancos.[6] 12 USC 1818 (s)(2) y 1786(q) exigen que la agencia bancaria federal respectiva incluya un control del programa de cumplimiento de la BSA en cada inspección de una institución de depósito asegurada. Las agencias bancarias federales pueden hacer uso de su autoridad, según la confiere la sección 8 de la Ley FDI, para exigir el cumplimiento de las reglas y los reglamentos bancarios respectivos, incluyendo el cumplimiento de la BSA.

Las agencias bancarias federales exigen que cada banco bajo su supervisión establezca y mantenga un programa de cumplimiento de la BSA.[7] Según la Ley PATRIOTA de los EE. UU., los reglamentos de FinCEN exigen que algunas instituciones financieras establezcan un programa de cumplimiento de AML que proteja contra el lavado de dinero y el financiamiento del terrorismo y asegure el cumplimiento de la BSA y sus reglamentos de ejecución. Cuando se aprobó la Ley PATRIOTA de los EE. UU., los bancos bajo la supervisión de las agencias bancarias federales ya tenían la obligación legal de establecer y mantener un programa de cumplimiento con la BSA que, entre otras cosas, exigía a los bancos identificar e informar prontamente toda actividad sospechosa. Por esta razón, 31 CFR 103.120 sostiene que se considera que los bancos regulados por agencias bancarias federales han cumplido con los requisitos del programa AML de la Ley PATRIOTA de los EE. UU. cuando desarrollan y mantienen un programa de cumplimiento de la BSA que cumple con los requisitos del ente regulador funcional federal[8] que rige dichos programas. En este manual, las exigencias del programa de cumplimiento de la BSA de cada agencia bancaria federal se denominan “programa de cumplimiento BSA/AML”.

---

[6] La Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos y la Oficina de Supervisión de Instituciones de Ahorro pueden colaborar con agencias bancarias estatales en la inspección, la supervisión y el cumplimiento BSA/AML de los bancos legalmente constituidos por autoridades estatales.

[7] Consulte 12 CFR 208.63, 12 CFR 211.5(m) y 12 CFR 211.24(j) (Junta de Gobernadores del Sistema de Reserva Federal); 12 CFR 326.8 (Corporación Federal de Seguro de Depósitos); 12 CFR 748.2 (Administración Nacional de Cooperativas de Crédito); 12 CFR 21.21 (Oficina del Interventor Monetario); y 12 CFR 563.177 (Oficina de Supervisión de Instituciones de Ahorro).

[8] Ente regulador funcional federal significa: Junta de Gobernadores del Sistema de Reserva Federal; Corporación Federal de Seguro de Depósitos; Administración Nacional de Cooperativas de Crédito; Oficina del Interventor Monetario; Oficina de Supervisión de Instituciones de Ahorro; Comisión de Valores y Bolsa o Comisión del Mercado de Futuros de Bienes.

Los bancos deben adoptar medidas razonables y prudentes para combatir el lavado de dinero y el financiamiento del terrorismo, y minimizar así su vulnerabilidad a los riesgos asociados con dichas actividades. Algunas organizaciones bancarias han sufrido daños en su reputación y han incurrido en sanciones monetarias civiles por no aplicar medidas de control apropiadas a nivel interno, lo que derivó en la falta de cumplimiento de las exigencias de la BSA. Además, debido a que la evaluación AML es parte del trámite de solicitud, todo lo que esté relacionado con BSA/AML puede afectar al plan estratégico del banco. Por esta razón, el compromiso de las agencias bancarias federales y de FinCEN de brindar orientación que pueda ayudar a los bancos a cumplir con la BSA constituye una alta prioridad en términos de supervisión.

Las agencias bancarias federales trabajan para asegurar que las organizaciones que supervisan comprendan la importancia que tiene disponer de un programa de cumplimiento BSA/AML eficaz. La gerencia debe estar alerta en este sentido, especialmente a medida que crecen los negocios y se incorporan nuevos productos y servicios. La evaluación de los bancos en cuanto al programa de cumplimiento BSA/AML y en cuanto al cumplimiento de las exigencias normativas de la BSA ha sido parte integral del proceso de supervisión durante años. Consulte el Apéndice A ("Normativa de la BSA") para obtener más información.

Como parte de un programa de cumplimiento BSA/AML firme, las agencias bancarias federales tienen como objetivo asegurar que los bancos cuenten con políticas, procedimientos y procesos que les permitan identificar e informar de transacciones sospechosas a las autoridades de aplicación pertinentes. Los procesos de supervisión de las agencias determinan si los bancos han establecido políticas, procedimientos y procesos adecuados, según su nivel de riesgo BSA/AML, para identificar e informar de actividades sospechosas y si brindan suficiente información detallada en los informes dirigidos a las autoridades de aplicación pertinentes para que éstos contribuyan a la investigación de las transacciones sospechosas informadas. Consulte los Apéndices B ("Directiva BSA/AML") y C ("Referencias BSA/AML") como guía.

El 19 de Julio de 2007, las agencias bancarias federales expidieron un informe estipulando sus políticas para exigir el cumplimiento de exigencias específicas de la BSA contra el lavado de dinero. El propósito del *Informe entre Agencias sobre el Cumplimiento de las Exigencias BSA/ AML (Informe entre Agencias sobre el Cumplimiento)* es garantizar que haya más coherencia entre las agencias en cuanto a las decisiones sobre el cumplimiento de las cuestiones de la BSA y brindar una perspectiva sobre los factores que fundamentan esas decisiones.[9]

OFAC

La OFAC administra e impone sanciones económicas y comerciales basadas en la política exterior estadounidense y sus objetivos de seguridad nacional; dichas sanciones están dirigidas a países extranjeros, terroristas y narcotraficantes internacionales, y aquellos que participen en actividades relacionadas con la proliferación de armas de

[9] Consulte el Apéndice R para obtener información adicional.

destrucción masiva. La OFAC actúa según las facultades especiales otorgadas al Presidente en tiempos de guerra o de emergencia nacional, así como bajo la autorización otorgada por legislación específica, que le permiten imponer controles a las transacciones y congelar los activos que estén bajo la jurisdicción de los EE. UU. Muchas de las sanciones se basan en mandatos de las Naciones Unidas y otros mandatos internacionales, son multilaterales en cuanto a su campo de aplicación, y suponen estrecha cooperación con gobiernos de países aliados.

Las exigencias de la OFAC son distintas a las de la BSA, pero ambas comparten un objetivo común de seguridad nacional. Por esta razón, muchas instituciones financieras consideran que el cumplimiento de las sanciones de la OFAC está relacionado con el cumplimiento de las obligaciones de la BSA; la inspección de supervisión del cumplimiento de la BSA tiene una conexión lógica con la inspección del cumplimiento de las instituciones financieras con las sanciones de la OFAC. Consulte el esquema general principal y los procedimientos de inspección, "Oficina de Control de Activos Extranjeros", en las páginas 165 a 175 y 176 a 178, respectivamente, como guía.

Lavado de Dinero y Financiamiento del Terrorismo

La BSA está destinada a proteger el sistema financiero de los Estados Unidos y las instituciones financieras que forman ese sistema de los abusos de los delitos financieros. Estos delitos financieros incluyen el lavado de dinero, el financiamiento del terrorismo y otras transacciones financieras ilícitas. El lavado de dinero y el financiamiento del terrorismo son delitos financieros que provocan efectos sociales y financieros potencialmente devastadores. Desde los beneficios del narcotraficante a los activos saqueados de las arcas del gobierno por funcionarios extranjeros deshonestos, los ingresos fraudulentos tienen el poder de corromper y en última instancia desestabilizar comunidades o economías en su totalidad. Las redes terroristas pueden agilizar sus actividades si tienen medios financieros y acceso al sistema financiero. Tanto en el lavado de dinero como en el financiamiento del terrorismo, los criminales pueden aprovecharse de las lagunas jurídicas y otras debilidades del sistema financiero legítimo para blanquear ingresos fraudulentos, financiar el terrorismo o llevar a cabo otras actividades ilegales, y, en última instancia, ocultar el propósito real de su actividad.

Las organizaciones bancarias deben desarrollar, implementar y mantener programas AML eficaces que se ocupen de las estrategias en constante cambio de los lavadores de dinero y los terroristas que intenten entrar al sistema financiero de los Estados Unidos. Un programa de cumplimiento BSA/AML responsable es decisivo para impedir y prevenir estos tipos de actividades dentro o por medio de los bancos y otras instituciones financieras. Consulte el Apéndice F ("Señales de advertencia de lavado de dinero y financiamiento del terrorismo") para ver ejemplos de actividades sospechosas que puedan indicar lavado de dinero o financiamiento del terrorismo.

Lavado de dinero

El lavado de dinero es una práctica delictiva que consiste en procesar las ganancias ilegales o el dinero "sucio", a través de una serie de transacciones, de esta manera los fondos son

"limpiados" para que parezcan ser fondos provenientes de actividades legales. El lavado de dinero generalmente no implica que haya moneda en cada fase del proceso de lavado. Aunque el lavado de dinero es un proceso variado y a veces complejo, fundamentalmente comprende tres pasos independientes que pueden ocurrir simultáneamente:

Colocación: La fase inicial y más vulnerable del lavado de dinero es la colocación. El objetivo consiste en introducir los ingresos ilegales en el sistema financiero sin atraer la atención de las instituciones financieras o las autoridades de aplicación de las leyes. Las técnicas de colocación incluyen el fraccionamiento de los depósitos en moneda en sumas que evadan las exigencias de presentar informes o la combinación de depósitos en moneda de empresas legales e ilegales. Un ejemplo puede incluir: dividir grandes sumas de dinero en efectivo en sumas más pequeñas y menos llamativas, las que son depositadas directamente en una cuenta bancaria; depositar un cheque recibido como reembolso por la cancelación de un paquete de vacaciones o una póliza de seguros; o comprar una serie de instrumentos monetarios (por ej., cheques de caja o giros postales) que luego son cobrados y depositados en cuentas de otras localidades o instituciones financieras. Consulte el Apéndice G ("Fraccionamiento") como guía adicional**.**

Transformación: La segunda fase del proceso de lavado de dinero es la transformación, que consiste en trasladar fondos por todo el sistema financiero, con frecuencia a través de una compleja serie de transacciones para crear confusión y complicar el rastreo documental. Los ejemplos de transformación incluyen el cambio de instrumentos monetarios por sumas mayores o menores, o la transferencia de fondos a varias cuentas y a través de éstas, en una o más instituciones financieras.

Integración: El objetivo final del proceso del lavado de dinero es la integración. Una vez que los fondos están en el sistema financiero y fueron aislados a través de la fase de transformación, se utiliza la fase de integración para crear la apariencia de legalidad por medio de transacciones adicionales. Estas transacciones protegen aun más a los delincuentes de una conexión registrada con los fondos brindando una explicación convincente acerca de la fuente de esos fondos. Los ejemplos incluyen la compra y reventa de bienes inmuebles, las inversiones en valores, los fideicomisos extranjeros u otros activos.

Financiamiento del Terrorismo

La motivación del financiamiento del terrorismo es ideológica, a diferencia de la búsqueda de beneficios económicos, que es generalmente la motivación de la mayoría de los delitos asociados con el lavado de dinero. El objetivo del terrorismo es intimidar a una población u obligar a un gobierno o a una organización internacional a realizar o abstenerse de realizar un determinado acto por medio de la amenaza de la violencia. Una infraestructura financiera efectiva es decisiva para las operaciones terroristas. Los grupos terroristas desarrollan fuentes de financiación que son relativamente móviles para garantizar que los fondos puedan ser utilizados para obtener materiales y otros elementos logísticos necesarios para perpetrar los actos terroristas. Por lo tanto, el lavado de dinero es con frecuencia un componente esencial del financiamiento del terrorismo.

Por lo general, los terroristas financian sus actividades a través de fuentes tanto ilegales como legítimas. Se ha descubierto que las actividades ilegales como la extorsión, el

secuestro y el narcotráfico, constituyen una fuente muy importante de financiamiento. Otras actividades que tienen esa característica incluyen el contrabando, el fraude, el hurto, el robo, el robo de identidad, la utilización de diamantes de sangre,[10] y el uso indebido de fondos de ayuda o de caridad. En el último caso, los donantes pueden desconocer que sus donaciones han sido desviadas para sustentar causas terroristas.

Se han descubierto también otras fuentes legítimas para proveer financiamiento a las organizaciones terroristas, estas fuentes legítimas de financiamiento son una diferencia clave entre los financistas del terrorismo y las organizaciones delictivas tradicionales. Además de las donaciones de caridad, las fuentes legítimas incluyen la protección de gobiernos extranjeros, la propiedad de negocios y el empleo de personal.

Aunque existe una motivación diferente entre los lavadores de dinero tradicionales y los financistas del terrorismo, los métodos reales utilizados para financiar las operaciones terroristas pueden ser los mismos o similares a aquellos métodos usados por otros delincuentes para lavar fondos. Por ejemplo, los financistas del terrorismo utilizan el contrabando de moneda, los depósitos fraccionados o las extracciones de cuentas bancarias; la compra de varios tipos de instrumentos monetarios, las tarjetas de crédito, de débito o prepagadas, y las transferencias de fondos. También existen pruebas de que algunas formas de banca informal (por ej., "*hawala*"[11]) han jugado un papel importante en la movilización de fondos terroristas. Las transacciones a través del *hawala* son difíciles de detectar dada la falta de documentación, su volumen y la naturaleza de las transacciones involucradas. El financiamiento de ataques terroristas no siempre requiere grandes sumas de dinero, y las transacciones asociadas pueden no ser complejas.

Sanciones Penales por Lavado de Dinero, Financiamiento del Terrorismo y Violaciones de la BSA

Las sanciones por lavado de dinero y financiamiento del terrorismo pueden ser graves. Una persona condenada por lavado de dinero puede tener que enfrentar hasta 20 años de prisión y una multa de hasta US$ 500.000.[12] Cualquier propiedad involucrada en una transacción, o que pueda ser localizable hasta los ingresos de la actividad delictiva, incluyendo bienes como

[10] Los diamantes de sangre provienen de áreas controladas por fuerzas o facciones opuestas a gobiernos legítimos y reconocidos internacionalmente, y se utilizan para financiar las acciones militares en oposición a esos gobiernos o en infracción a las decisiones del Consejo de Seguridad de las Naciones Unidas (www.un.org).

[11] El término "*hawala*" se refiere a un tipo específico de sistema informal de transferencia de valores. La FinCEN lo describe como "un método de transmisión de valores monetarios que es utilizado en algunas partes del mundo para realizar remesas, la mayoría de las veces realizadas por personas que desean enviar dinero de forma legítima a familiares que se encuentran en su país de origen". También se ha destacado que el *hawala*, y otros sistemas similares, están posiblemente siendo utilizados como canales para el financiamiento del terrorismo u otras actividades ilegales. Para obtener información adicional y orientación sobre los *hawalas* y el informe de la FinCEN al Congreso, según la sección 359 de la Ley PATRIOTA de los EE. UU., consulte el sitio Web de la FinCEN: www.fincen.gov.

[12] 18 USC 1956.

préstamos con garantía colateral, propiedad personal, y, bajo ciertas condiciones, cuentas bancarias en su totalidad (aun cuando parte de los fondos de la cuenta sea legítima), puede estar sujeta a confiscación. De conformidad con diversas leyes vigentes, los bancos y las personas físicas pueden incurrir en responsabilidad civil y penal por violaciones a leyes contra el lavado de dinero (AML) y contra el financiamiento del terrorismo. Por ejemplo, de acuerdo con el 18 USC 1956 y 1957, el Departamento de Justicia de los EE. UU. puede iniciar acciones penales por lavado de dinero que pueden incluir multas penales, prisión y acciones de confiscación.[13] Además, los bancos corren el riesgo de perder sus licencias, y los empleados bancarios corren el riesgo de ser despedidos e inhabilitados para ejercer la función bancaria.

Además, existen sanciones penales por violaciones dolosas a la BSA y sus reglamentos de ejecución según el 31 USC 5322 y por transacciones de fraccionamiento para evadir las exigencias de informe de la BSA según el 31 USC 5324(d). Por ejemplo, una persona, incluido un empleado bancario, que viole dolosamente la BSA o sus reglamentos de ejecución, está sujeta a una multa penal de hasta US$ 250.000 o a cinco años de prisión, o a ambas.[14] Una persona que cometa tal violación y también infrinja cualquier otra ley de los Estados Unidos o participe en un patrón de actividad delictiva está sujeta a una multa de hasta US$ 500.000 o a diez años de prisión, o a ambas.[15] Un banco que viole ciertas normas de la BSA, incluido el 31 U SC 5318(i) o (j), o las medidas especiales impuestas por el 31 U SC 5318A, enfrenta sanciones monetarias penales de hasta USD1 millón o del doble del valor de la transacción.[16]

Sanciones Civiles por Violaciones a la BSA

Según el 12 USC 1818(i) y 1786(k), y el 31 USC 5321, las agencias bancarias federales y la FinCEN, respectivamente, pueden iniciar acciones civiles para aplicar sanciones monetarias por violaciones a la BSA. Por otra parte, además de las acciones civiles y penales para aplicar sanciones monetarias iniciadas contra ellas, las personas físicas pueden ser apartadas de la actividad bancaria de acuerdo con el 12 USC 1818(e)(2) por violación a las leyes AML según el Título 31 del Código de los Estados Unidos, siempre que la violación no haya sido involuntaria o no deliberada. Todas estas acciones pueden ser iniciadas de oficio.

---

[13] 18 USC 981 y 982.

[14] 31 USC 5322(a).

[15] Id.

[16] Id.

ESQUEMA GENERAL PRINCIPAL Y PROCEDIMIENTOS DE INSPECCIÓN PARA EVALUAR EL PROGRAMA DE CUMPLIMIENTO BSA/AML

Establecimiento del Campo de Aplicación y Planificación: Esquema General

Objetivo*:* *Identificar los riesgos BSA/AML del banco, desarrollar el campo de aplicación de la inspección y documentar el plan. Este proceso incluye la determinación de la necesidad de personal de inspección y la pericia técnica, y la selección de los procedimientos de inspección que se llevarán a cabo.*

La inspección BSA/AML está destinada a analizar la eficacia del programa de cumplimiento BSA/AML del banco y el cumplimiento del banco con las exigencias normativas concernientes a BSA, que incluyen un control de las prácticas de gestión de riesgos.

Siempre que sea posible, se debe realizar el proceso de establecimiento del campo de aplicación y planificación antes de entrar al banco. Durante este proceso, puede ser útil tratar las cuestiones relativas a BSA/AML con la gerencia del banco, inclusive con el funcionario a cargo del cumplimiento de la BSA, personalmente o por teléfono. El proceso de establecimiento del campo de aplicación y planificación de la inspección generalmente comienza con el análisis de:

- Información de supervisión fuera del sitio.
- Informes de inspección y documentos previos.
- Puntos de la carta de solicitud llevados a cabo por la gerencia del banco. Consulte el Apéndice H (“Puntos de la carta de solicitud [Sección principal y ampliada]”) para obtener información adicional.
- Análisis de riesgos BSA/AML del banco.
- Base de datos que almacena la información de los informes sobre la BSA (Sistema en línea de recuperación de moneda y banca [Web CBRS]).
- Controles o auditorías independientes.

Control del análisis de riesgos BSA/AML del banco

El proceso de establecimiento del campo de aplicación y planificación de la inspeccion del análisis de riesgos BSA/AML del banco debe ser guiado por el inspector del análisis de

riesgos BSA/AML del banco. La información obtenida por el inspector permitirá el proceso de establecimiento del campo de aplicación y planificación, así como la evaluación de la suficiencia del programa de cumplimiento BSA/AML. Si el banco no ha desarrollado un análisis de riesgos, este hecho debe tratarse con la gerencia. A los efectos de la inspección, siempre que el banco no haya llevado a cabo un análisis de riesgos o que el análisis de riesgos no sea idóneo, el inspector debe realizar un análisis de riesgos. Consulte la sección del esquema general principal, "Análisis de riesgos BSA/AML", en las páginas 23 a 33, como guía en el desarrollo de un análisis de riesgos BSA/AML. La evaluación del análisis de riesgos BSA/AML forma parte de los procedimientos para establecer el campo de aplicación y planificación de la inspección, y la inclusión en el manual de una sección sobre análisis de riesgos no significa que los dos procesos se deban tratar por separado. Por el contrario, se le ha dado al análisis de riesgos su propia sección para enfatizar su importancia en el proceso de inspección y en el diseño de controles eficaces en función del riesgo de cada banco.

Pruebas Independientes

Como parte del proceso de establecimiento del campo de aplicación y planificación, los inspectores deben obtener y evaluar los documentos acreditantes de las pruebas independientes (auditoría)[17] del programa de cumplimiento BSA/AML del banco. El campo de aplicación y la calidad de la auditoría pueden proporcionar a los inspectores una noción de los riesgos particulares del banco, cómo se están gestionando y controlando esos riesgos y el nivel de cumplimiento de la BSA. El campo de aplicación y los documentos de las pruebas independientes pueden ayudar a los inspectores a comprender el alcance de la auditoría, y la calidad y cantidad de las pruebas de la transacción. Este conocimiento servirá al inspector para determinar el campo de aplicación de la inspección, la identificación de las áreas que requieran un examen más (o menos) riguroso, y para identificar cuándo se pueden necesitar procedimientos de inspección ampliados.

Plan de Inspección

Como mínimo, los inspectores deben realizar los procedimientos de inspección incluidos en las siguientes secciones de este manual para asegurar que el banco cuenta con un programa apto para el cumplimiento BSA/AML acorde a su perfil de riesgo:

- Establecimiento del campo de aplicación y planificación (consulte las páginas 20 a 22).
- Análisis de riesgos BSA/AML (consulte la página 34).
- Programa de cumplimiento BSA/AML (consulte las páginas 42 a 48).
- Desarrollo de conclusiones y finalización de la inspección (consulte las páginas 53 a 56).

[17] La referencia de las agencias bancarias federales a "auditar" no crea una expectativa de que la prueba independiente requerida deba ser realizada por un auditor específicamente designado, ya sea interno o externo. Sin embargo, la persona que realiza la prueba independiente no debe participar en ninguna parte del programa de cumplimiento BSA/AML del banco. Se deben informar los resultados directamente a la junta directiva o a un comité de auditoría constituido fundamental o íntegramente por directores externos.

La sección “Esquema general principal y procedimientos de inspección de las exigencias normativas y temas relacionados” incluye un esquema general y procedimientos de inspección de las políticas, los procedimientos y los procesos de los bancos para garantizar el cumplimiento de las sanciones de la OFAC. Como parte de los procedimientos de establecimiento del campo de aplicación y planificación, los inspectores deben examinar el análisis de riesgos de la OFAC y las pruebas independientes del banco para determinar la profundidad del examen del programa de cumplimiento con la OFAC que se llevará a cabo durante la inspección. Consulte el esquema general principal y los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 165 a 178, como guía.

El inspector debe desarrollar y documentar un plan de inspección inicial acorde al perfil de riesgo BSA/AML general del banco. Este plan puede cambiar durante la inspección como consecuencia de los resultados obtenidos dentro del sitio y cualquier cambio en el plan debe ser documentado de la misma manera. El inspector debe preparar una carta de solicitud para el banco. Los puntos de la carta de solicitud propuestos están detallados en el Apéndice H (“Puntos de la Carta de Solicitud [Sección Principal y Ampliada]”). Sobre la base del perfil de riesgo, la calidad de la auditoría, los resultados previos a la investigación y el trabajo de inspección inicial, los inspectores deben llevar a cabo procedimientos de inspección principales y ampliados adicionales, según sea pertinente. El inspector debe incluir una evaluación del programa de cumplimiento BSA/AML dentro del plan o ciclo de supervisión. En las organizaciones bancarias más grandes y más complejas, los inspectores pueden llevar a cabo varios tipos de investigaciones durante todo el plan o ciclo de supervisión para analizar el cumplimiento BSA/AML. Estos controles pueden enfocarse en uno o más rubros de la actividad comercial (p. ej., banca privada, financiación del comercio o relaciones con bancos corresponsales extranjeros), basados en el análisis de riesgos de la organización bancaria, y los resultados de auditorías e inspecciones recientes.

Pruebas de transacciones

Los inspectores realizan pruebas de transacciones para evaluar la aptitud del programa de cumplimiento del banco con las exigencias normativas, determinar la eficacia de sus políticas, procedimientos y procesos, y evaluar los sistemas de supervisión de actividades sospechosas. Las pruebas de transacciones constituyen un factor importante para sacar conclusiones acerca de la integridad de los procesos de gestión de riesgos y los controles generales del banco. Las pruebas de transacciones se deben realizar en cada inspección y deben hacerse en función del riesgo. Se pueden realizar las pruebas de transacciones tanto aplicando los procedimientos para las pruebas de transacciones que se encuentran en la sección de las pruebas independientes (auditoría) (consulte los procedimientos de inspección de la sección principal, “Programa de Cumplimiento BSA/AML”, en las páginas 42 a 48, como guía) o aplicando los procedimientos de las pruebas de transacciones que figuran en cualquier otra parte de las secciones principales o ampliadas.

El alcance de las pruebas de transacciones y las actividades realizadas está basado en diversos factores, que incluyen la estimación del inspector de los riesgos, los controles y la aptitud de las pruebas independientes. Una vez dentro del medio, se puede extender

el campo de aplicación de las pruebas de transacciones para tratar cualquier tema o inquietud que surja durante la inspección. Los inspectores deben documentar sus decisiones respecto al alcance de las pruebas de transacciones que realicen, las actividades sobre las cuales se llevarán a cabo, y los motivos de los cambios en el campo de aplicación de las pruebas de transacciones que se produzcan durante la inspección.

Información Disponible en el Banco de Datos de los Informes sobre la BSA

La planificación de la inspección también debe incluir un análisis de los SAR, los Informes de transacciones en efectivo (CTR, por sus siglas en inglés) y las exenciones a los CTR que el banco haya presentado. Los SAR, los CTR y las exenciones a los CTR se pueden descargar u obtener directamente del banco de datos en línea de los informes sobre la BSA (Web CBRS). Cada agencia bancaria federal cuenta con personal autorizado para obtener esta información del banco de datos de los informes sobre la BSA. Cuando se soliciten búsquedas en el banco de datos de los informes sobre la BSA, el inspector debe comunicarse con la persona o las personas adecuadas, dentro de su agencia, con la anticipación suficiente a la fecha del comienzo de la inspección para obtener la información requerida. Cuando un banco ha comprado otro banco o se ha fusionado con otro banco recientemente, el inspector también debe obtener información sobre los SAR, los CTR y las exenciones a los CTR del banco adquirido.

Se puede exhibir la información descargada en una hoja de cálculo electrónica, que contiene toda la información incluida en el documento original presentado por el banco, así como el Número de control del documento (DCN, por sus siglas en inglés) del Servicio de Impuestos Internos (IRS), y la fecha en la que se ingresó el documento en el banco de datos de los informes sobre la BSA. La información descargada puede ser importante para la inspección, ya que ayudará a los inspectores a:

- Identificar a clientes con grandes volúmenes de moneda de uso corriente.
- Colaborar con la selección de cuentas para las pruebas de transacciones.
- Identificar la cantidad y las características de los SAR presentados.
- Identificar la cantidad y el carácter de las exenciones.

Procedimientos de Inspección

Campo de aplicación y planificación

Objetivo*:* *Identificar los riesgos BSA/AML del banco, desarrollar el campo de aplicación de la inspección y documentar el plan. Este proceso incluye la determinación de la necesidad de personal de inspección y la pericia técnica, y la selección de los procedimientos de inspección que se llevarán a cabo.*

Para facilitar la comprensión del inspector del perfil de riesgo del banco y para establecer adecuadamente el campo de aplicación de la inspección BSA/AML, el inspector debe cumplir los siguientes pasos, en conjunción con el control del análisis de riesgos BSA/AML del banco:

1. Revisar los informes de inspecciónes anteriores, los documentos relacionados y las respuestas de la gerencia a los problemas de la BSA identificados anteriormente; identificar procedimientos de inspección que se hayan realizado; obtener información de contacto de la BSA; identificar informes y procesos que utiliza el banco para detectar actividades poco habituales; identificar operaciones bancarias de mayor riesgo que se hayan detectado anteriormente; y examinar las recomendaciones para la siguiente inspección. Además, debe comunicarse con la gerencia del banco, según corresponda, para tratar los siguientes temas:

   - Programa de cumplimiento BSA/AML.
   - Análisis de riesgos BSA/AML.
   - Sistemas de informe y supervisión de actividades sospechosas.
   - Nivel y grado de los sistemas automatizados BSA/AML.

   Para ver los temas anteriores, consulte las secciones de los procedimientos del esquema general y la inspección de este manual como guía.

2. Desarrollar una lista de puntos de la BSA que se incorporarán en la carta de solicitud de inspección integrada. Si la inspeccion del programa BSA es una inspeccion independiente, enviar la carta de solicitud al banco. Analizar los documentos de la carta de solicitud proporcionados por el banco. Consulte el Apéndice H (“Puntos de la carta de solicitud [Sección principal y ampliada]”).

3. Revisar la correspondencia entre el banco y su regulador principal, si esto no fue realizado con anterioridad por el inspector a cargo u otro personal dedicado a la inspección. Además, revisar la correspondencia que el banco o los reguladores principales han recibido de o han enviado a las agencias regulatorias externas y de aplicación de la ley relacionadas con el cumplimiento BSA/AML. Los comunicados, particularmente aquellos que se reciben de la FinCEN y del Centro de Cómputo Empresarial de Detroit del IRS (anteriormente el Centro de Cómputos de Detroit) pueden documentar cuestiones relevantes para la inspección, como las siguientes:

- Presentación de errores en los SAR, los CTR y las exenciones a los CTR.
- Sanciones monetarias civiles emitidas por o en curso de la FinCEN.
- Citaciones legales o confiscaciones de las autoridades de aplicación de la ley.
- Notificación de cierres obligatorios de cuentas de clientes extranjeros que no presten su cooperación y que mantengan cuentas corresponsales como exige el Secretario del Tesoro o el Procurador General de los Estados Unidos.

4. Revisar la información de los SAR, los CTR y las exenciones a los CTR obtenida de las descargas del banco de datos de los informes sobre la BSA. La cantidad de SAR, CTR y exenciones a los CTR presentadas deben obtenerse por un período definido, según lo determine el inspector. Tener en cuenta la siguiente información y analizar los datos de patrones inusuales, tales como:

   - Volumen de actividad y si es acorde con la ocupación del cliente o el tipo de negocio.
   - Cantidad y volumen en dólares de las transacciones que involucran a clientes de mayor riesgo.
   - Volumen de los CTR en relación con el volumen de las exenciones (p. ej.: si las exenciones adicionales causaron una disminución significativa en la presentación de CTR).
   - Volumen de los SAR y los CTR en relación con el tamaño del banco, los activos o los depósitos, y la ubicación geográfica.

   Las agencias bancarias federales no tienen volúmenes definidos o "cuotas" para las presentaciones de los SAR y los CTR para un tamaño de banco o una ubicación geográfica determinados. Los inspectores no deben criticar a un banco exclusivamente porque la cantidad presentada de SAR o CTR es menor que la presentada por bancos de similares características. Sin embargo, como parte de la inspección, los inspectores deben revisar los cambios significativos en el volumen o el carácter de los SAR y los CTR presentados, y analizar las razones potenciales de estos cambios.

5. Revisar los informes de auditoría interna y externa y los documentos para el cumplimiento BSA/AML, según sea necesario, para determinar la extensión y la calidad de las auditorías, los resultados, las respuestas de la gerencia y las medidas correctivas. Un control del campo de aplicación de la auditoría independiente, sus procedimientos y sus calificaciones proporcionará información valiosa sobre la aptitud del programa de cumplimiento BSA/AML.

6. En tanto que los reglamentos de la OFAC no forman parte de la BSA, la evaluación del cumplimiento con la OFAC se incluye frecuentemente en las inspecciones BSA/AML. Las agencias bancarias federales no tienen la función principal de identificar las violaciones a la OFAC, sino de evaluar la suficiencia de la implementación de políticas,

procedimientos y procesos del banco para asegurar el cumplimiento de las normativas de la OFAC. Para facilitar la comprensión del inspector del perfil de riesgo del banco y establecer adecuadamente el campo de aplicación de la inspección de la OFAC, el inspector debe cumplir los siguientes pasos:

- Revisar el análisis de riesgos del banco según la OFAC. El análisis de riesgos, que se puede incorporar al análisis de riesgos general de BSA/AML del banco, debe tener en cuenta los diversos tipos de productos, servicios, clientes, entidades, transacciones y ubicaciones geográficas en las que el banco participa, incluidos aquellos que son procesados por, a través de o hacia el banco para identificar la posible exposición de la OFAC.

- Revisar las pruebas independientes del banco de sus programas de cumplimiento con la OFAC.

- Revisar la correspondencia recibida de la OFAC y, según sea necesario, el área de las sanciones civiles en el sitio Web de la OFAC para determinar si el banco tenía cartas de advertencia, multas o sanciones impuestas por la OFAC desde la inspección más reciente.

- Revisar la correspondencia entre el banco y la OFAC (p. ej., los informes periódicos sobre transacciones prohibidas y, si es aplicable, los informes anuales de la OFAC sobre propiedad congelada).

Además de lo mencionado anteriormente, en las organizaciones bancarias más grandes y más complejas, los inspectores pueden llevar a cabo diversos tipos de inspecciones durante todo el plan o ciclo de supervisión para analizar el cumplimiento con la OFAC. Estos controles se pueden enfocar en uno o más rubros de la actividad comercial.

7. Sobre la base de los procedimientos de inspección ya descritos, en conjunción con el control del análisis de riesgos BSA/AML del banco, desarrollar un plan de inspección inicial. El inspector debe documentar adecuadamente el plan, así como cualquier cambio en el plan que se realice durante la inspección. El proceso de establecimiento del campo de aplicación y planificación debe asegurar que el inspector conozca el programa de cumplimiento BSA/AML del banco, el programa de cumplimiento con la OFAC, los antecedentes del cumplimiento y el perfil de riesgo (p. ej. productos, servicios, clientes, entidades, transacciones y ubicaciones geográficas).

Según sea necesario, se pueden llevar a cabo procedimientos de inspección de la sección principal y de la sección ampliada adicionales. En tanto que el plan de inspección puede cambiar en cualquier momento como consecuencia de los resultados obtenidos dentro del sitio, el análisis de riesgos inicial permitirá al inspector establecer un campo de aplicación razonable para el control BSA/AML. Para que el proceso de inspección sea exitoso, los inspectores deben mantener abierta la comunicación con la gerencia del banco y tratar las inquietudes relevantes a medida que surjan.

Análisis de Riesgos BSA/AML: Esquema General

Objetivo*:* *Evaluar el perfil de riesgo BSA/AML del banco y la aptitud del proceso de análisis de riesgos BSA/AML del banco.*

La evaluación del análisis de riesgos BSA/AML debe formar parte de los procedimientos de establecimiento del campo de aplicación y planificación de la inspección, y la inclusión en el manual de una sección sobre análisis de riesgos no significa que los dos procesos se daban tratar por separado. Por el contrario, se le ha dado al análisis de riesgos su propia sección para enfatizar su importancia en el proceso de inspección y en el diseño de controles eficaces en función del riesgo de cada banco.

Se deben aplicar los mismos principios de gestión de riesgos que el banco utiliza en las áreas operativas tradicionales para el análisis y la gestión de riesgos BSA/AML. Un análisis de riesgos bien definido permitirá identificar el perfil de riesgo BSA/AML del banco. Comprender el perfil de riesgo permite que el banco aplique procesos de gestión de riesgos adecuados al programa de cumplimiento BSA/AML para mitigar el riesgo. El proceso de análisis de riesgos permite a la gerencia identificar y mitigar rápidamente las deficiencias de los controles del banco. El análisis de riesgos debe proporcionar una observación exhaustiva de los riesgos BSA/AML presentándolos de una manera concisa y organizada y esta información debe intercambiarse y comunicarse a todos los rubros de la actividad comercial que tengan lugar en el banco, la junta directiva, la gerencia y el personal pertinente; como tal, la presentación del análisis de riesgos por escrito constituye una práctica responsable.

Existen muchos métodos y formatos eficaces que se utilizan para llevar a cabo un análisis de riesgos BSA/AML; por lo tanto, los inspectores no deben postular un método o formato en particular. La gerencia del banco debe decidir el método o formato adecuado, según el perfil de riesgo particular del banco. Cualquiera sea el formato que la gerencia opte por utilizar para su análisis de riesgos, todas las partes correspondientes deberán ser capaces de comprenderlo con facilidad.

El desarrollo del análisis de riesgos BSA/AML generalmente comprende dos pasos: primero, identificar las categorías de riesgos específicas (es decir, productos, servicios, clientes, entidades, transacciones y ubicaciones geográficas) que son exclusivas del banco; y segundo, llevar a cabo un análisis más detallado de los datos identificados para analizar los riesgos de la manera más óptima dentro de estas categorías. Al revisar el análisis de riesgos durante el proceso de establecimiento del campo de aplicación y planificación, el inspector debe determinar si la gerencia ha tenido en cuenta todos los productos, servicios, clientes, entidades, transacciones y ubicaciones geográficas y si fue adecuado el análisis detallado hecho por la gerencia de estas categorías de riesgos específicas. Si el banco no ha desarrollado un análisis de riesgos, este hecho debe tratarse con la gerencia. A los efectos de la inspección, siempre que el banco no haya llevado a

cabo un análisis de riesgos, o que el análisis de riesgos no sea adecuado, el inspector debe llevar a cabo un análisis de riesgos basándose en la información disponible.[18]

Evaluación del análisis de riesgos BSA/AML del banco

Un inspector debe revisar el programa de cumplimiento BSA/AML con suficiente conocimiento de los riesgos BSA/AML del banco para determinar si el programa de cumplimiento BSA/AML es idóneo y proporciona los controles necesarios para mitigar los riesgos. Por ejemplo, durante el proceso de establecimiento del campo de aplicación y planificación de la inspección, inicialmente, el inspector puede determinar que el banco tiene un perfil de riesgo alto, pero durante la inspección, puede determinar que el programa de cumplimiento BSA/AML mitiga estos riesgos de manera adecuada. Por otro lado, el inspector puede determinar, inicialmente, que el banco tiene un perfil de riesgo moderado a bajo; sin embargo, durante la inspección, puede determinar que el programa de cumplimiento BSA/AML del banco no mitiga estos riesgos de manera adecuada.

Cuando evalúa el análisis de riesgos, un inspector no debe necesariamente considerar cualquier indicador por sí solo como determinante de la existencia de un riesgo BSA/AML más bajo o más alto. El análisis de los factores de riesgo depende del banco y la conclusión sobre el perfil de riesgo debe realizarse teniendo en cuenta toda la información pertinente. Los bancos pueden determinar que algunos factores se deban ponderar más que otros. Por ejemplo, la cantidad de transferencias de fondos es, inequívocamente, un factor que debe tenerse en cuenta en el análisis de riesgos; sin embargo, para identificar y ponderar los riesgos de manera eficaz, el inspector debe observar otros factores asociados con esas transferencias de fondos, por ejemplo si se establecen a nivel internacional o nacional, los montos en dólares incluidos y el carácter de las relaciones con el cliente.

Identificación de categorías de riesgos específicas

El primer paso del proceso de análisis de riesgos es identificar los productos, los servicios, los clientes, las entidades y las ubicaciones geográficas específicos que son exclusivos del banco. Aunque los intentos de lavar dinero, financiar el terrorismo y llevar a cabo otras actividades ilegales a través de un banco pueden emanar de muchas fuentes diferentes, ciertos productos, servicios, clientes, entidades y ubicaciones geográficas pueden ser más vulnerables o pueden haber sido elegidos históricamente como centros de lavado dinero por responsables del lavado de dinero y criminales. Según las características específicas del producto, servicio o cliente en particular, los riesgos no son siempre los mismos. Diversos factores, como la cantidad y el volumen de las transacciones, las ubicaciones geográficas y el carácter de las relaciones con el cliente, deben tenerse en cuenta cuando el banco prepara su análisis de riesgos. Las diferencias en la manera en que el banco interactúa con el cliente (contacto directo o por medio de banca electrónica) también deben tenerse en cuenta. Debido a estos factores, los riesgos

[18] Consulte “Desarrollo de un análisis de riesgos BSA/AML por parte del inspector”, páginas 31 y 32, como guía.

variarán de un banco a otro. Al revisar el análisis de riesgos del banco, los inspectores deben determinar si la gerencia ha desarrollado un análisis de riesgos adecuado que identifique los riesgos significativos del banco.

Las secciones ampliadas de este manual tratan temas y proporcionan guías sobre rubros de la actividad comercial, productos y clientes específicos que pueden presentar desafíos y exposiciones únicos por los cuales los bancos necesiten instituir políticas, procedimientos y procesos adecuados. Si no existieran los controles adecuados, estos rubros de la actividad comercial, productos o clientes podrían elevar los riesgos BSA/AML agregados. El inspector debe prever que el proceso de análisis de riesgos continuo del banco trate los grados variables de riesgos asociados con sus productos, servicios, clientes, entidades y ubicaciones geográficas, según corresponda.

Productos y servicios

Ciertos productos y servicios ofrecidos por los bancos pueden plantear un mayor riesgo de lavado de dinero o financiamiento del terrorismo según el carácter del producto o servicio específico ofrecido. Tales productos y servicios pueden facilitar un mayor grado de anonimato o implicar la manipulación de grandes volúmenes de moneda o equivalentes a la moneda. A continuación, se enumeran algunos de estos productos y servicios, pero la lista no incluye a todos los existentes:

- Servicios de pago de fondos electrónicos: efectivo electrónico (p. ej., tarjetas prepagadas y de nómina), transferencias de fondos (a nivel internacional o nacional), transacciones pagaderas mediante la presentación de identificación apropiada (PUPID, por sus siglas en inglés), procesadores de pagos de terceros, remesas, cámara de compensación automatizada (ACH, por sus siglas en inglés), y cajeros automáticos (ATM, por sus siglas en inglés).
- Banca electrónica.
- Banca privada (a nivel internacional o nacional).
- Servicios fiduciarios y de gestión de activos.
- Instrumentos monetarios.[19]
- Cuentas corresponsales extranjeras (por ej., envíos en efectivo de grandes cantidades, actividad de depósitos vía maletines/bolsos, cuentas empleadas para pagos [PTA, por sus siglas en inglés] y giros en dólares estadounidenses).
- Financiación del comercio internacional.

[19] En este contexto, los instrumentos monetarios incluyen los cheques oficiales de bancos, cheques de gerencia, giros postales y cheques viajeros. Consulte la sección del esquema general ampliado "Compraventa de instrumentos monetarios", página 270, para obtener más información sobre los factores de riesgo y la mitigación de riesgo con respecto a los instrumentos monetarios.

- Servicios proporcionados a remitentes o procesadores de pagos de terceros.
- Cambio de moneda extranjera.
- Cuentas especiales o de concentración.
- Préstamos, especialmente préstamos garantizados con efectivo y valores negociables.
- Servicios de cuentas no depositables (p. ej., productos de inversión que no son para depositar y seguros).

Las secciones ampliadas de este manual tratan temas y proporcionan guías sobre los productos y servicios específicos que se describieron anteriormente.

Clientes y entidades

Si bien todo tipo de cuenta es potencialmente vulnerable al lavado de dinero o al financiamiento del terrorismo, ciertos clientes y entidades pueden plantear riesgos concretos de lavado de dinero debido al carácter de sus actividades comerciales, su ocupación o las actividades transaccionales anticipadas. En esta etapa del proceso de análisis de riesgos, es fundamental que los bancos tomen decisiones y no definan ni traten a todos los miembros de una categoría de clientes específica como capaces de plantear el mismo nivel de riesgo. Al analizar el riesgo que puedan plantear los clientes, los bancos deben tener en cuenta otras variables, como los servicios que se solicitan y las ubicaciones geográficas. Las secciones ampliadas de este manual tratan temas y proporcionan guías sobre los clientes y entidades específicos que se describen a continuación:

- Instituciones financieras extranjeras, incluyendo bancos y prestadores de servicios en moneda extranjera (p. ej., casas de cambio, tipo de cambio y transmisores de dinero).
- Instituciones financieras no bancarias (p. ej., negocios de servicios monetarios; casinos y clubes de apuestas; agentes de valores y comerciantes de piedras preciosas, metales preciosos o joyas).
- Políticos extranjeros de alto nivel y los miembros más cercanos de su familia y su círculo de colaboradores inmediatos (colectivamente conocidos como personalidades sujetas a exposición política [PEP, por sus siglas en inglés]).[20]
- Extranjeros no residentes (NRA)[21] y cuentas de ciudadanos extranjeros.

---

[20] Consulte el esquema general principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 145 a 150, y el esquema general ampliado, "Personalidades sujetas a exposición política", en las páginas 329 a 333, como guía.

[21] Es posible identificar las cuentas de los Extranjeros No Residentes (NRA) si se obtiene una lista de los clientes de las instituciones financieras que hayan presentado formularios W-8. Se puede obtener más información en www.irs.gov/formspubs.

- Corporaciones extranjeras y entidades comerciales nacionales, particularmente corporaciones instaladas en el exterior (tales como compañías fantasma nacionales y Compañías de inversión privada [PIC, por sus siglas en inglés] y corporaciones comerciales internacionales [IBC, por sus siglas en inglés])[22] situadas en ubicaciones geográficas de mayor riesgo.

- Agentes de depósitos, particularmente extranjeros.

- Negocios que manejan un alto flujo de efectivo (por ej., minimercados, restaurantes, tiendas minoristas, licorerías, distribuidores de cigarrillos, cajeros automáticos de propiedad privada, operadores de máquinas expendedoras, y garajes de estacionamiento de vehículos).

- Organizaciones no gubernamentales y entidades de beneficencia (extranjeras y nacionales).

- Prestadores de servicios profesionales (p. ej., abogados, contadores, médicos o agentes inmobiliarios).

Ubicaciones geográficas

Identificar las ubicaciones geográficas que puedan plantear un mayor riesgo es fundamental para los programas de cumplimiento BSA/AML de los bancos. Los bancos estadounidenses deben comprender y evaluar el riesgo específico que implica realizar negocios en ciertas ubicaciones geográficas, abrir cuentas a clientes provenientes de dichas ubicaciones y facilitar transacciones relacionadas con las mismas. Sin embargo, el riesgo geográfico en sí mismo no determina necesariamente el nivel de riesgo que puede plantear un cliente o una transacción, ni positiva ni negativamente.

Las ubicaciones geográficas de mayor riesgo pueden ser nacionales o internacionales. Las ubicaciones geográficas de mayor riesgo internacionales generalmente incluyen:

- Países sujetos a las sanciones de la OFAC, incluidos los estados que propician el terrorismo.[23]

- Países identificados por apoyar el terrorismo internacional bajo la sección 6(j) de la Ley de Administración de Exportaciones de los EE. UU. de 1979, según lo determinado por el Secretario de Estado.[24]

---

[22] Para ver una explicación sobre las PIC y IBC y orientación adicional al respecto, consulte el esquema general ampliado “Entidades comerciales (nacionales y extranjeras)”, en las páginas 357 a 363.

[23] En el sitio Web de la OFAC está disponible una lista de estos países, jurisdicciones y gobiernos: www.treas.gov/offices/enforcement/ofac.

[24] En el Informe sobre Terrorismo en los Países), realizado de forma anual, del Departamento de Estado titulado aparece una lista de los países que apoyan el terrorismo internacional. Este informe está disponible en el sitio Web de la Oficina de Lucha Contra el Terrorismo del Departamento de Estado, en: www.state.gov/s/ct/.

- Las jurisdicciones clasificadas como "de interés principal con respecto al lavado de dinero" por parte del Secretario del Tesoro de Estados Unidos, y las jurisdicciones sujetas a medidas especiales impuestas por este, a través de FinCEN, de conformidad con la sección 311 de la Ley PATRIOTA de los EE. UU.[25]

- Las jurisdicciones o los países en los que entidades internacionales, como el Grupo de Acción Financiera en Contra del Lavado de Dinero (FATF, por sus siglas en inglés), supervisan las deficiencias de los regímenes para combatir el lavado de dinero y el financiamiento del terrorismo.

- Importantes países y jurisdicciones de lavado de dinero identificados por el Informe Estratégico para el Control Internacional de Narcóticos (INCSR, por sus siglas en inglés) anual del Departamento de Estado de los Estados Unidos, particularmente, los países que han sido identificados como jurisdicciones de interés principal.[26]

- Centros financieros instalados en el exterior (OFC, por sus siglas en inglés).[27]

- Otros países identificados por el banco como de mayor riesgo debido a experiencia previa u otros factores (p. ej., consideraciones jurídicas o presunta corrupción oficial).

- Las ubicaciones geográficas nacionales de mayor riesgo pueden incluir, entre otras, oficinas bancarias que realizan actividades comerciales en ubicaciones designadas por el Gobierno de los EE. UU. como de mayor riesgo, o cuyos clientes se encuentran en dichas ubicaciones geográficas. Las ubicaciones geográficas de mayor riesgo nacionales incluyen:

    - Zonas de alta densidad de narcotráfico (HIDTA, por sus siglas en inglés).[28]

    - Zonas de alta densidad de delitos financieros (HIFCA).[29]

---

[25] Las notificaciones sobre las reglamentaciones propuestas y la reglamentación definitiva que acompañan la determinación de ser "de interés principal con respecto al lavado de dinero" y la imposición de medidas especiales de conformidad con la sección 311 de la Ley PATRIOTA de los EE. UU. están disponibles en el sitio Web de la FinCEN: www.fincen.gov/reg_section311.html.

[26] El INCSR, así como las listas de países y jurisdicciones que plantean un alto riesgo de lavado de dinero, se pueden consultar en la página Web (www.state.gov/p/inl/rls/nrcrpt) de la Oficina de Narcóticos Internacionales y Control de Autoridades del Departamento de Estado de los Estados Unidos.

[27] Los OFC ofrecen una variedad de productos y servicios financieros. Para obtener más información, incluidos los análisis de OFC, visite www.imf.org/external/ns/cs.aspx?id=55.

[28] La Ley contra el Abuso de Drogas de 1988 y la Ley de Reautorización del Gabinete de Política Nacional de Control de las Drogas (ONDCP) de 1998 autorizaron al Director del ONDCP a que designara las zonas de los Estados Unidos que exhiben graves problemas de narcotráfico y tienen un impacto nocivo en otras zonas del país como Zonas de alta densidad de narcotráfico (HIDTA). El Programa de HIDTA proporciona recursos federales adicionales a aquellas zonas que ayudan a eliminar o disminuir el narcotráfico y sus consecuencias nocivas. Se puede encontrar una lista de estas zonas en www.whitehousedrugpolicy.gov/hidta/index.html.

[29] Las Zonas de alta densidad de delitos financieros (HIFCA) se anunciaron por primera vez en la Estrategia Nacional contra el Lavado de Dinero de 1999 y se concibieron en la Ley Estratégica contra el Lavado de Dinero y los Delitos Financieros de 1998 a fin de concentrar las iniciativas de las autoridades de aplicación de la ley a nivel federal, estatal y local en las zonas de alta densidad de lavado de dinero. Se puede encontrar una lista de estas zonas en www.fincen.gov/hifcaregions.html.

Análisis de categorías de riesgos específicas

El segundo paso del proceso de análisis de riesgos implica un análisis más detallado de los datos obtenidos durante la etapa de identificación a fin de analizar de manera más adecuada el riesgo BSA/AML. Este paso implica la evaluación de los datos concernientes a las actividades de los bancos (p. ej., cantidad de: transferencias de fondos nacionales e internacionales; clientes de banca privada; cuentas de bancos corresponsales extranjeros; PTA; y ubicaciones geográficas nacionales e internacionales del área comercial y las transacciones de clientes del banco) con respecto al Programa de identificación de clientes (CIP, por sus siglas en inglés) e información de debida diligencia de los clientes (CDD, por sus siglas en inglés). El nivel y la complejidad del análisis pueden variar de un banco al otro. El análisis detallado es fundamental ya que dentro de cada tipo de producto o categoría de clientes existirán titulares de cuenta que planteen niveles variables de riesgo.

Este paso del proceso de análisis de riesgos le permite a la gerencia comprender aún más el perfil de riesgo del banco a fin de desarrollar las políticas, los procedimientos y los procesos adecuados para mitigar el riesgo general. Concretamente, en el análisis de los datos concernientes a las actividades del banco se deben tener en cuenta, según sea pertinente, los siguientes factores:

- Propósito de la cuenta.
- Actividad real o prevista de la cuenta.
- Tipo de negocio/ocupación del cliente.
- Ubicación del cliente.
- Tipos de productos y servicios utilizados por el cliente.

El valor de un proceso de análisis de riesgos de dos pasos se muestra en el siguiente ejemplo. Los datos recopilados en el primer paso del proceso de análisis de riesgos reflejan que un banco emite 100 transferencias de fondos internacionales por día. Si se continúa con el análisis, éste puede revelar que el 90 % de las transferencias de fondos son periódicas, están bien documentadas y son realizadas por clientes a largo plazo. Por otro lado, el análisis puede revelar que el 90 % de estas transferencias no son periódicas o son para individuos o entidades que no son clientes. A pesar de que en estos dos ejemplos las cantidades son las mismas, los riesgos generales son diferentes.

Como se mostró anteriormente, el CIP y la información de CDD del banco desempeñan papeles importantes en este proceso. Consulte las secciones del esquema general principal, “Programa de identificación de clientes” y “Debida diligencia de los clientes”, que se encuentran en las páginas 57 a 64 y 69 a 71, respectivamente, como guía adicional.

Desarrollo del programa de cumplimiento BSA/AML del banco según su análisis de riesgos

La gerencia debe estructurar el programa de cumplimiento BSA/AML del banco para tratar de manera adecuada su perfil de riesgo, según lo establece el análisis de riesgos. La gerencia debe comprender la exposición al riesgo BSA/AML del banco y desarrollar las políticas, los procedimientos y los procesos adecuados para supervisar y controlar los riesgos BSA/AML. Por ejemplo, los sistemas de supervisión del banco a cargo de la identificación, la investigación y el informe de actividades sospechosas deben constituirse en función del riesgo, concentrándose, particularmente, en los productos, los servicios, los clientes, las entidades y las ubicaciones geográficas de mayor riesgo, según lo establece el análisis de riesgos BSA/AML del banco.

Los responsables de las pruebas independientes (auditorías) deben revisar que el análisis de riesgos del banco sea razonable. Además, la gerencia debe tener en cuenta los recursos de personal y el nivel de capacitación necesarios para fomentar el cumplimiento de estas políticas, procedimientos y procesos. En aquellos bancos en los que se asume un perfil BSA/AML de mayor riesgo, la gerencia debe proporcionar un programa de cumplimiento BSA/AML más firme que supervise y revise de manera específica los riesgos mayores que la gerencia y la junta han aceptado. Consulte el Apéndice I (“Vinculación del análisis de riesgos al programa de cumplimiento BSA/AML”) donde encontrará un cuadro que describe la vinculación del análisis de riesgos al programa de cumplimiento BSA/AML.

Análisis de riesgos de cumplimiento BSA/AML consolidado

Los bancos que implementan un programa de cumplimiento BSA/AML consolidado o parcialmente consolidado deben analizar los riesgos, tanto de manera individual dentro de los rubros de la actividad comercial como en todas las actividades y entidades legales. La determinación de los riesgos BSA/AML según la consolidación en organizaciones más grandes o más complejas puede permitir a una organización identificar de manera óptima los riesgos y las exposiciones a los riesgos dentro y en todos los rubros de la actividad comercial o las categorías de productos. La información concreta también permite que la alta gerencia y la junta directiva comprendan y mitiguen de manera adecuada los riesgos en toda la organización. Para evitar no contar con información actualizada de las exposiciones a los riesgos BSA/AML, la organización bancaria debe volver a analizar continuamente los riesgos BSA/AML y comunicarse con las unidades comerciales, funciones y entidades legales. La identificación de un riesgo o deficiencia BSA/AML en un área comercial puede indicar que es posible que existan peligros en otras partes de la organización, los que la gerencia debe identificar y controlar. Consulte la sección del esquema general ampliado, “Estructuras de programas de cumplimiento BSA/AML”, en las páginas 179 a 185, como guía adicional.

Actualización del análisis de riesgos del banco

Un programa de cumplimiento BSA/AML eficaz controla los riesgos asociados con los productos, servicios, clientes, entidades y ubicaciones geográficas del banco; por lo tanto,

un análisis de riesgos eficaz debe ser un proceso continuo, no un ejercicio que deba realizarse una sola vez. La gerencia debe actualizar su análisis de riesgos para identificar los cambios en el perfil de riesgo del banco, según sea necesario (p. ej., cuando se incorporan nuevos productos y servicios, se modifican los existentes, los clientes de mayor riesgo abren o cierran cuentas o el banco se expande a través de fusiones y adquisiciones). Si no existieran tales cambios, constituye una práctica responsable para los bancos volver a analizar periódicamente sus riesgos BSA/AML al menos cada 12 a 18 meses.

Desarrollo de un análisis de riesgos BSA/AML por parte del inspector

En algunos casos, los bancos pueden no haber realizado o completado un análisis de riesgos BSA/AML idóneo y los inspectores deban realizar uno basándose en la información disponible. Cuando lo realicen, los inspectores no deben utilizar ningún formato en particular. En tales casos, los documentos deben incluir el análisis de riesgos del banco, las deficiencias observadas en el análisis de riesgos del banco y el análisis de riesgos preparado por el inspector.

Los inspectores deben asegurarse de contar con una comprensión general de los riesgos BSA/AML del banco y, como mínimo, documentar estos riesgos dentro del proceso de establecimiento del campo de aplicación de la inspección. Esta sección proporciona una guía general que los inspectores pueden utilizar cuando deban realizar un análisis de riesgos BSA/AML. Además, los inspectores pueden compartir esta información con los banqueros para que desarrollen o mejoren su propio análisis de riesgos BSA/AML.

Generalmente, el análisis de riesgos desarrollado por los inspectores no será tan exhaustivo en comparación con el desarrollado por un banco. Sin embargo, de manera similar a lo que se espera en un análisis de riesgos de un banco, los inspectores deben obtener información sobre los productos, servicios, clientes, entidades y ubicaciones geográficas del banco para determinar el volumen y las tendencias de las áreas que sean potencialmente de alto riesgo. Este proceso puede comenzar con el análisis de:

- Información del banco de datos de los informes sobre la BSA (Sistema en línea de recuperación de información de moneda y banca [Web CBRS, por sus siglas en inglés]).
- Informes y documentos de inspecciones previas.
- Respuesta a los puntos de la carta de solicitud.
- Temas tratados con la gerencia del banco y el personal de la agencia regulatoria pertinente.
- Informes de condición e ingreso (Informe financiero o *Call Report*) e Informe uniforme de desempeño bancario (UBPR, por sus siglas en inglés).

Los inspectores deben realizar este análisis controlando el nivel y la tendencia de la información concerniente a las actividades bancarias identificadas, por ejemplo:

- Transferencias de fondos.

- Banca privada.
- Ventas de instrumentos monetarios.
- Cuentas de bancos corresponsales extranjeros y PTA.
- Ubicaciones de sucursales.
- Ubicaciones geográficas nacionales e internacionales del área comercial del banco.

Esta información se debe evaluar en relación con factores como la cantidad de activos totales, el tipo de clientela, las entidades, los productos, los servicios y las ubicaciones geográficas del banco. Los inspectores deben tener precaución al comparar información entre bancos y hacer uso de su experiencia y perspectiva al realizar este análisis. Específicamente, los inspectores deben evitar comparar la cantidad de SAR presentados por un banco con aquellos presentados por otro que se encuentre en la misma ubicación geográfica. Los inspectores pueden y deben hacer uso de su conocimiento sobre los riesgos asociados con productos, servicios, clientes, entidades y ubicaciones geográficas para ayudar a determinar el perfil de riesgo BSA/AML del banco. Los inspectores pueden consultar el Apéndice J ("Cuadro de nivel de riesgos") cuando realicen esta evaluación.

Después de identificar las operaciones de mayor riesgo potenciales, los inspectores deben delinear un perfil de riesgo BSA/AML preliminar del banco. El perfil de riesgo preliminar proporcionará al inspector una base para establecer el campo de aplicación de la inspección BSA/AML inicial y la habilidad de determinar la aptitud del programa de cumplimiento BSA/AML del banco. Los bancos pueden tener un gran interés en las actividades de mayor riesgo, pero estos riesgos se deben mitigar de manera adecuada mediante un programa de cumplimiento BSA/AML eficaz adaptado a esos riesgos específicos.

El inspector debe elaborar un documento que establezca el campo de aplicación y planificación de la inspección inicial adecuado al perfil de riesgo BSA/AML preliminar. Según sea necesario, el inspector debe identificar procedimientos de inspección adicionales además de los procedimientos mínimos que se deban llevar a cabo durante la inspección. Aunque el campo de aplicación inicial puede cambiar durante la inspección, el perfil de riesgo preliminar permitirá que el inspector establezca un campo de aplicación razonable para el control BSA/AML.

Determinación del perfil de riesgo BSA/AML agregado del banco por parte del inspector

El inspector, durante la fase del "Desarrollo de conclusiones y finalización de la inspección" de la inspección BSA/AML, debe analizar si los controles del programa de cumplimiento BSA/AML del banco son adecuados para gestionar y mitigar sus riesgos BSA/AML. A través de este proceso el inspector debe determinar un perfil de riesgo agregado para el banco. En este perfil de riesgo agregado se debe tener en cuenta el análisis de riesgos desarrollado por el banco o el inspector y dicho perfil debe ser un factor en la aptitud del programa de cumplimiento BSA/AML. Los inspectores deben determinar si el programa de cumplimiento BSA/AML es idóneo para mitigar de manera

adecuada los riesgos BSA/AML, según el análisis de riesgos. La existencia del riesgo BSA/AML dentro del perfil riesgo agregado no debe criticarse, siempre y cuando el programa de cumplimiento BSA/AML del banco identifique, mida, supervise y revise de manera adecuada este riesgo como parte de una estrategia de riesgo deliberada. Cuando los riesgos no se controlen de manera adecuada, los inspectores deben comunicar a la gerencia y la junta directiva la necesidad de mitigar el riesgo BSA/AML. Los inspectores deben documentar las deficiencias según se indica en los procedimientos de inspección de la sección principal, "Desarrollo de conclusiones y finalización de la inspección", en las páginas 53 a 56.

Procedimientos de Inspección

Análisis de riesgos BSA/AML

Objetivo*:* *Evaluar el perfil de riesgo BSA/AML del banco y la aptitud del proceso de análisis de riesgos BSA/AML del banco.*

1. Revise el análisis de riesgos BSA/AML del banco. Determine si el banco ha incluido todas las áreas de riesgo, inclusive productos o servicios nuevos, o clientes, entidades y ubicaciones geográficas señalados como objetivo. Determine si el proceso del banco para revisar y actualizar periódicamente su análisis de riesgos BSA/AML es adecuado.

2. Si el banco no ha elaborado un análisis de riesgos, o si éste no es adequado, el inspector debe llevar a cabo un análisis de riesgos.

3. Los inspectores deben documentar y hablar con la gerencia sobre el perfil de riesgo BSA/AML del banco y cualquier deficiencia que hayan identificado en el proceso de análisis de riesgos BSA/AML del banco.

Programa de Cumplimiento BSA/AML: Esquema General

Objetivo*:* *Evaluar la aptitud del programa de cumplimiento BSA/AML del banco. Determinar si el banco ha desarrollado, administrado y mantenido un programa eficaz para el cumplimiento de la BSA y de todos sus reglamentos de ejecución.*

El control de las políticas, los procedimientos y los procesos escritos del banco es el primer paso para determinar la aptitud general del programa de cumplimiento BSA/AML. La realización de los procedimientos de inspección de la sección principal y, si se requiere, los de la sección ampliada es necesaria para respaldar las conclusiones generales con respecto a la aptitud del programa de cumplimiento BSA/AML. Los resultados de la inspección se deben tratar con la gerencia del banco y los resultados significativos se deben incluir en el informe de inspección o la correspondencia de supervisión.

El programa de cumplimiento BSA/AML[30] debe haberse realizado por escrito, haber sido aprobado por la junta directiva,[31] y haberse registrado en el acta de la junta. Un banco debe contar con un programa de cumplimiento BSA/AML que sea adecuado según su respectivo perfil de riesgo BSA/AML. Consulte la sección del esquema general principal, "Análisis de riesgos BSA/AML", en las páginas 23 a 33, como guía adicional en el desarrollo de un análisis de riesgos BSA/AML. Consulte el Apéndice I ("Vinculación del análisis de riesgos al programa de cumplimiento BSA/AML") donde encontrará un cuadro que describe la vinculación del análisis de riesgos al programa de cumplimiento BSA/AML. Además, el programa de cumplimiento BSA/AML debe implementarse en su totalidad y diseñarse de

[30] La Junta Directiva del Banco Central de los EE. UU. exige que las corporaciones que se rigen por la Ley de organizaciones bancarias extranjeras (*Edge Act*) y por un acuerdo con ésta y las sucursales, agencias y otras oficinas estadounidenses de bancos extranjeros supervisados por la Reserva Federal, establezcan y mantengan procedimientos diseñados de manera razonable para garantizar y supervisar el cumplimiento de la BSA y los reglamentos relacionados; consulte el Reglamento K, 12 CFR 211.5(m)(1) y 12 CFR 211.24(j)(1). Además, debido a que la BSA no se aplica a fuera del territorio, se espera que las oficinas extranjeras de bancos nacionales dispongan de políticas, procedimientos y procesos para protegerse de los riesgos del lavado de dinero y el financiamiento del terrorismo (12 CFR 208.63 y 12 CFR 326.8).

[31] La Junta de Gobernadores del Sistema de Reserva Federal., la Corporación Federal de Seguro de Depósitos y la Oficina del Interventor Monetario exigen que las sucursales, agencias y oficinas representativas estadounidenses de los bancos extranjeros que éstos supervisan y que operan en los Estados Unidos, elaboren programas de cumplimiento de la BSA por escrito que hayan sido aprobados por la junta directiva de su respectivo banco y hayan sido registrados en el acta, o bien que hayan sido aprobados por delegados que actúen bajo la autoridad expresa de la junta directiva de su respectivo banco para aprobar los programas de cumplimiento de la BSA. "Autoridad expresa" significa que la oficina central debe conocer las exigencias de su programa AML estadounidense y que debe existir alguna indicación de delegación intencionada. La exigencia del programa de cumplimiento de la BSA no debe imponer mayores responsabilidades para aquellas sucursales, agencias y oficinas representativas estadounidenses de bancos extranjeros que ya cumplían con las obligaciones existentes según la BSA (y las prácticas comerciales comunes y prevalecientes). Consulte 71 FR 13936 (20 de Marzo de 2006). Consulte la sección del esquema general ampliado, "Sucursales y oficinas en el extranjero de bancos estadounidenses", en las páginas 189 a 193, como guía.

manera razonable para cumplir con las exigencias de la BSA.[32] Los informes de políticas por sí solos no son suficientes, las prácticas deben coincidir con las políticas, los procedimientos y los procesos escritos del banco. El programa de cumplimiento BSA/AML debe hacer posible el cumplimiento de las siguientes exigencias mínimas:

- Un sistema de controles internos para garantizar el cumplimiento continúo.
- Pruebas independientes del cumplimiento BSA/AML.
- Designación de una o varias personas responsables de la gestión del cumplimiento de la BSA (funcionario de cumplimiento de la BSA).
- Capacitación del personal correspondiente.

Además, se debe incluir un CIP como parte del programa de cumplimiento BSA/AML. Consulte la sección del esquema general principal, "Programa de identificación de clientes", en las páginas 57 a 64, como guía adicional.

Controles internos

La junta directiva, que actúa mediante la alta gerencia, es la responsable final de garantizar que el banco mantenga la eficacia de la estructura de control interno de BSA/AML, incluidos el informe y la supervisión de actividades sospechosas. La junta directiva y la gerencia deben crear una cultura de cumplimiento para garantizar que el personal se adhiera voluntariamente a las políticas, los procedimientos y los procesos BSA/AML del banco. Los controles internos constituyen las políticas, los procedimientos y los procesos del banco diseñados para limitar y controlar los riesgos y lograr el cumplimiento con la BSA. El nivel de complejidad de los controles internos debe ser acorde al tamaño, la estructura, los riesgos y la complejidad del banco. Existe una mayor probabilidad de que los bancos más grandes y más complejos implementen controles internos departamentales para el cumplimiento BSA/AML. Los controles internos departamentales habitualmente se ocupan de los riesgos y las exigencias de cumplimiento que son exclusivos de un rubro de actividad comercial o departamento en particular y forman parte de un programa de cumplimiento BSA/AML exhaustivo.

Los controles internos deben:

- Identificar las operaciones bancarias (p. ej., productos, servicios, clientes, entidades y ubicaciones geográficas) que son más vulnerables al abuso por parte de lavadores de dinero y delincuentes; proporcionar actualizaciones periódicas del perfil de riesgo del banco y suministrar un programa de cumplimiento BSA/AML adaptado para gestionar riesgos.
- Informar a la junta directiva, o a un comité de dicha junta, y a la alta gerencia sobre las iniciativas de cumplimiento, las deficiencias identificadas en el cumplimiento

[32] Consulte el Apéndice R ("Guía sobre cumplimiento") para obtener información adicional.

y las medidas correctivas adoptadas, así como notificar a los directores y a la alta gerencia sobre los SAR presentados.

- Identificar a la persona o las personas responsables del cumplimiento BSA/AML.
- Asegurar la continuidad del programa a pesar de los cambios que puedan darse en la composición o estructura de la gerencia o de los empleados.
- Cumplir con todas las exigencias normativas sobre conservación y presentación de registros, cumplir con las recomendaciones para el cumplimiento BSA/AML y realizar actualizaciones oportunas en respuesta a cambios en los reglamentos.[33]
- Implementar políticas, procedimientos y procesos de CDD basados en el riesgo.
- Identificar transacciones declarables y diligenciar correctamente todos los informes requeridos, incluidos los SAR, los CTR y las exenciones a los CTR. (Los bancos deben contemplar la posibilidad de centralizar las funciones de control y presentación de informes dentro de la organización bancaria).
- Disponer controles dobles y separación de tareas en la medida que sea posible. Por ejemplo, los empleados que están encargados de completar los formularios de los informes (como los SAR, los CTR y las exenciones a los CTR) por lo general no deberían ser responsables también de la decisión de presentar los informes o conceder las exenciones.
- Proporcionar suficientes controles y sistemas para la presentación de los CTR y las exenciones a los CTR.
- Suministrar suficientes sistemas de control y supervisión para una detección e informe oportunos de cualquier actividad sospechosa.
- Brindar una adecuada supervisión de los empleados encargados de manejar transacciones en efectivo, llevar a cabo informes, conceder exenciones, supervisar actividades sospechosas o participar en cualquier otra actividad cubierta por la BSA y sus reglamentos de ejecución.
- Agregar el cumplimiento BSA a las descripciones de los cargos y a las evaluaciones de desempeño del personal del banco, según corresponda.
- Capacitar a los empleados para que sean conscientes de sus responsabilidades según los reglamentos de la BSA y las pautas de la política interna.

La lista anterior no pretende ser exhaustiva y se debe adaptar para reflejar el perfil de riesgo BSA/AML del banco. En las secciones ampliadas de este manual se incluyen guías de políticas adicionales para tratar áreas de riesgo específicas.

[33] Consulte el Apéndice P ("Exigencias respecto a la conservación de registros de la BSA") como guía.

Pruebas independientes

Las pruebas independientes (auditorías) deben ser realizadas por el departamento de auditoría interna, auditores externos, consultores u otros terceros independientes calificados. Si bien la frecuencia de las auditorías no está definida específicamente en ninguna ley, es una práctica responsable que el banco realice pruebas independientes por lo general cada 12 a 18 meses, acordes al perfil de riesgo BSA/AML del banco. Los bancos que no emplean auditores ni consultores externos o que no cuentan con departamentos de auditoría interna pueden cumplir con esta exigencia utilizando personal calificado que no esté involucrado en las funciones que están siendo analizadas. Las personas que llevan a cabo las pruebas BSA/AML deben informar directamente a la junta directiva o a un comité especialmente designado de la misma, compuesto principal o enteramente por directores externos.

Las personas encargadas de la evaluación objetiva e independiente del programa de cumplimiento BSA/AML escrito deben realizar pruebas para verificar el cumplimiento específico de la BSA, y evaluar los sistemas de información de gestión (MIS, por sus siglas en inglés) pertinentes. La auditoría debe basarse en el riesgo y evaluar la calidad de la gestión de riesgo en todas las operaciones, los departamentos y las subsidiarias del banco. Los programas de auditoría basados en el riesgo variarán según el tamaño del banco, su complejidad, el campo de aplicación de sus actividades, su perfil de riesgo, la calidad de sus funciones de control, su diversidad geográfica y el uso que hace de la tecnología. Un programa de auditoría basado en riesgo eficaz cubrirá todas las actividades del banco. La frecuencia y minuciosidad de cada actividad de auditoría variará según el análisis de riesgos de la actividad. La auditoría basada en el riesgo permite a la junta directiva y a los auditores utilizar el análisis de riesgos del banco para concentrar el campo de aplicación de la auditoría en las áreas que generan mayor preocupación. Las pruebas deben ayudar a la junta directiva y a la gerencia a identificar las áreas que presentan debilidades o las que requieren mejoras o controles más estrictos.

Las pruebas independientes deben incluir lo siguiente, como mínimo:

- Una evaluación de la aptitud general y la eficacia del programa de cumplimiento BSA/AML del banco, incluidos sus políticas, procedimientos y procesos. En general, esta evaluación incluirá una declaración explícita sobre la eficacia y la aptitud general del programa de cumplimiento BSA/AML y el cumplimiento con las exigencias normativas pertinentes. Como mínimo, la auditoría debe contener información suficiente para que el evaluador (p. ej., un inspector, un auditor de evaluación o un funcionario de la BSA) llegue a una conclusión sobre la calidad general del programa de cumplimiento BSA/AML.

- Determinar que tan razonable es el análisis de riesgos del banco, en acorde con su perfil de riesgo (productos, servicios, clientes, entidades y ubicaciones geográficas).

- Pruebas adecuadas de transacciones que se basen en el riesgo y que permitan verificar el cumplimiento del banco con los requisitos de conservación y presentación de

registros e informes de la BSA (p. ej., CIP, SAR, CTR y exenciones a los CTR, y solicitudes para compartir información).

- Una evaluación de los esfuerzos de la gerencia para lograr la eliminación de violaciones y deficiencias observadas en auditorías e inspecciones normativas previas, que incluyen avances con respecto al cumplimiento de requerimientos de supervisión que aún estén pendientes, si es pertinente.

- Un análisis de la capacitación del personal en cuanto a la adecuación, precisión e integridad de la misma.

- Una revisión de la eficacia de los sistemas de supervisión de actividades sospechosas (sistemas manuales, automatizados o una combinación de ambos) empleados para el cumplimiento BSA/AML. Los informes relacionados pueden incluir lo siguiente, sin limitarse únicamente a ello:

  - Informes de supervisión de actividades sospechosas.

  - Informes sobre acumulación de grandes volúmenes de moneda.

  - Registros de instrumentos monetarios.

  - Registros de transferencias de fondos.

  - Informes de insuficiencia de saldos (NSF, por sus siglas en inglés).

  - Informes de grandes fluctuaciones de saldo.

  - Informes de las relaciones asociadas a las cuentas.

- Un análisis del proceso general de identificación y elaboración de informes de actividades sospechosas, que incluya un control de los informes SAR presentados o elaborados, para determinar la precisión y oportunidad de los mismos y si están completos, y la eficacia de la política del banco.

- Un análisis de la integridad y la precisión de los MIS utilizados en el programa de cumplimiento BSA/AML. Los sistemas de información de gestión incluyen los informes empleados para identificar transacciones en grandes volúmenes de moneda, transacciones de moneda acumuladas diarias, transacciones de transferencias de fondos, transacciones de ventas de instrumentos monetarios, e informes analíticos y de pautas.

Los auditores deben documentar el campo de aplicación de la auditoría, los procedimientos realizados, las pruebas de transacciones realizadas y los resultados del control. Toda la documentación auditada debe ponerse a disposición del inspector para su control. Toda violación, excepción a las políticas o los procedimientos u otras deficiencias observadas durante la auditoría deben ser incluidas en un informe de auditoría e informadas a la junta directiva o un comité oportunamente designado para tal efecto. La junta directiva o el comité designado, así como el personal de auditoría, deben hacer un seguimiento de las deficiencias de la auditoría y documentar las medidas correctivas que correspondan.

Funcionario de cumplimiento de la BSA

La junta directiva del banco deberá designar a un empleado calificado como funcionario de cumplimiento de la BSA.[34]El funcionario de cumplimiento de la BSA está encargado de coordinar y supervisar el cumplimiento diario de BSA/AML. Dicho funcionario también tiene a su cargo la gestión de todo lo relativo al programa de cumplimiento BSA/AML y del cumplimiento por parte del banco de la BSA y sus reglamentos de ejecución. Sin embargo, la junta directiva es quien tiene la responsabilidad en última instancia del cumplimiento BSA/AML del banco.

Si bien el cargo de la persona responsable del cumplimiento general BSA/AML del banco no es importante, su nivel de autoridad y responsabilidad dentro del banco es fundamental. El funcionario de cumplimiento de la BSA puede delegar obligaciones BSA/AML en otros empleados, pero es responsable del cumplimiento general BSA/AML del banco. La junta directiva tiene la responsabilidad de garantizar que el funcionario de cumplimiento de la BSA cuente con la autoridad y los recursos suficientes (monetarios, físicos y de personal) para administrar un programa de cumplimiento BSA/AML eficaz conforme al perfil de riesgo del banco.

El funcionario de cumplimiento de la BSA debe conocer plenamente dicha ley y todos los reglamentos relacionados con la misma. Dicho funcionario también debe comprender los productos, los servicios, los clientes, las entidades y las ubicaciones geográficas del banco, y los riesgos potenciales de lavado de dinero y financiamiento del terrorismo que están asociados a estas actividades. No basta con nombrar un funcionario de cumplimiento de la BSA para cumplir con la exigencia normativa si dicha persona carece de la experiencia, la autoridad o el tiempo que se requieren para realizar esta tarea satisfactoriamente.

Las comunicaciones deben permitirle al funcionario de cumplimiento de la BSA informar regularmente a la junta directiva y a la alta gerencia sobre el cumplimiento existente de la BSA. Toda la información relativa a la BSA, que incluye los informes SAR presentados ante la FinCEN, debe ser presentada ante la junta directiva o un comité apropiado de ésta para que estas personas puedan tomar decisiones sobre el cumplimiento general BSA/AML. El funcionario de cumplimiento de la BSA es responsable de ejecutar las instrucciones impartidas por la junta directiva y asegurarse de que los empleados se adhieran a las políticas, los procedimientos y los procesos BSA/AML del banco.

Capacitación

Los bancos deben garantizar que el personal apropiado esté capacitado en los aspectos aplicables de la BSA. La capacitación debe incluir las exigencias normativas así como las

[34] El banco debe designar a una o más personas para coordinar y supervisar el cumplimiento diario. Esta exigencia se detalla en los reglamentos del programa de cumplimiento de la BSA de las agencias bancarias federales: 12 CFR 208.63, 12 CFR 211.5(m) y 12 CFR 211.24(j) (Junta de Gobernadores del Sistema de Reserva Federal); 12 CFR 326.8 (Corporación Federal de Seguro de Depósitos); 12 CFR 748.2 (Administración Nacional de Cooperativas de Crédito); 12 CFR 21.21 (Oficina del Interventor Monetario) y 12 CFR 563.177 (Oficina de Supervisión de Instituciones de Ahorro).

políticas, los procedimientos y los procesos BSA/AML internos del banco. Como mínimo, el programa de capacitación del banco debe suministrar capacitación a todo el personal del banco cuyas obligaciones requieran conocimiento de la BSA. La capacitación debe estar adaptada a las responsabilidades específicas de cada persona. Además, se debe brindar a todo personal nuevo un esquema general de las exigencias BSA/AML durante la orientación profesional. La capacitación debe incluir información relativa a los rubros de la actividad comercial aplicables, como servicios fiduciarios, internacionales y banca privada. El funcionario de cumplimiento de la BSA debe recibir capacitación periódica que sea relevante y adecuada a los cambios en las exigencias normativas, así como las actividades y el perfil de riesgo BSA/AML general del banco.

La junta directiva y la alta gerencia deben estar informadas de los cambios y nuevos desarrollos de la BSA, sus reglamentos e instrucciones de ejecución, y los reglamentos de las agencias bancarias federales. Si bien la junta directiva puede no requerir el mismo nivel de capacitación que el personal de operaciones del banco, es necesario que comprenda la importancia de las exigencias normativas BSA/AML, las implicaciones del incumplimiento y los riesgos que enfrenta el banco. Sin una comprensión general de la BSA, la junta directiva no podrá supervisar adecuadamente el cumplimiento BSA/AML, ni aprobar las políticas, los procedimientos y los procesos BSA/AML, o proporcionar suficientes recursos BSA/AML.

La capacitación debe ser continua e incorporar desarrollos actuales, así como cambios introducidos en la BSA y todo reglamento relacionado. Los cambios efectuados en las políticas, los procedimientos, los procesos y los sistemas de supervisión internos también deben ser cubiertos en la capacitación. El programa de capacitación debe reforzar la importancia que le otorgan la junta directiva y la alta gerencia al cumplimiento del banco con la BSA y garantizar que todos los empleados comprendan el papel que desempeñan en el mantenimiento de un programa de cumplimiento BSA/AML eficaz.

Los ejemplos de las actividades de lavado de dinero, supervisión e informes sobre actividades sospechosas pueden y deben adaptarse a la medida de cada auditorio particular. Por ejemplo, la capacitación dirigida a los cajeros debe enfocarse en ejemplos que involucren transacciones de grandes volúmenes de moneda u otras actividades sospechosas; la capacitación dirigida al departamento de préstamos debe dar ejemplos relacionados con el lavado de dinero a través de distintos tipos de préstamos.

Los bancos deben documentar sus programas de capacitación. El banco debe conservar y poner a disposición del inspector el material utilizado en las capacitaciones y en las pruebas, las fechas de las clases de capacitación y la asistencia a las mismas.

Procedimientos de Inspección

Programa de cumplimiento de BSA/AML

Objetivo*:* *Evaluar la aptitud del programa de cumplimiento BSA/AML del banco. Determinar si el banco ha desarrollado, administrado y mantenido un programa eficaz para el cumplimiento de la BSA y de todos sus reglamentos de ejecución.*

1. Revise el programa de cumplimiento BSA/AML escrito del banco [35] aprobado por la junta directiva [36] para garantizar que contiene los siguientes elementos requeridos:

   - Un sistema de controles internos para garantizar el cumplimiento continuo.
   - Pruebas independientes del cumplimiento de la BSA.
   - Una persona o personas específicamente designadas como responsables de gestionar el cumplimiento de la BSA (funcionario de cumplimiento de la BSA).
   - Capacitación del personal correspondiente.

   Un banco debe contar con un programa de cumplimiento BSA/AML que sea adecuado según su respectivo perfil de riesgo BSA/AML. Además, se debe incluir un CIP como parte del programa de cumplimiento BSA/AML.

2. Analice si la junta directiva y la alta gerencia reciben informes idóneos del cumplimiento BSA/AML.

---

[35] La Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos y la Oficina del Interventor Monetario exigen que las sucursales, agencias y oficinas representativas estadounidenses de bancos extranjeros que supervisen y que operen en los Estados Unidos, desarrollen programas de cumplimiento de la BSA por escrito que hayan sido aprobados por la junta directiva de su respectivo banco y hayan sido registrados en el acta, o bien que hayan sido aprobados por delegados que actúen bajo la autoridad expresa de la junta directiva de su respectivo banco para aprobar los programas de cumplimiento de la BSA. "Autoridad expresa" significa que la oficina central debe conocer las exigencias de su programa AML estadounidense y que debe existir alguna indicación de delegación intencionada. La exigencia del programa de cumplimiento de la BSA no debe imponer mayores responsabilidades para aquellas sucursales, agencias y oficinas representativas estadounidenses de bancos extranjeros que ya cumplían con las obligaciones existentes según la BSA (y las prácticas comerciales comunes y prevalecientes). Consulte 71 FR 13936 (20 de Marzo de 2006). Consulte la sección del esquema general ampliado, "Sucursales y oficinas en el extranjero de bancos estadounidenses", en las páginas 189 a 193, como guía.

[36] La Junta Directiva del Banco Central de los EE. UU. exige que las corporaciones que se rigen por la Ley de organizaciones bancarias extranjeras (Edge Act) y por un acuerdo con ésta y las sucursales, agencias y otras oficinas estadounidenses de bancos extranjeros supervisados por la Reserva Federal, establezcan y mantengan procedimientos diseñados de manera razonable para garantizar y supervisar el cumplimiento de la BSA y los reglamentos relacionados; consulte el Reglamento K, 12 CFR 211.5(m)(1) y 12 CFR 211.24(j)(1). Además, debido a que la BSA no se aplica fuera del territorio, se espera que las oficinas extranjeras de bancos nacionales dispongan de políticas, procedimientos y procesos para protegerse del lavado de dinero y el financiamiento del terrorismo (12 CFR 211.24(j)(1) y 12 CFR 326.8).

Vinculación del análisis de riesgos al programa de cumplimiento BSA/AML

3. En función de los procedimientos de inspección realizados en el proceso de establecimiento del campo de aplicación y planificación, que incluyen el control del análisis de riesgos, determine si el banco ha identificado adecuadamente el riesgo existente dentro de sus operaciones bancarias (productos, servicios, clientes, entidades y ubicaciones geográficas) y lo ha incorporado al programa de cumplimiento BSA/AML. Consulte el Apéndice I ("Vinculación del análisis de riesgos al programa de cumplimiento BSA/AML") cuando realice este análisis.

Controles internos

4. Determine si el programa de cumplimiento BSA/AML incluye políticas, procedimientos y procesos que:

   - Identifiquen las operaciones bancarias de mayor riesgo (productos, servicios, clientes, entidades y ubicaciones geográficas); proporcionen actualizaciones periódicas del perfil de riesgo del banco y suministren un programa de cumplimiento BSA/AML adaptado para gestionar riesgos.
   - Informen a la junta directiva, o a un comité de dicha junta, y a la alta gerencia sobre las iniciativas de cumplimiento, las deficiencias identificadas en el cumplimiento, los SAR presentados y las medidas correctivas adoptadas.
   - Identifiquen a la persona o las personas responsables del cumplimiento BSA/AML.
   - Aseguren la continuidad del programa a pesar de los cambios que puedan darse en la composición o estructura de la gerencia o de los empleados.
   - Cumplan con todas las exigencias normativas y recomendaciones para el cumplimiento BSA/AML y estipulen actualizaciones oportunas para implementar los cambios en los reglamentos.
   - Implementen políticas, procedimientos y procesos de CDD basados en el riesgo.
   - Identifiquen transacciones declarables y diligencien correctamente todos los informes requeridos, incluidos los SAR, los CTR y las exenciones a los CTR. (Los bancos deben contemplar la posibilidad de centralizar las funciones de control y presentación de informes dentro de la organización bancaria).
   - Dispongan controles dobles y separación de tareas en la medida que sea posible. Por ejemplo, los empleados que están encargados de completar los formularios de los informes (como los SAR, los CTR y las exenciones a los CTR) por lo general no deberían ser responsables también de la decisión de presentar los informes o conceder las exenciones.

- Proporcionen suficientes sistemas de control y supervisión para una detección e informe oportunos de cualquier actividad sospechosa.
- Brinden una adecuada supervisión de los empleados encargados de manejar transacciones en efectivo, llevar a cabo informes, conceder exenciones, supervisar actividades sospechosas o participar en cualquier otra actividad cubierta por la BSA y sus reglamentos de ejecución.
- Capaciten a los empleados para que sean conscientes de sus responsabilidades según los reglamentos de la BSA y las pautas de la política interna.
- Agreguen el cumplimiento de la BSA a las descripciones de los cargos y a las evaluaciones de desempeño del personal correspondiente.

Pruebas independientes

5. Determine si la prueba (auditoría) BSA/AML es independiente (es decir, si la realiza una persona [o personas] que no está involucrada con el personal de cumplimiento BSA/AML del banco) y si las personas que llevan a cabo las pruebas dependen directamente de la junta directiva o de un comité designado compuesto principal o íntegramente por directores externos.
6. Evalúe las competencias de la persona o las personas que realizan las pruebas independientes para analizar si el banco puede confiar en los resultados y las conclusiones.
7. Valide los informes y documentos del auditor para determinar si las pruebas independientes del banco son exhaustivas, precisas, idóneas y oportunas. La prueba independiente debe centrarse en lo siguiente:
   - La aptitud general y la eficacia del programa de cumplimiento BSA/AML, incluidos procedimientos, políticas y procesos. En general, esta evaluación incluirá una declaración explícita sobre la eficacia y la aptitud general del programa de cumplimiento BSA/AML y el cumplimiento con las exigencias normativas pertinentes. Como mínimo, la auditoría debe contener información suficiente para que el evaluador (p. ej., un inspector, un auditor de evaluación o un funcionario de la BSA) llegue a una conclusión sobre la calidad general del programa de cumplimiento BSA/AML.
   - El análisis de riesgos BSA/AML.
   - Las exigencias con respecto a la conservación y presentación de informes de la BSA.
   - La implementación del CIP.
   - Las políticas, los procedimientos y los procesos de CDD y el cumplimiento con las exigencias internas.
   - La adhesión del personal a las políticas, los procedimientos y los procesos BSA/AML del banco.

- Las pruebas de transacciones adecuadas, que pongan particular atención en las operaciones de mayor riesgo (productos, servicios, clientes y ubicaciones geográficas).
- La capacitación, que incluye su extensión, precisión de materiales, cronograma de capacitación y seguimiento de asistencia.
- La integridad y la precisión del informe de MIS utilizado en el programa de cumplimiento BSA/AML. Los sistemas de información de gestión incluyen los informes empleados para identificar transacciones en grandes volúmenes de moneda, transacciones de moneda acumuladas diarias, transacciones de transferencias de fondos, transacciones de ventas de instrumentos monetarios, e informes analíticos y de pautas.
- El seguimiento de las deficiencias y los problemas identificados anteriormente y la verificación de que la gerencia los haya corregido.
- Si no se utiliza un sistema automatizado para identificar o acumular transacciones de grandes volúmenes, determine si la auditoría o el control independientes incluye una muestra de verificación de los comprobantes de dinero en efectivo del cajero, grabación en cinta u otra documentación para establecer si dichas transacciones están identificadas e informadas adecuadamente.

8. Determine si el control de los sistemas de supervisión de actividades sospechosas de la auditoría incluye una evaluación de la capacidad del sistema para identificar actividades no habituales. Garantice a través de la validación de los informes y documentos del auditor que las pruebas independientes del banco:
   - Controlan políticas, procedimientos y procesos para la supervisión de actividades sospechosas.
   - Evalúan la metodología del sistema para establecer y aplicar actividades previstas o criterios de filtrado.
   - Evalúan la capacidad del sistema para generar informes de supervisión.
   - Determinan si los criterios de filtrado del sistema son razonables e incluyen, como mínimo, efectivo, instrumentos monetarios, transferencias de fondos y otros productos, servicios, clientes o ubicaciones geográficas de mayor riesgo, según corresponda.
9. Compruebe si el control de los sistemas de supervisión de actividades sospechosas de la auditoría incluye una evaluación de la investigación y la remisión de actividades poco habituales. Garantice a través de una validación de los informes y documentos del auditor que las pruebas independientes del banco incluyen un control de políticas, procedimientos y procesos para la remisión de actividades poco habituales de todos los rubros de la actividad comercial (p. ej., legales, banca privada, bancos corresponsales extranjeros) al personal o el departamento responsables de evaluar dichas actividades.

10. Revise el campo de aplicación, los procedimientos y los documentos de la auditoría para determinar la aptitud de la misma, de acuerdo con lo siguiente:

    - Cobertura y frecuencia de la auditoría general en relación con el perfil de riesgo del banco.
    - Informe y supervisión de la junta directiva de los resultados de la auditoría y su respuesta a estos resultados.
    - Aptitud de las pruebas de transacciones, particularmente de las operaciones bancarias de mayor riesgo y los sistemas de supervisión de actividades sospechosas.
    - Competencia de los auditores o inspectores independientes respecto a las exigencias BSA/AML.

Funcionario de cumplimiento de la BSA

11. Determine si la junta directiva ha designado a una persona o personas responsables del programa de cumplimiento BSA/AML general. Determine si el funcionario de cumplimiento de la BSA tiene la autoridad y los recursos suficientes para cumplir con todas las obligaciones de manera eficaz.

12. Analice la pericia del funcionario de cumplimiento de la BSA y su personal, según sea necesario. Determine si el área de cumplimiento de la BSA cuenta con el personal suficiente para el nivel de riesgo general del banco (según productos, servicios, clientes, entidades y ubicaciones geográficas), el tamaño y las necesidades de cumplimiento BSA/AML. Además, garantice que no exista conflicto de intereses y que el personal cuente con el tiempo suficiente para cumplir con todas las obligaciones.

Capacitación

13. Determine si los siguientes elementos están tratados adecuadamente en el programa y los materiales de capacitación:

    - La importancia que le otorgan la junta directiva y la alta gerencia a la educación, la capacitación y el cumplimiento continuos.
    - La responsabilidad de los empleados de garantizar el cumplimiento de la BSA.
    - La extensión de la capacitación, considerando los riesgos específicos de los rubros de la actividad comercial individuales.
    - La capacitación del personal de todas las áreas aplicables del banco.[37]
    - La frecuencia de las capacitaciones.

[37] Como parte de este elemento, determine si el banco realiza capacitaciones adecuadas para todo agente responsable de elaborar CIP u otras funciones relacionadas con la BSA en nombre del banco.

- La documentación de los registros de asistencia y los materiales de capacitación.
- La cobertura de las políticas, los procedimientos, y los procesos del banco, así como de las reglas y los reglamentos nuevos.
- La cobertura de las diferentes formas de lavado de dinero y financiamiento del terrorismo en lo que se relaciona con la identificación y los ejemplos de actividad sospechosa.
- Las sanciones por incumplimiento de las políticas internas y las exigencias normativas.

Pruebas de transacciones

Las pruebas de transacciones deben incluir, como mínimo, los procedimientos de inspección detallados más adelante (pruebas independientes) o los procedimientos de las pruebas de transacciones seleccionados de las secciones principales o ampliadas. Si bien se requieren algunas pruebas de transacciones, los inspectores pueden decidir a discreción qué tipo de pruebas se deben realizar. Los inspectores deben documentar sus decisiones respecto al grado de las pruebas de transacciones que realicen, las actividades sobre las que serán llevadas a cabo, así como los motivos de cualquier cambio en el campo de aplicación de las pruebas de transacciones que ocurra durante la inspección. Al determinar cómo proceder respecto a las pruebas de transacción, los inspectores deben considerar lo siguiente:

- Las cuentas o los clientes identificados en el control de la información obtenida de las descargas de las bases de datos de informes sobre la BSA.
- Los productos, los servicios, los clientes, las entidades y las ubicaciones geográficas de mayor riesgo según el proceso de establecimiento del campo de aplicación y planificación para los que el banco puede no tener controles internos adecuados.
- Nuevos productos, servicios, clientes, entidades y ubicaciones geográficas que se presentan en la cartera del banco desde la inspección de BSA/AML anterior.

Pruebas independientes

14. Seleccione una muestra evaluativa que incluya transacciones diferentes a aquellas probadas por el auditor independiente y determine si la prueba independiente:
    - Es exhaustiva, adecuada y oportuna.
    - Ha controlado la precisión del informe de MIS utilizado en el programa de cumplimiento BSA/AML.
    - Ha controlado los sistemas de supervisión de actividades sospechosas para incluir la identificación de la actividad poco común.
    - Ha controlado si los sistemas de supervisión de actividades sospechosas incluyen la investigación y la remisión de actividades poco comunes.

Evaluación preliminar

Luego de que el inspector haya llevado a cabo la revision de los cuatro elementos exigidos por el programa de cumplimiento BSA/AML del banco, debe documentar una evaluación preliminar del programa del banco. En ese momento, el inspector debe tratar nuevamente el plan inicial de inspección, para determinar si se identifican fortalezas o debilidades durante el control del programa de cumplimiento BSA/AML de la institución que requieran correcciones en el campo de aplicación inicial planificado. El inspector debe realizar los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, páginas 176 a 178. Asimismo, debe documentar y respaldar todo cambio en el campo de aplicación de la inspección, luego continuar con los procedimientos de inspección de la sección principal y, si se requiere, los de la sección ampliada. Si no hay cambios en la inspección del campo de aplicación, el inspector debe continuar con los procedimientos de inspección de la sección principal, “Desarrollo de conclusiones y finalización de la inspección”, en las páginas 53 a 56.

Desarrollo de Conclusiones y Finalización de la Inspección: Esquema General

Objetivo*: Formular conclusiones, comunicar los resultados a la gerencia, preparar comentarios sobre el informe, dar una respuesta de supervisión adecuada y concluir la inspección.*

En la fase final de la inspección BSA/AML, el inspector debe agrupar todos los resultados de los procedimientos de inspección realizados. A partir de estos resultados, debe sacar conclusiones sobre la aptitud del programa de cumplimiento BSA/AML, documentarlas, analizar las conclusiones preliminares con la gerencia del banco, presentar estas conclusiones por escrito para incluirlas en el informe de inspección (ROE, por sus siglas en inglés) y, por último, determinar y documentar cuál es la respuesta reglamentaria apropiada, en caso de existir alguna.

En algunos casos, la respuesta reglamentaria adecuada incluirá la citación de una violación penal. La citación de violaciones de la ley y los reglamentos se realiza, generalmente, en el contexto de las actividades de supervisión. La medida en que las violaciones afectan la inspección del programa de cumplimiento BSA/AML de un banco se basa en la naturaleza, la duración y la gravedad del incumplimiento. En algunos casos, una agencia puede permitir al banco subsanar la violación como parte del proceso de supervisión. Sin embargo, en las circunstancias adecuadas, una agencia puede tomar medidas de cumplimiento formales o informales para abordar las violaciones de las exigencias de la BSA.[38]

Violaciones sistemáticas o recurrentes

Las violaciones sistemáticas o recurrentes de la BSA y sus reglamentos de ejecución implican una cantidad considerable de deficiencias o el hecho repetido de no registrar ni presentar de manera eficaz y precisa la información requerida según la BSA, en caso de que los errores o la falta de información perjudiquen la integridad del registro o informe, no representen adecuadamente las transacciones que se deben informar o afecten la eficacia de los procesos de control e informe de actividades sospechosas del banco. Las violaciones sistemáticas son el resultado de controles o sistemas ineficaces para obtener, analizar y mantener la información requerida, o para informar sobre clientes, cuentas o transacciones, según se requiere en varias cláusulas de la BSA. Las violaciones recurrentes son apariciones repetitivas de los mismos problemas o de problemas similares. A diferencia de los problemas aislados o accidentales, los problemas sistemáticos o recurrentes demuestran un patrón o una práctica de incumplimiento con la BSA y sus reglamentos de ejecución.

[38] El Informe entre Agencias sobre el Cumplimiento (consulte el Apéndice R) explica las bases del cumplimiento de las agencias bancarias federales con las exigencias AML específicas de la BSA.

Al evaluar si las violaciones representan un patrón o una práctica, los inspectores deben analizar los hechos y las circunstancias pertinentes. En general, las prácticas repetidas, regulares, habituales o institucionalizadas constituirán un patrón o una práctica. Cuando se evalúa si existe un patrón o una práctica, se debe considerar la totalidad de las circunstancias.

Las consideraciones para determinar si existe un patrón o una práctica incluyen, entre otras:

- Si el número de violaciones es alto en comparación con la actividad total del banco. En general, esta evaluación se determina a través de un muestreo de transacciones o registros. Según este proceso, las determinaciones se realizan en relación con el nivel general de incumplimiento. Sin embargo, incluso si son pocas en cantidad, las violaciones pueden reflejar un incumplimiento sistemático, según sea la gravedad (p. ej., considerables o flagrantes).

- Si existe evidencia de violaciones similares por parte del banco en una serie de transacciones o en diferentes divisiones o departamentos. Esto no es un cálculo exacto y los inspectores deben considerar la cantidad, la importancia y la frecuencia de las violaciones identificadas en la organización. Las violaciones identificadas en diversas divisiones o departamentos pueden indicar o no una violación sistemática. Estas violaciones se deben evaluar en un contexto más amplio para determinar si existen problemas en la capacitación u otras debilidades del sistema en cuanto al cumplimiento.

- La relación entre las violaciones (p. ej., si todas ocurrieron en la misma área del banco, línea de productos, sucursal o departamento, o con un empleado en particular).

- El efecto que tienen las violaciones en las capacidades de control e informe de actividades sospechosas del banco.

- Si las violaciones parecen estar basadas en una política escrita o no escrita o en un procedimiento establecido, o surgen por la falta de un procedimiento establecido.

- Si existe una fuente o causa común de las violaciones.

- Si las violaciones fueron el resultado de un problema de software aislado en un producto de software de informe de BSA/AML y si el banco ha tomado las medidas adecuadas para abordar el problema.

Las violaciones sistemáticas o recurrentes de la BSA pueden tener un efecto considerable en la idoniedad del programa de cumplimiento BSA/AML del banco. Cuando se identifican casos sistemáticos de incumplimiento, el inspector debe tener en cuenta el incumplimiento en el contexto del programa general (controles internos, capacitación, pruebas independientes, persona responsable, etc.) y consultar el Informe entre Agencias sobre el Cumplimiento (vea el Apéndice R) para determinar si el programa de cumplimiento BSA/AML es insuficiente como resultado del incumplimiento sistemático. Todas las violaciones sistemáticas se deben señalar a la gerencia y a la junta directiva del banco, y deben documentarse en el informe de inspección o la correspondencia de supervisión.

Los tipos de violaciones sistemáticas o recurrentes pueden incluir, entre otros:

- Falta de establecimiento de un programa de debida diligencia que incluya un enfoque en función del riesgo y, si fuera necesario, políticas, procedimientos y controles mejorados en relación con las cuentas corresponsales extranjeras.
- Falta de aplicación de un programa de debida diligencia diseñado razonablemente para las cuentas bancarias privadas de ciudadanos no estadounidenses (según se define en 31 CFR 103.175).
- Presentación con demora frecuente, constante o recurrente de los CTR o SAR.
- Cantidad considerable de CTR o SAR con errores u omisiones de elementos de datos.
- Falta constante de obtención o verificación de la información requerida de identificación de clientes en el momento de apertura de cuentas.
- Falta constante de realización de búsquedas en solicitudes de información según la sección 314(a).
- Falta constante de mantenimiento o conservación de los registros requeridos por la BSA.

Además, el Informe entre Agencias sobre el Cumplimiento indica que "las agencias citarán una violación de los reglamentos del SAR y tomarán las medidas de supervisión adecuadas, si el hecho de que una organización no presente los SAR evidencia un mal funcionamiento sistemático en sus políticas, procedimientos o procesos para identificar e investigar actividades sospechosas, implica un patrón o una práctica de incumplimiento con la exigencia de presentación o representa una situación considerable o flagrante".[39]

Violaciones aisladas o técnicas

Las violaciones aisladas o técnicas son casos limitados de incumplimiento con la BSA que ocurren dentro de un sistema de políticas, procedimientos y procesos que, por lo demás, es apropiado. En general, estas violaciones no constituyen una gran preocupación normativa ni se reflejan de manera negativa en la supervisión o el compromiso de la gerencia con el cumplimiento BSA, a menos que la violación aislada represente una situación considerable o flagrante, o esté acompañada por evidencia de mala fe. Si existen varias violaciones aisladas en los departamentos o las divisiones de un banco, esto puede indicar debilidades del sistema o violaciones sistemáticas o recurrentes.

Habitualmente, la gerencia del banco toma medidas correctivas en relación con las violaciones aisladas durante el curso normal del funcionamiento comercial. Todas las violaciones, independientemente del tipo o la importancia, se deben señalar a la gerencia del banco y se deben documentar de manera adecuada.

[39] Informe entre Agencias sobre el Cumplimiento, página R-6.

Los tipos de violaciones aisladas o técnicas pueden incluir, entre otras:

- Falta de presentación o presentación tardía de los CTR, situación poco frecuente, inconstante y no recurrente.
- Falta de obtención de información completa de identificación del cliente en una transacción de ventas de instrumentos monetarios, situación aislada y poco frecuente.
- Información incompleta o incorrecta, situación poco frecuente, inconstante o no recurrente en los campos de datos de los SAR.
- Falta de obtención o verificación de la información requerida de identificación del cliente, situación poco frecuente, inconstante o no recurrente.
- Falta de realización de una solicitud de información según la sección 314(a), situación accidental o no recurrente.

Cuando realice la conclusión por escrito, el inspector no necesita tratar cada procedimiento realizado durante la inspección. Durante el tratamiento con la gerencia de los temas relacionados con las conclusiones de la inspección, los inspectores deben dialogar también sobre las virtudes y las debilidades del cumplimiento BSA/AML del banco. Los inspectores deben documentar todas las determinaciones y conclusiones pertinentes.

Procedimientos de Inspección

Desarrollo de conclusiones y finalización de la inspección

Objetivo*:* *Formular conclusiones, comunicar los resultados a la gerencia, preparar comentarios sobre el informe, dar una respuesta de supervisión adecuada y concluir la inspección.*

Formulación de conclusiones

1. Recopile todos los resultados pertinentes de los procedimientos de inspección BSA/AML realizados. Evalúe la exhaustividad y fiabilidad de cualquier análisis de riesgos realizado por el banco. Llegue a una conclusión preliminar en relación con el cumplimiento de las siguientes exigencias:

   - Se supervisa de manera eficaz el programa de cumplimiento BSA/AML con respecto al perfil de riesgo del banco, según lo determinado por el análisis de riesgos. El inspector debe cerciorarse de que el programa de cumplimiento BSA/AML sea eficaz y mitigue el riesgo general del banco.
   - La junta directiva y la alta gerencia tienen conocimiento de las exigencias normativas BSA/AML, supervisan de manera eficaz el programa de cumplimiento BSA/AML y se comprometen, según sea necesario, a tomar medidas correctivas (p. ej., auditorías e inspecciones regulatorias).
   - Las políticas, los procedimientos y los procesos BSA/AML son adecuados para garantizar el cumplimiento de la normativa vigente y tratar de manera adecuada las operaciones de mayor riesgo (productos, servicios, clientes, entidades y ubicaciones geográficas).
   - Los controles internos garantizan el cumplimiento de la BSA y proporcionan una gestión de riesgos suficiente, especialmente en las operaciones de mayor riesgo (productos, servicios, clientes, entidades y ubicaciones geográficas).
   - Las pruebas independientes (auditorías) son adecuadas y prueban de manera apropiada el cumplimiento con las leyes, reglamentos y políticas. La cobertura y la frecuencia de la auditoría general son apropiadas en relación con el perfil de riesgo del banco. Las pruebas de transacciones son adecuadas, particularmente de las operaciones bancarias de mayor riesgo y los sistemas de supervisión de actividades sospechosas.
   - El responsable designado para coordinar y supervisar el cumplimiento diario es competente y cuenta con los recursos necesarios.
   - El personal está lo suficientemente capacitado para cumplir con las exigencias legales, regulatorias y de las políticas.

- Las políticas, los procedimientos y los procesos de información y comunicación son adecuados y exactos.

Todas las determinaciones relevantes se deben documentar y explicar.

Determinación de la causa subyacente

2. Si se las identifica, determine la causa subyacente a las deficiencias de las políticas, los procedimientos y los procesos. Estas deficiencias pueden ser el resultado de una cantidad de factores, incluidos, entre otros, los siguientes:

   - La gerencia no ha analizado, o no ha analizado de manera adecuada, los riesgos BSA/AML del banco.
   - La gerencia no tiene conocimiento de los asuntos relevantes.
   - La gerencia se rehusa a crear o mejorar las políticas, los procedimientos y los procesos.
   - La gerencia o los empleados hacen caso omiso de las políticas, los procedimientos y los procesos establecidos.
   - La gerencia o los empleados no tienen conocimiento o entienden erróneamente las exigencias normativas, las políticas, los procedimientos o los procesos.
   - Las operaciones de mayor riesgo (productos, servicios, clientes, entidades y ubicaciones geográficas) se han incrementado más rápidamente que las capacidades del programa de cumplimiento BSA/AML.
   - Las modificaciones en las políticas, los procedimientos y los procesos internos se comunican de manera deficiente.

3. Determine si las deficiencias o violaciones fueron identificadas previamente por la gerencia o durante una auditoría o si se identificaron sólo como resultado de esta inspección.

Debate sobre los resultados con el inspector a cargo e identificación de las medidas necesarias

4. Trate los resultados preliminares con el inspector a cargo (EIC) o el inspector responsable de controlar el cumplimiento BSA/AML general del banco. Registre los documentos de manera adecuada con la siguiente información:

   - Una conclusión sobre la aptitud del programa de cumplimiento BSA/AML y respecto a si cumple con todas las exigencias normativas al proporcionar lo siguiente:
     - Un sistema de controles internos.
     - Pruebas independientes del cumplimiento.
     - Una persona específica que coordine y supervise el programa

de cumplimiento BSA/AML.

- Capacitación del personal adecuado.

- Una conclusión con respecto al programa CIP describiendo su adequacion deacuerdo al tamaño, la ubicación y el tipo de actividad comercial del banco.
- Todas las violaciones identificadas y una evaluación de la gravedad de dichas violaciones.
- Identificación de las medidas necesarias para corregir deficiencias o violaciones y, según sea pertinente, la posibilidad, entre otras cosas, de exigir al banco que lleve a cabo análisis de riesgos más detallados o tome medidas coercitivas de cumplimiento formales.
- Recomendaciones de medidas de supervisión, según sea necesario. Además, consulte con la gerencia de supervisión de la agencia y el personal legal de la agencia, según sea necesario.
- Una valoración adecuada basada en las conclusiones y los resultados generales.
- Resultados que se hayan tratado o que se tratarán con la gerencia del banco y, si corresponde, compromisos del banco para hacer mejoras o tomar medidas correctivas.

Preparación de los comentarios BSA/AML del informe de inspección

5. Documente su conclusión sobre la aptitud del programa de cumplimiento BSA/AML del banco. Analice la eficacia de cada uno de los elementos del programa de cumplimiento BSA/AML del banco. Indique si el programa de cumplimiento BSA/AML cumple con todas las exigencias normativas al proveer lo siguiente:

   - Un sistema de controles internos.
   - Pruebas independientes del cumplimiento.
   - Una persona específica que coordine y supervise el programa de cumplimiento BSA/AML.
   - Capacitación del personal adecuado.

   El programa de cumplimiento BSA/AML también debe incluir un Programa de identificación de clientes (CIP) escrito adecuado según el tamaño, la ubicación y el tipo de actividad comercial del banco.

   No es necesario que el inspector proporcione un comentario por escrito sobre cada uno de los siguientes puntos 6 a 13. Los comentarios por escrito deben abarcar sólo las áreas o temas correspondientes a los resultados y conclusiones del inspector. Todos los resultados significativos se deben incluir en el ROE. El inspector debe garantizar que los documentos sean lo suficientemente detallados como para respaldar

los asuntos tratados en el ROE. En la medida que los siguientes puntos se tratan en los documentos, pero no en el ROE, el inspector debe garantizar que los documentos registren exhaustiva y adecuadamente cada control, como también cualquier otro aspecto del programa de cumplimiento BSA/AML del banco que amerite atención, pero que no tenga el nivel de importancia necesario como para incluirse en el ROE. El inspector debe organizar y relacionar documentos, y documentar conclusiones e información de respaldo en las bases de datos internas, según el caso. Según corresponda, el inspector debe organizar un debate sobre los siguientes puntos.

6. Describa si las políticas y los procedimientos del banco para las solicitudes de las autoridades de aplicación de la ley sobre información según la sección 314(a) de la Ley PATRIOTA de los EE. UU. (31 CFR 103.100) cumplen con las exigencias normativas.

7. Si el banco mantiene cualquier cuenta en bancos privados o corresponsales extranjeros de ciudadanos no estadounidenses, describa si las políticas, los procedimientos y los procesos de debida diligencia del banco cumplen con las exigencias normativas bajo la sección 312 de la Ley PATRIOTA de los EE. UU. (31 CFR 103.176 y 103.178).

8. Describa el compromiso de la junta directiva y la alta gerencia con respecto al cumplimiento BSA/AML. Analice si la gerencia cuenta con lo siguiente:

   - Un programa de cumplimiento BSA/AML firme respaldado en su totalidad por la junta directiva.

   - Una exigencia que requiera que la junta directiva y la alta gerencia estén informadas de las iniciativas para el cumplimiento BSA/AML, los informes de auditoría, cualquier falta de cumplimiento y el estado de las medidas correctivas.

9. Describa si las políticas, los procedimientos y los procesos del banco para la presentación del SAR cumplen con las exigencias normativas y son eficaces.

10. Describa si las políticas, los procedimientos y los procesos del banco para las transacciones de grandes volúmenes de dinero cumplen con las exigencias de 31 CFR 103.22 y son eficaces.

11. Si procede, describa si las políticas, los procedimientos y los procesos del banco para las exenciones al CTR cumplen con las exigencias normativas de realización de informes, conceden exenciones de manera adecuada y hacen uso de los formularios correctos.

12. Describa si las políticas, los procedimientos y los procesos del banco sobre transferencia de fondos cumplen con las exigencias de 31 CFR 103.33(e) y (g). Discuta brevemente si las políticas, los procedimientos y los procesos incluyen controles internos eficaces (p. ej., división de responsabilidades, debida autorización para enviar y recibir, y asiento en cuentas) y proporcionan un medio para supervisar las transferencias a los efectos del informe del CTR.

13. Describa las políticas, los procedimientos y los procesos del banco para la conservación de registros. Indique si cumplen las exigencias de 31 CFR 103..

ESQUEMA GENERAL PRINCIPAL Y PROCEDIMIENTOS DE INSPECCIÓN DE LAS EXIGENCIAS NORMATIVAS Y TEMAS RELACIONADOS

Programa de Identificación de Clientes: Esquema General

Objetivo*: Evaluar el cumplimiento del banco con las exigencias normativas y legales para el Programa de identificación de clientes (CIP).*

Todos los bancos deben contar con un CIP escrito.[40] La reglamentación del CIP implementa la sección 326 de la Ley PATRIOTA de los EE. UU. y exige que cada banco implemente un CIP escrito adaptado según su tamaño y tipo de actividad comercial, y que incluya ciertas exigencias mínimas. El CIP debe incorporarse al programa de cumplimiento BSA/AML del banco, que está sujeto a la aprobación de la junta directiva del banco.[41] La implementación de un CIP por parte de las subsidiarias de los bancos es adecuada por cuestiones de seguridad, solidez y protección contra los riesgos que puedan afectar la reputación de la institución. Las subsidiarias nacionales de los bancos (que no sean las reguladas funcionalmente y que estén sujetas a otras reglamentaciones del CIP) deben cumplir con la reglamentación del CIP que se aplica a la casa matriz al abrir una cuenta según la definición dada por 31 CFR 103.121.[42]

El objetivo del CIP consiste en permitirle al banco creer razonablemente que conoce la verdadera identidad de cada uno de sus clientes. El CIP debe incluir los procedimientos de apertura de cuentas que especifiquen la información de identificación que se debe obtener de cada cliente. También debe incluir procedimientos prácticos y razonables en función del riesgo para verificar la identidad de cada cliente. Los bancos deben llevar a

[40] Consulte 12 CFR 208.63(b), 211.5(m), 211.24(j) (Junta de Gobernadores del Sistema de Reserva Federal.); 12 CFR 326.8(b) (Corporación Federal de Seguro de Depósitos); 12 CFR 748.2(b) (Administración Nacional de Cooperativas de Crédito); 12 CFR 21.21 (Oficina del Interventor Monetario); 12 CFR 563.177(b) (Oficina de Supervisión de Instituciones de Ahorro); y 31 CFR 103.121 (FinCEN).

[41] Desde la fecha de publicación de este manual, los bancos privados no regulados por agencias federales, las instituciones fiduciarias y las cooperativas de crédito no cuentan con exigencias del programa de cumplimiento BSA/AML; no obstante, la junta del banco debe igualmente aprobar el CIP.

[42] *Frequently Asked Questions Related to Customer Identification Program Rules* (Preguntas frecuentes relacionadas con las reglamentaciones del Programa de identificación de clientes) publicadas el 28 de Abril de 2005 por la FinCEN, la Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Administración Nacional de Cooperativas de Crédito, la Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro.

cabo un análisis de riesgos de su propia base de clientes y ofertas de productos, y al determinar los riesgos, tener en cuenta:

- Los tipos de cuentas que el banco ofrece.
- Los métodos de apertura de cuentas que emplea el banco.
- Los distintos tipos de información de identificación disponibles.
- El tamaño, la ubicación y el tipo de clientela del banco, incluyendo los tipos de productos y servicios utilizados por clientes en diferentes ubicaciones geográficas.

De conformidad con la reglamentación del CIP, una "cuenta" es una relación bancaria formal para proporcionar o participar en, servicios, negociaciones u otras transacciones financieras, e incluye una cuenta de depósito, una cuenta de transacciones o de activos, una cuenta de crédito u otra concesión de crédito. Una cuenta también incluye una relación establecida para proporcionar una caja de seguridad u otro servicio de custodia o para proporcionar servicios fiduciarios, de gestión de caja o de custodia.

Una cuenta no incluye:

- Productos o servicios para los cuales no se establece una relación bancaria formal con una persona, como cobro de cheques, transferencia de fondos o la venta de cheques o giros postales.
- Cuentas que el banco adquiera. Esto puede incluir cuentas individuales o múltiples como resultado de la compra de activos, la adquisición, la fusión o la toma de los pasivos.
- Cuentas abiertas para participar en el plan de beneficios para empleados creado bajo la Ley de Seguridad de los Ingresos para el Retiro de los Empleados de 1974.

La reglamentación del CIP se aplica a un "cliente". Un cliente es una "persona" (persona física, corporación, sociedad, fideicomiso, cuerpo político o cualquier otra entidad con personalidad jurídica) que abre una cuenta, una persona física que abre una cuenta para otra persona que no tiene capacidad legal y una persona física que abre una cuenta para una entidad que no es una persona jurídica (p. ej., un club cívico). La definición de cliente excluye a quienes no reciben servicios bancarios, como una persona cuya solicitud de préstamo es rechazada.[43] La definición de "cliente" tampoco incluye a un cliente existente, siempre y cuando el banco tenga la convicción razonable de que conoce la verdadera identidad del cliente.[44] Quedan excluidos de esta definición de cliente los

[43] Cuando la cuenta es un préstamo, debe considerarse "abierta" cuando el banco celebra un contrato exigible para conceder un préstamo al cliente.

[44] El banco puede demostrar que conoce la verdadera identidad de un cliente existente demostrando que antes de la expedición de la reglamentación definitiva del CIP, disponía de procedimientos equiparables para verificar la identidad de personas que tenían cuentas en el banco desde el 1 de Octubre de 2003, aunque el banco no haya recopilado la misma información acerca de dichas personas que requiere la reglamentación definitiva del CIP. Otras alternativas incluyen demostrar que el banco ha tenido una relación activa y perdurable con una persona en particular, según queda demostrado en los registros de

bancos sujetos a una agencia de regulación federal, bancos regulados por un ente regulador bancario estatal, entidades gubernamentales y compañías que cotizan en la Bolsa de Valores (como se describe en 31 CFR 103.22(d)(2)(ii) hasta (iv)).

Información requerida del cliente

El CIP debe contener procedimientos de apertura de cuenta que especifiquen la información de identificación que debe obtenerse de cada cliente.[45] Como mínimo, el banco debe obtener la siguiente información de identificación de cada cliente antes de que se abra la cuenta:[46]

- Nombre.
- Fecha de nacimiento (para personas físicas).
- Domicilio.[47]
- Número de identificación.[48]

Según su análisis de riesgos, es posible que un banco exija información de identificación adicional, además de lo enumerado anteriormente para ciertos clientes y líneas de productos.

---

estados de cuenta enviados a la persona, la información enviada al Servicio de Impuestos Internos (IRS) sobre las cuentas sin expedir de la persona, los préstamos efectuados y reembolsados y otros servicios prestados a la persona durante cierto período. Sin embargo, los procedimientos equiparables utilizados para verificar la identidad descritos anteriormente pueden no ser suficientes para las personas que el banco considere de alto riesgo.

[45] Cuando una persona abre una cuenta para una entidad que no es persona jurídica o para otro individuo que no tiene capacidad legal, debe obtenerse la información de identificación del individuo que abre la cuenta. Por el contrario, cuando un agente en nombre de otra persona abre una cuenta, el banco debe obtener la información de identificación de la persona en nombre de quien se abre la cuenta.

[46] Para los clientes de tarjetas de crédito, el banco debe obtener la información de identificación de un tercero antes de conceder el crédito.

[47] Para personas físicas: un domicilio particular o comercial, o si la persona física no cuenta con dicho domicilio, el número de Apartado postal del ejército (APO, por sus siglas en inglés) o de la marina (FPO, por sus siglas en inglés), el domicilio particular o comercial de un pariente u otro individuo que sea su contacto, o una descripción de la ubicación física del cliente. Para una "persona" que no sea una persona física (como una corporación, sociedad o fideicomiso): un lugar donde esté el asiento principal de los negocios, oficina local u otra ubicación física.

[48] Un número de identificación para un ciudadano estadounidense es un número de identificación fiscal (TIN, por sus siglas en inglés) (o una constancia de solicitud de éste) y un número de identificación para un ciudadano no estadounidense es uno o más de los siguientes: un TIN; número de pasaporte y el país que lo expidió; un número de tarjeta de identificación de extranjero; o un número y país de expedición de cualquier otro documento que no haya caducado expedido por un gobierno que sirva de constancia de la nacionalidad o residencia y que muestre una fotografía o garantía similar. El TIN se define en la sección 6109 del Código de Impuestos Internos de 1986 (26 USC 6109) y los reglamentos del IRS que implementan esa sección (p. ej., el número del Seguro Social [SSN, por sus siglas en inglés], el número de identificación fiscal individual [ITIN, por sus siglas en inglés], o el número de identificación del empleador).

Verificación del cliente

El CIP debe contener procedimientos en función del riesgo para verificar la identidad del cliente dentro de un período prudencial luego de que se abre la cuenta. Los procesos de verificación deben hacer uso de "la información obtenida según [31 CFR 103.121] párrafo (b)(2)(i)", particularmente la información de identificación obtenida por el banco. No es necesario que un banco establezca la veracidad de cada elemento de la información de identificación obtenida, pero debe verificar información suficiente para que tenga la convicción razonable de que conoce la verdadera identidad del cliente. Los procedimientos del banco deben describir cuando se utilizarán documentos, métodos no documentales o una combinación de ambos.

Verificación mediante documentos

Un banco que utiliza métodos documentales para verificar la identidad de un cliente debe contar con procedimientos que establezcan la documentación mínima aceptable. La reglamentación del CIP da ejemplos de los tipos de documentos que se han considerado tradicionalmente como fuentes primarias de identificación. La reglamentación refleja las expectativas de las agencias bancarias federales en cuanto a que los bancos controlen una forma de identificación expedida por el gobierno que no haya caducado a la mayoría de los clientes. La identificación debe proporcionar una constancia de la nacionalidad o residencia del cliente y mostrar una fotografía o garantía similar; los ejemplos incluyen una licencia de conducir o un pasaporte. Sin embargo, se pueden utilizar otras formas de identificación si permiten que el banco tenga la convicción razonable de que conoce la verdadera identidad del cliente. No obstante, debido a la existencia de documentos falsificados u obtenidos de manera fraudulenta, se exhorta a los bancos a que controlen más de un documento para asegurarse de tener la convicción razonable de que conocen la verdadera identidad del cliente.

Respecto a una "persona" que no sea una persona física (como una corporación, sociedad o fideicomiso), el banco debe obtener documentos que muestren la existencia legal de la entidad, como actas constitutivas certificadas, una licencia comercial expedida por el gobierno que no haya caducado, un acuerdo de sociedad o un instrumento fiduciario.

Verificación mediante métodos no documentales

No se exige que los bancos utilicen métodos no documentales para verificar la identidad de un cliente. Sin embargo, un banco que utiliza métodos no documentales para verificar la identidad de un cliente debe contar con procedimientos que establezcan los métodos que el banco utilizará. Los métodos no documentales pueden incluir el contacto con un cliente; verificar de manera independiente la identidad del cliente mediante la comparación de la información proporcionada por el cliente con información obtenida de una agencia de información a consumidores, una base de datos pública u otra fuente; verificar referencias con otras instituciones financieras; y obtener un estado financiero.

Los procedimientos no documentales del banco también deben ocuparse de las siguientes situaciones: Una persona física no puede presentar un documento de identificación expedido por el gobierno que no haya caducado que muestre una fotografía o garantía similar; el banco no está familiarizado con los documentos presentados; se abre la cuenta sin obtener documentos (p. ej., el banco obtiene la información requerida del cliente con el propósito de verificarla); el cliente abre la cuenta sin presentarse en persona; o, de otro modo, el banco enfrenta circunstancias que incrementan el riesgo de que éste no pueda verificar la verdadera identidad de un cliente mediante documentos.

Verificación adicional para ciertos clientes

El CIP debe contemplar casos donde, según su análisis de riesgos de una nueva cuenta abierta por un cliente que no sea una persona física, el banco obtendrá información de personas físicas con autoridad o control sobre dichas cuentas, incluidos los firmantes, con el objetivo de verificar la identidad del cliente. Este método de verificación se aplica sólo cuando el banco no puede verificar la verdadera identidad del cliente utilizando métodos documentales o no documentales. Por ejemplo, es posible que un banco necesite obtener información sobre la identidad de un empresario individual o los socios principales de una sociedad cuando el banco no puede, de otro modo, identificar de manera satisfactoria la compañía unipersonal o la sociedad.

Falta de verificación

El CIP también debe contar con procedimientos para las circunstancias en las que el banco no pueda tener la convicción razonable de que conoce la verdadera identidad del cliente. Estos procedimientos deben describir:

- Las circunstancias en las que el banco no debe abrir una cuenta.
- Los términos bajo los cuales un cliente puede hacer uso de una cuenta mientras el banco intenta verificar la identidad de dicho cliente.
- Las circunstancias en las cuales el banco debe cerrar una cuenta, luego de que no fuera posible verificar la identidad de un cliente.
- El momento en que el banco debe presentar un SAR de conformidad con la normativa vigente.

Exigencias con respecto a la gestión y conservación de registros

El CIP de un banco debe incluir procedimientos de conservación de registros. Como mínimo, el banco debe conservar la información de identificación (nombre, domicilio, fecha de nacimiento de una persona física, TIN y cualquier otra información exigida por

el CIP).[49] Para las tarjetas de crédito, el período de conservación es de cinco años luego de que la cuenta se haya cerrado o haya permanecido inactiva.

El banco también debe conservar una descripción de los siguientes elementos durante los cinco años siguientes a la creación del registro:

- Todo documento empleado para verificar la identidad, registrando el tipo de documento, el número de identificación, el lugar de expedición y, si corresponde, la fecha de expedición y la de caducidad.
- El método utilizado y los resultados obtenidos a partir de las medidas tomadas para verificar la identidad.
- Los resultados de cualquier discrepancia sustantiva que se haya descubierto al verificar la identidad.

Comparación con las listas gubernamentales

El CIP debe incluir procedimientos para determinar si el cliente aparece en las listas del gobierno federal de organizaciones terroristas o terroristas conocidos o bajo sospecha.[50] Cada vez que se expida una lista, el Tesoro de los Estados Unidos se comunicará con los bancos tras consultar con su agencia bancaria federal. En ese momento, los bancos deben comparar los nombres de los clientes con los de la lista dentro de un tiempo prudencial luego de la apertura de la cuenta o antes; si así lo exigiera el gobierno, y deben cumplir las instrucciones que acompañen dicha lista.

---

[49] Un banco puede conservar fotocopias de documentos de identificación que utilice para verificar la identidad de un cliente; sin embargo, el reglamento del CIP no lo exige. Los procedimientos de verificación de un banco deben desarrollarse en función del riesgo y, en algunos casos, la conservación de copias de documentos de identificación puede justificarse. Además, es posible que un banco cuente con procedimientos para conservar copias de los documentos para otros fines, por ejemplo, para facilitar la investigación de un fraude potencial. Sin embargo, si un banco opta por conservar fotocopias de documentos de identificación, debe asegurarse de que dichas fotocopias estén protegidas físicamente contra un posible robo de identidad. (Estos documentos deben conservarse según las exigencias generales con respecto a la conservación de registros en 31 CFR 103.38.) No obstante, un banco debe tener presente que no debe utilizar de manera inadecuada ningún documento que contenga una fotografía de una persona física, como una licencia de conducir, en relación con ningún aspecto de una transacción de crédito. Consulte *Frequently Asked Questions Related to Customer Identification Program Rules* (Preguntas frecuentes relacionadas con las reglamentaciones del programa de identificación de clientes), publicadas el 28 de Abril de 2005 por la FinCEN, la Junta de Gobernadores del Sistema de Reserva Federal., la Corporación Federal de Seguro de Depósitos, la Administración Nacional de Cooperativas de Crédito, la Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro.

[50] A la fecha de publicación de este manual, no existen listas gubernamentales designadas para verificar específicamente los fines del CIP. Las comparaciones de clientes con las listas exigidas por la OFAC y las solicitudes según 31 CFR 103.100 se consideran por separado e imponen diferentes exigencias.

Notificación adecuada al cliente

El CIP debe incluir procedimientos para proporcionar a los clientes una notificación adecuada de que el banco se encuentra en proceso de solicitud de información para verificar sus identidades. La notificación debe describir en términos generales las exigencias de identificación fijadas por el banco y proporcionarse de tal manera que se le permita al cliente verla de manera razonable o recibirla de alguna forma antes de que se abra la cuenta. Ejemplos de ello son la exhibición de la notificación en el vestíbulo del banco, la publicación en un sitio Web, o como adjunto a los documentos de solicitud de préstamo. El reglamento proporciona un modelo de lo que debe especificar la notificación:

> INFORMACIÓN IMPORTANTE ACERCA DE LOS PROCEDIMIENTOS PARA ABRIR UNA CUENTA: Para colaborar con el gobierno en la lucha contra el financiamiento del terrorismo y las actividades de lavado de dinero, la ley federal exige que toda institución financiera obtenga, verifique y registre información que permita identificar a toda persona que abra una cuenta. Para usted, esto significa que: cuando abre una cuenta, le preguntaremos su nombre, domicilio, fecha de nacimiento y otra información que nos permitirá identificarlo. También podremos solicitar que nos muestre su licencia de conducir u otros documentos de identificación.

Dependencia de otra institución financiera

Se permite que un banco dependa de otra institución financiera (incluida una filial) para llevar a cabo algunos o todos los elementos que constituyen el CIP, si esta dependencia se plantea en este programa y se cumplen los siguientes criterios:

- La institución financiera de la que se depende está sujeta a una reglamentación que implementa las exigencias del programa AML de 31 USC 5318(h) y está regulada por un ente regulador funcional federal.[51]
- El cliente tiene una cuenta o está a punto de abrir una cuenta en el banco y en la otra institución regulada funcionalmente.
- La dependencia es razonable, bajo las circunstancias dadas.
- La otra institución financiera celebra un contrato por medio del cual se compromete a certificar anualmente ante el banco que ha implementado su programa AML y que cumplirá (o su agente cumplirá) con las exigencias especificadas del CIP del banco.

[51] Ente regulador funcional federal significa: Junta de Gobernadores del Sistema de Reserva Federal; Corporación Federal de Seguro de Depósitos; Administración Nacional de Cooperativas de Crédito; Oficina del Interventor Monetario; Oficina de Supervisión de Instituciones de Ahorro; Comisión de Valores y Bolsa o Comisión del Mercado de Futuros de Bienes.

Utilización de terceros

La reglamentación del CIP no modifica la potestad de un banco de utilizar un tercero, como un agente o proveedor de servicios, para que preste servicios en su nombre. Por lo tanto, se permite que un banco concierte con un tercero, como un concesionario de automóviles o agente hipotecario, para que éste, desempeñándose como su agente en relación con un préstamo, verifique la identidad de su cliente. El banco también puede concertar con un tercero la conservación de sus registros. Sin embargo, como con cualquier otra responsabilidad que se delega a un tercero, el banco es el responsable en última instancia del cumplimiento del tercero conforme a las exigencias del CIP del banco. Como resultado, los bancos deben establecer controles adecuados y controlar los procedimientos de esas relaciones. Esta exigencia es contraria a la disposición sobre dependencia de la reglamentación que permite que la parte de la que se depende asuma responsabilidad. Consulte “Dependencia de otra institución financiera”, página 63.

Otras exigencias legales

Ninguna parte de la reglamentación del CIP libera a un banco de sus obligaciones bajo cualquier disposición de la BSA u otras leyes, reglamentaciones y reglamentos AML, particularmente con respecto a las disposiciones concernientes a la información que debe obtenerse, verificarse o conservarse en relación con toda cuenta o transacción.

El Tesoro de los Estados Unidos y las agencias bancarias federales le han proporcionado a los bancos Preguntas frecuentes (FAQ, por sus siglas en inglés) que se revisan periódicamente. Las Preguntas frecuentes y otros documentos relacionados (p. ej., la reglamentación del CIP) están disponibles en los sitios Web de la FinCEN y de las agencias bancarias federales.

Procedimientos de Inspección

Programa de identificación de clientes

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para el Programa de identificación de clientes (CIP).*

1. Verifique que las políticas, los procedimientos y los procesos del banco cuenten con un programa exhaustivo para identificar a los clientes que abren una cuenta después del 1 de Octubre de 2003. El programa escrito debe estar incluido dentro del programa de cumplimiento BSA/AML del banco y debe contar, como mínimo, con políticas, procedimientos y procesos para lo siguiente:

   - Identificación de la información que debe ser obtenida (incluidos el nombre, la dirección, el número de identificación fiscal [TIN] y la fecha de nacimiento para los individuos particulares), y procedimientos de verificación de identidad en función del riesgo (incluidos los procedimientos que tratan sobre situaciones en las que no se puede realizar la verificación).

   - Procedimientos para cumplir con las exigencias respecto a la conservación de los registros.

   - Procedimientos para comparar cuentas nuevas con las listas gubernamentales establecidas, si es pertinente.

   - Procedimientos para brindar una adecuada notificación al cliente.

   - Procedimientos que cubren la dependencia del banco de otra institución financiera o un tercero, si es pertinente.

   - Procedimientos para determinar si debe presentarse un SAR y cuándo.

2. Determine si el CIP del banco tiene en cuenta los tipos de cuentas ofrecidas; los métodos de apertura de cuentas y el tamaño, la ubicación y el tipo de clientela del banco.

3. Determine si es razonable la política del banco respecto a la apertura de nuevas cuentas para clientes existentes.

4. Revise el acta de la junta y verifique que la junta directiva apruebe el CIP, por separado o como parte del programa de cumplimiento BSA/AML (31 CFR 103.121(b)(1)).

5. Evalúe los programas de auditoría y capacitación del banco para garantizar que el CIP esté incorporado de manera adecuada (31 CFR 103.121(b)(1)).

6. Evalúe las políticas, los procedimientos y los procesos del banco para verificar que todas las cuentas nuevas sean comparadas con las listas gubernamentales establecidas sobre terroristas bajo sospecha u organizaciones terroristas de manera oportuna, si tales listas son emitidas (31 CFR 103.121(b)(4)).

Pruebas de transacciones

7. En función del análisis de riesgos, los informes de inspección previos y un control de los resultados de la auditoría del banco, seleccione una muestra de las nuevas cuentas abiertas desde la inspección más reciente para revisar el cumplimiento con el CIP del banco. La muestra debe ser representativa de las diferentes cuentas (p. ej., particulares y empresas, préstamos y depósitos, relaciones con tarjetas de créditos, y cuentas de Internet). La muestra debe, además, incluir lo siguiente:

   - Cuentas abiertas para un cliente que proporciona una solicitud para un TIN o cuentas abiertas con procedimientos de verificación incompletos.
   - Cuentas nuevas abiertas utilizando métodos documentales y cuentas nuevas abiertas utilizando métodos no documentales.
   - Cuentas identificadas como de mayor riesgo.[52]
   - Cuentas abiertas por clientes de mayor riesgo existentes.
   - Cuentas abiertas con excepciones.
   - Cuentas abiertas por terceros (p. ej., préstamos indirectos).

8. De la muestra previa de cuentas nuevas, determine si el banco ha realizado los siguientes procedimientos:

   - Ha abierto la cuenta según las exigencias del CIP (31 CFR 103.121(b)(1)).
   - Ha tenido la convicción razonable respecto a la verdadera identidad de un cliente, que incluye un cliente de mayor riesgo. (El banco debe tener con anterioridad una convicción razonable respecto a la identidad de un cliente existente [31 CFR 103.121(b)(2)]).
   - Ha obtenido de cada cliente, antes de la apertura de la cuenta, la información sobre la identidad exigida por el CIP (31 CFR 103.121(b)(2)(i)) (p. ej., nombre, fecha de nacimiento, dirección y número de identificación).
   - Dentro de un plazo prudencial luego de la apertura de la cuenta, ha verificado la información sobre la identidad del cliente lo suficiente como para tener una convicción razonable respecto a la verdadera identidad del mismo (31 CFR 103.121(b)(2)(ii)).
   - Ha resuelto de manera adecuada las situaciones en las que la identidad del cliente no haya podido establecerse razonablemente (31 CFR 103.121(b)(2)(iii)).

[52] Las cuentas de mayor riesgo, a los efectos del CIP, pueden incluir cuentas en las que la verificación de la identificación es generalmente más difícil (p. ej., banca privada extranjera y cuentas fiduciarias, cuentas de políticos extranjeros de alto nivel, cuentas fuera del país, y cuentas fuera del área y en las que no hay contacto directo).

- Ha mantenido un registro de la información sobre la identidad exigida por el CIP, el método utilizado para verificar la identidad y los resultados de la verificación (incluidos los resultados de las discrepancias) (31 CFR 103.121(b)(3)).

- Ha comparado el nombre del cliente con la lista de organizaciones terroristas o terroristas conocidos o bajo sospecha, si es pertinente (31 CFR 103.121(b)(4)).

- Ha presentado los informes SAR, según corresponda.

9. Evalúe el nivel de las excepciones al CIP para determinar si el banco ha implementado su CIP de manera eficaz. Una política del banco puede no permitir al personal realizar o aprobar excepciones al CIP. Sin embargo, un banco puede excluir errores aislados y errores no sistemáticos (como una cantidad insignificante de errores de entrada de datos) de las exigencias del CIP sin comprometer la eficacia del mismo (31 CFR 103.121(b)(1)).

10. En función del análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de las relaciones con terceros que sean confiables para el banco a fin de realizar su CIP (o porciones de su CIP), si es pertinente. Si el banco está utilizando la "disposición sobre dependencia":

    - Determine si el tercero es una institución regulada por una agencia federal sujeta a una reglamentación final de ejecución de las exigencias del programa AML de 31 USC 5318(h).

    - Revise el contrato entre las partes, las certificaciones anuales y otra información, como el CIP de terceros (31 CFR 103.121(b)(6)).

    - Determine si la dependencia es razonable. El contrato y la certificación brindarán un recurso estándar para que el banco demuestre que ha cumplido la "disposición sobre dependencia", a menos que el inspector tenga motivos para creer que la dependencia del banco no es razonable (p. ej., el tercero ha sido sujeto a una acción de aplicación de la ley a causa de deficiencias o violaciones AML o a la BSA).

11. Si el banco está utilizando un agente o prestador de servicios para realizar elementos de su CIP, determine si el banco ha establecido controles internos apropiados y procedimientos de control para garantizar que su CIP está siendo implementado por el agente de terceros o en las relaciones de prestación de servicios (p. ej., concesionarios de automóviles).

12. Revise la aptitud de la notificación que envía el banco a sus clientes y que la entrega de la notificación sea oportuna (31 CFR 103.121(b)(5)).

13. Evalúe la política de conservación de registro del CIP del banco y asegúrese de que se corresponda con las exigencias normativas sobre conservación de ciertos registros. El banco debe conservar la información sobre la identidad obtenida en el momento de la apertura de cuenta durante cinco años luego del cierre de dicha cuenta. El banco debe conservar también una descripción de los documentos empleados, los métodos

utilizados para verificar la identidad y la resolución de las discrepancias durante cinco años luego de que sea asentado el registro (31 CFR 103.121(b)(3)(ii)).

14. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos para cumplir con las exigencias normativas asociadas con el CIP.

Debida Diligencia de los Clientes: Esquema General

Objetivo: *Evaluar si las políticas, los procedimientos y los procesos de debida diligencia de los clientes (CDD) del banco son apropiados y lo suficientemente completos para obtener información sobre los clientes y evaluar el valor de esta información en la detección, la supervisión y el informe de actividades sospechosas.*

La piedra angular de un programa de cumplimiento BSA/AML sólido es la adopción e implementación de políticas, procedimientos y procesos de CDD exhaustivos para todos los clientes, especialmente para aquellos que presentan un mayor riesgo de lavado de dinero y financiamiento del terrorismo. El objetivo de CDD debe ser permitir que el banco pronostique con relativa certeza los tipos de transacciones en las que es probable que el cliente participe. Estos procesos ayudan al banco a determinar en qué momento las transacciones pueden ser sospechosas. El concepto de CDD comienza con la verificación de la identidad del cliente y el análisis del riesgo asociado con dicho cliente. Los procesos deben incluir también CDD especiales para clientes de mayor riesgo y debida diligencia continua aplicada a el tipo de clientela.

Las políticas, los procedimientos y los procesos de CDD efectivos proporcionan un marco decisivo que permite al banco cumplir con las exigencias normativas e informar toda actividad sospechosa. Un ejemplo de este concepto se ofrece en el Apéndice K ("Riesgo del cliente frente a la debida diligencia y la supervisión de actividades sospechosas"). Las políticas, los procedimientos y los procesos de CDD son decisivos para el banco porque contribuyen a:

- Detectar e informar sobre transacciones poco habituales o sospechosas que exponen potencialmente al banco a pérdidas financieras, aumento de gastos o riesgos que puedan afectar la reputación de la institución.
- Evitar la exposición delictiva causada por personas que utilizan o intentan utilizar los productos y servicios del banco con fines ilícitos.
- Adherir a prácticas bancarias responsables y seguras.

Guía para la debida diligencia de los clientes

Las políticas, los procedimientos y los procesos BSA/AML deben incluir guías para la debida diligencia del cliente (CDD) que:

- Sean adecuadas al perfil de riesgo BSA/AML del banco, especialmente con respecto a clientes de mayor riesgo.
- Contengan una declaración clara acerca de las expectativas generales de la gerencia y fijen las responsabilidades concretas del personal, incluyendo a la persona encargada de revisar o aprobar los cambios en la valoración del riesgo o el perfil de riesgo del cliente, según corresponda.

- Garanticen que el banco posee suficiente información del cliente para implementar un sistema eficaz de supervisión de actividades sospechosas.
- Proporcionen orientación para la documentación de análisis asociados con los procesos de debida diligencia, que incluyan guías para resolver problemas de casos en que no se cuente con suficiente información o ésta sea incorrecta o imprecisa.
- Garanticen que el banco disponga de información actualizada sobre los clientes.

Riesgos que puedan plantear los clientes

La gerencia debe tener una comprensión exhaustiva de todos los riesgos del lavado del dinero o financiamiento del terrorismo que implica el tipo de clientela del banco. Bajo este enfoque, el banco debe obtener suficiente información al momento de apertura de una cuenta que le permita lograr comprender cuál es la actividad normal que puede esperarse de un cliente debido a su ocupación u operaciones comerciales. Esta comprensión puede fundamentarse en el tipo de cuenta o en la clasificación del cliente. Como guía adicional, consulte el Apéndice K (“Riesgo del cliente frente a la debida diligencia y la supervisión de actividades sospechosas”).

Esta información debe permitir al banco diferenciar entre los clientes de bajo riesgo y los de alto riesgo en el momento de apertura de la cuenta. Los bancos deben supervisar a los clientes de bajo riesgo a través de la supervisión periódica de actividades sospechosas y los procesos de debida diligencia de los clientes. Si existe una indicación de un cambio potencial en el perfil de riesgo del cliente (p. ej., actividad de la cuenta prevista, cambio de empleo u operaciones comerciales), la gerencia debe volver a analizar la valoración del riesgo del cliente y seguir las políticas y los procedimientos del banco establecidos para mantener o cambiar la valoración del riesgo del cliente.

Gran parte de la información de CDD se puede confirmar a través de una agencia dedicada al envío de información, referencias bancarias (para las cuentas grandes), correspondencia y conversaciones telefónicas con el cliente, y visitas a la sede comercial del cliente. Algunas medidas adicionales pueden incluir las referencias de terceros o la investigación de información disponible al público (p. ej., a través de Internet o bases de datos comerciales).

Los procesos de CDD deben incluir una supervisión periódica en función del riesgo de la relación con el cliente para determinar si se han presentado cambios importantes en la información de CDD original (p. ej., cambios en el empleo u operaciones comerciales).

Debida diligencia especial para clientes de mayor riesgo

Los clientes que representan un mayor riesgo de lavado de dinero o financiamiento del terrorismo incrementan el grado de exposición del banco; como consecuencia de ello, las políticas, los procedimientos y los procesos de debida diligencia deben ser especiales. Es fundamental aplicar una debida diligencia especial (EDD, por sus siglas en inglés) a los clientes de mayor riesgo para poder comprender sus transacciones anticipadamente e implementar un sistema de supervisión de actividades sospechosas que permita reducir

riesgos que puedan afectar la reputación, el cumplimiento y las transacciones del banco. Los clientes de mayor riesgo y sus transacciones se deben revisar más de cerca en el momento de apertura de las cuentas y con mayor frecuencia durante el transcurso de su relación con el banco. En las páginas 23 a 33 de la sección del esquema general, "Análisis de riesgos BSA/AML", se puede encontrar una guía para identificar a los clientes de mayor riesgo.

El banco puede determinar que un cliente representa un riesgo mayor debido a su actividad comercial, la estructura de sus propiedades, el tipo y volumen de sus transacciones planeadas o reales, incluidas aquellas relacionadas con jurisdicciones de mayor riesgo. Si es así, el banco debe considerar la posibilidad de obtener, tanto al momento de apertura de la cuenta como durante el transcurso de la relación con el cliente, la siguiente información sobre el mismo:

- Propósito de la cuenta.
- Origen de los fondos y de la riqueza.
- Personas físicas propietarias o que tengan control sobre la cuenta, como usufructuarios, firmantes o garantes.
- Ocupación o tipo de negocio (del cliente u otras personas beneficiarias de un usufructo o que tengan control sobre la cuenta).
- Estados financieros.
- Referencias bancarias.
- Domicilio (donde se constituyó el negocio).
- Proximidad de la residencia, lugar de empleo o sede comercial del cliente con respecto al banco.
- Descripción de la zona de actividad comercial principal del cliente e información sobre si éste efectuará transacciones internacionales de manera habitual.
- Descripción de las operaciones de negocios, el volumen previsto de moneda y las ventas totales, y una lista de los principales clientes y proveedores.
- Explicación sobre los cambios efectuados en la actividad de la cuenta.

Como la debida diligencia es un proceso continuo, un banco debe tomar medidas para garantizar que los perfiles de cuenta sean actuales y la supervisión se establezca en función del riesgo. Los bancos deben tener en cuenta si los perfiles de riesgo deben ajustarse o la actividad sospechosa debe informarse cuando ésta no sea coherente con el perfil.

Procedimientos de Inspección

Debida diligencia de los clientes

Objetivo: *Evaluar si las políticas, los procedimientos y los procesos de debida diligencia de los clientes (CDD) del banco son apropiados y lo suficientemente completos para obtener información sobre los clientes y evaluar el valor de esta información en la detección, la supervisión y el informe de actividades sospechosas.*

1. Determine si las políticas, los procedimientos y los procesos del banco son adecuados al perfil de riesgo del banco. Determine si el banco dispone de procesos para obtener información al momento de la apertura de la cuenta, además de garantizar que se mantenga la información actualizada del cliente.

2. Determine si las políticas, los procedimientos y los procesos permiten cambios en la valoración del riesgo o el perfil de riesgo del cliente. Determine quién es responsable de revisar o aprobar tales cambios.

3. Revise los procedimientos y procesos de debida diligencia especial que el banco utiliza para identificar a los clientes que puedan plantear un mayor riesgo de lavado de dinero o financiamiento del terrorismo.

4. Determine si el banco proporciona orientación para la documentación de análisis asociados con los procesos de debida diligencia, que incluyan guías para resolver problemas cuando se obtenga información insuficiente o incorrecta.

Pruebas de transacciones

5. En función de un análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, realice una muestra de información de CDD para clientes de mayor riesgo. Determine si el banco recopila información apropiada e incorpora eficazmente esta información en los procesos de supervisión de actividades sospechosas. Se puede realizar esta muestra cuando se verifica el cumplimiento del banco con sus políticas, procedimientos y procesos, así como cuando se controlan las transacciones o las cuentas en busca de posibles actividades sospechosas.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con CDD.

Informes de Actividades Sospechosas: Esquema General

Objetivo: *Evaluar las políticas, los procedimientos y los procesos del banco, y el cumplimiento general de las exigencias normativas y legales para la supervisión, la detección y la elaboración de informes sobre actividades sospechosas.*

Los formularios empleados para informar sobre actividades sospechosas constituyen la piedra angular del sistema de informes de la BSA. Esto es fundamental para la capacidad de los Estados Unidos de utilizar información financiera para combatir el terrorismo, el financiamiento del terrorismo, el lavado de dinero y otros delitos financieros. Los inspectores y los bancos deben reconocer que la calidad del contenido de los SAR es fundamental para la aptitud y eficacia del sistema de informe de actividades sospechosas.

Dentro de este sistema, la FinCEN y las agencias bancarias federales reconocen que, desde una perspectiva práctica, no es posible que los bancos detecten e informen todas las actividades potencialmente ilícitas que fluyen por el banco. Los inspectores se deben concentrar en la evaluación de las políticas, los procedimientos y los procesos del banco para identificar, evaluar e informar actividades sospechosas. Sin embargo, como parte del proceso de inspección, los inspectores deben revisar las decisiones individuales sobre presentación de SAR para determinar la eficacia de los procesos de identificación, evaluación e informe del banco. Los bancos, las sociedades de control de bancos y las subsidiarias de las mismas están obligados por reglamentos federales[53] a presentar un SAR en los siguientes casos:

- Violaciones penales que impliquen abuso por parte de personal interno, por cualquier monto.
- Violaciones penales por un monto acumulado de USD 5.000 o más, cuando sea posible identificar a un sospechoso.
- Violaciones penales por un monto acumulado de USD 25.000 o más, sin importar quién sea el sospechoso potencial.
- Transacciones realizadas por el banco, en el banco o a través de éste (o una subsidiaria), o el intento de realizarlas, por un monto acumulado de USD 5.000 o más, siempre que el banco o la subsidiaria sepa, sospeche o tenga fundamento para sospechar que dichas transacciones:
  - Pueden implicar la posibilidad de lavado de dinero u otras actividades ilícitas (p. ej., financiamiento del terrorismo).

[53] Consulte 12 CFR 208.62, 211.5(k), 211.24(f) y 225.4(f) (Junta de Gobernadores del Sistema de Reserva Federal); 12 CFR 353 (Corporación Federal de Seguro de Depósitos); 12 CFR 748 (Administración Nacional de Cooperativas de Crédito); 12 CFR 21.11 (Oficina del Interventor Monetario); 12 CFR 563.180 (Oficina de Supervisión de Instituciones de Ahorro) y 31 CFR 103.18 (FinCEN).

- Están diseñadas para evadir la BSA o sus reglamentos de ejecución.[54]
- No tienen un propósito comercial o lícito aparente o no constituyen el tipo de transacción que se esperaría del cliente particular en cuestión, y el banco no encuentra una explicación razonable que justifique dicha transacción luego de examinar los datos y hechos disponibles, inclusive los antecedentes y el posible propósito de la transacción.

Una transacción incluye depósitos; extracciones; transferencias entre cuentas; intercambios de divisas; ampliación de créditos; compra o venta de acciones, bonos, certificados de depósito u otros instrumentos monetarios o valores de inversión; o cualquier otro pago, transferencia o entrega realizada por un banco, a través de un banco o destinado a éste.

Protección legal de los bancos contra responsabilidad civil por los informes de actividades sospechosas

La ley federal (31 USC 5318 (g)(3)) protege contra la responsabilidad civil derivada de todos los informes de actividades sospechosas entregados a las autoridades respectivas, que incluyen toda la documentación respaldatoria, sin importar si dichos informes han sido presentados de conformidad o no con las instrucciones de los SAR. Concretamente, la ley dispone que los bancos y sus directores, funcionarios, empleados y agentes que divulguen información a las autoridades pertinentes sobre posibles violaciones a la ley o las normativas, que incluyen la divulgación de información relacionada con la elaboración de los informes SAR, "no serán responsables ante persona alguna bajo ley o normativa alguna de los Estados Unidos, constitución, ley o normativa de Estado alguno o subdivisión política alguna de Estado alguno o bajo contrato o acuerdo alguno que se pueda hacer cumplir legalmente (incluyendo acuerdos sobre arbitraje) en razón de dicha divulgación o por no haber notificado sobre la misma a la persona objeto de tal divulgación o a cualquier otra persona identificada en ella". La protección legal se aplica a los SAR presentados según los parámetros fijados para la elaboración de dichos informes, así como para los SAR sobre cualquier actividad presentados voluntariamente que cumplan las pautas fijadas para los mismos.

Sistemas para identificar, investigar e informar sobre actividades sospechosas

La supervisión y el informe de actividades sospechosas son controles internos fundamentales. Los procesos adecuados de supervisión e informe son esenciales para garantizar que el banco tenga un programa de cumplimiento BSA adecuado y eficaz. Deben existir políticas, procedimientos y procesos apropiados para supervisar e identificar actividades inusuales. La sofisticación de los sistemas de supervisión debe ser determinada por el perfil de riesgo del banco, con énfasis especial en la composición de

[54] Consulte el Apéndice G ("Fraccionamiento") como guía adicional**.**

productos, servicios, clientes, entidades y ubicaciones geográficas de mayor riesgo. El banco debe asegurarse de asignar personal adecuado para la identificación, investigación y elaboración de informes de actividades sospechosas según el perfil de riesgo general que tenga la entidad, así como el volumen de sus transacciones. Los sistemas de supervisión generalmente incluyen identificación de empleados o casos de remisiones, sistemas (manuales) basados en transacciones, sistemas (automatizados) de vigilancia o cualquier combinación de estos.

En general, los sistemas eficaces de supervisión e informe de actividades sospechosas incluyen cuatro componentes clave (consulte el Apéndice S, "Componentes clave de supervisión de actividades sospechosas"). Los componentes, indicados más adelante, son interdependientes, y un proceso eficaz de supervisión e informe de actividades sospechosas debe incluir la implementación satisfactoria de cada componente. Las irregularidades en cualquiera de estos componentes pueden afectar de manera desfavorable los informes SAR y el cumplimiento de la BSA. Los cuatro componentes clave de un sistema eficaz de supervisión e informe son:

- Identificación o alerta de actividades poco habituales (que pueden incluir: identificación de empleados, consultas de las autoridades de aplicación de la ley, otros casos de remisiones y resultados del sistema de supervisión de vigilancia y transacciones).
- Gestión de alertas.
- Toma de decisiones en relación con los SAR.
- Realización y presentación de SAR.

Estos cuatro componentes están presentes en los bancos de todos los tamaños. Sin embargo, la estructura y la formalidad de los componentes pueden variar. En general, los bancos más grandes tendrán una mayor diferenciación y distinción entre funciones, y pueden dedicar departamentos completos a la realización de cada componente. Los bancos más pequeños pueden designar a uno o más empleados para realizar varias tareas (p. ej., revisión de informes de supervisión, actividad de investigación y realización de SAR). Las políticas, los procedimientos y los procesos deben describir los pasos que toma el banco para abordar cada componente e indicar las personas o los departamentos responsables de la identificación o producción de una alerta de actividades poco habituales, la gestión de alertas, la decisión de presentación y la realización y presentación del SAR.

Identificación de actividades poco habituales

Los bancos usan varios métodos para identificar posibles actividades sospechosas, incluidas, entre otras, actividades identificadas por los empleados durante las operaciones diarias, consultas de las autoridades de aplicación de la ley o solicitudes, como las que se ven generalmente en las solicitudes según las secciones 314(a) y 314(b), resultados del sistema de supervisión de vigilancia y transacciones, o cualquier combinación de estos.

Identificación de empleados

Durante el curso de las operaciones diarias, los empleados pueden observar actividades de transacciones poco habituales o posiblemente sospechosas. Los bancos deben implementar capacitación, políticas y procedimientos adecuados para garantizar que el personal adhiera a los procesos internos para identificar o remitir posibles actividades sospechosas. Los bancos deben tener en cuenta todos los métodos de identificación y deben garantizar que su sistema de supervisión de actividades sospechosas incluya procesos para facilitar la transferencia de remisiones internas al personal adecuado para que investigue en profundidad.

Solicitudes y consultas de las autoridades de aplicación de la ley

Los bancos deben establecer políticas, procedimientos y procesos para identificar a quienes sean objeto de solicitudes de las autoridades de aplicación de la ley, supervisar las actividades transaccionales de dichas personas, si corresponde, identificar las posibles actividades sospechosas o poco habituales relacionadas con dichas personas y presentar, según el caso, los SAR relacionados con esas personas. Las solicitudes y consultas de las autoridades de aplicación de la ley pueden incluir citaciones del jurado de acusación, Cartas de Seguridad Nacional (NSL, por sus siglas en inglés) y solicitudes según la sección 314(a).[55]

La mera recepción de cualquier consulta de las autoridades de aplicación de la ley no exige, por sí misma, la presentación de un SAR por parte del banco. No obstante, dicha consulta puede resultar relevante al análisis de riesgos general del banco en relación con sus clientes y cuentas. Por ejemplo, la recepción de una citación del jurado de acusación puede implicar que un banco revise la actividad de cuenta del cliente en cuestión.[56] El banco debe analizar toda la información que conozca sobre su cliente, incluida la recepción de una consulta de las autoridades de aplicación de la ley, de acuerdo con su programa de cumplimiento BSA/AML en función del riesgo.

El banco debe determinar si se debe presentar un SAR en función de toda la información del cliente disponible. Debido a la confidencialidad del proceso judicial del jurado de acusación, si un banco presenta un SAR luego de la recepción de una citación de este jurado, las autoridades de aplicación de la ley disuaden a los bancos de incluir cualquier referencia a la recepción o existencia de tal citación en el SAR. En cambio, el SAR debe hacer referencia sólo a aquellos datos y actividades que respalden el descubrimiento de transacciones sospechosas identificadas por el banco.

---

[55] Consulte la sección del esquema general principal, “Intercambio de información”, en las páginas 108 a 114, donde se tratan las solicitudes de la sección 314(a).

[56] Grupo de Asesoría de la Ley de Secreto Bancario, “Section 5 — Issues and Guidance” The SAR Activity Review – Trends, Tips & Issues (“Sección 5: Temas y orientación” Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas), edición 10 de Mayo de 2006, páginas 42 a 44, en www.fincen.gov.

Cartas de Seguridad Nacional

Las Cartas de Seguridad Nacional (NSL) son peticiones de investigación escritas que la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) local y otras autoridades gubernamentales federales pueden expedir en investigaciones de contraespionaje y contraterrorismo para obtener lo siguiente:

- Registros de comunicaciones electrónicas y telefónicas de prestadores de servicios de Internet y compañías telefónicas.[57]
- Información de oficinas de crédito.[58]
- Registros financieros de instituciones financieras.[59]

Las NSL son documentos sumamente confidenciales y, por esta razón, los inspectores no revisarán ni tomarán como muestra las NSL específicas.[60] De conformidad con 12 USC 3414(a)(3) y (5)(D), ningún banco, funcionario, empleado o agente de la institución puede divulgar a ninguna persona que una autoridad gubernamental o el FBI ha buscado u obtenido acceso a registros mediante una NSL según la Ley del Derecho a la Privacidad Financiera. Los bancos que reciben una NSL deben tomar las medidas adecuadas para garantizar la confidencialidad de las cartas y disponer de procedimientos para procesar y mantener la confidencialidad de las NSL.

Si un banco presenta un SAR luego de la recepción de una NSL, el SAR no deberá contener ninguna referencia sobre la recepción o existencia de la NSL. El SAR debe hacer referencia sólo a aquellos datos y actividades que respalden el descubrimiento de transacciones sospechosas o poco habituales identificadas por el banco.

Las preguntas respecto a las NSL deben enviarse a la oficina local del FBI del banco. La información de contacto de las oficinas locales del FBI puede encontrarse en www.fbi.gov.

Supervisión de transacciones (supervisión manual de transacciones)

En general, un sistema de supervisión de transacciones, a veces denominado sistema manual de supervisión de transacciones, aborda tipos específicos de transacciones (p. ej., aquellas que implican grandes cantidades de efectivo, aquellas que se realizan hacia o desde ubicaciones geográficas extranjeras, etc.) e incluye una revisión manual de diversos informes generados por los sistemas de proveedores o de MIS del banco, con el fin de identificar actividades poco habituales. Ejemplos de informes de MIS incluyen los

---

[57] Ley sobre la Privacidad en las Comunicaciones Electrónicas, 18 USC 2709.

[58] Ley sobre Informes de Crédito Justos, 15 USC 1681u.

[59] Ley del Derecho a la Privacidad Financiera de 1978, 12 USC 3401 *et seq.*

[60] Consulte Grupo de asesoría de la ley de secreto bancario, The SAR Activity Review — Trends, Tips & Issues (Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas), edición 8 de Abril de 2005 para obtener más información sobre la NSL disponible en www.fincen.gov.

informes sobre actividades en efectivo, informes de transferencias de fondos, informes de ventas de instrumentos monetarios, informes detallados de gran tamaño, informes de cambios significativos en el saldo e informes de fondos insuficientes (NSF). Muchos de los sistemas de proveedores o de MIS incluyen modelos de filtrado para identificar posibles actividades poco habituales. Es posible que el proceso implique un control de informes diarios, informes que cubren un período (p. ej., informes continuos de 30 días, informes mensuales) o una combinación de ambos tipos. El tipo y la frecuencia de los controles y los informes resultantes utilizados deben ser acordes con el perfil de riesgo BSA/AML del banco y deben cubrir de manera adecuada sus productos, servicios, clientes, entidades y ubicaciones geográficas de mayor riesgo.

Los informes de MIS o generados por sistemas de proveedores generalmente utilizan un umbral en dólares discrecional. Los umbrales seleccionados por la gerencia para la producción de informes de transacciones deben permitir que la gerencia detecte las actividades poco habituales. Al identificar una actividad poco habitual, el personal asignado debe revisar la información de CDD y otra información pertinente para determinar si la actividad es sospechosa. La gerencia debe evaluar periódicamente la validez de los criterios de filtrado y los umbrales utilizados en el proceso de supervisión. Cada banco debe evaluar e identificar los criterios de filtrado más adecuados para sus procesos. La programación de los sistemas de supervisión del banco se debe revisar independientemente para verificar que los criterios de filtrados sean razonables. Los informes de supervisión de transacciones típicos se describen a continuación.

Informes sobre actividades en moneda. La mayoría de los proveedores ofrecen informes que identifican todas las actividades en moneda o aquellas que superan los USD 10.000. Estos informes ayudan a los banqueros en la presentación de los CTR y en la identificación de actividades en efectivo sospechosas. La mayoría de los prestadores de servicios de información bancaria ofrecen informes sobre actividades en efectivo que pueden filtrar transacciones utilizando diversos parámetros, por ejemplo:

- Actividad en efectivo, incluidas transacciones múltiples por un valor superior a USD 10.000.
- Actividad en efectivo (una transacción o múltiples) por debajo de la exigencia de declaración de USD 10.000 (p. ej., entre USD 7.000 y USD 10.000).
- Transacciones en efectivo que impliquen múltiples transacciones en dólares menores (p. ej., USD 3.000) que durante un período (p. ej., 15 días) se acumulan hasta llegar a una suma de dinero sustancial (p. ej., USD 30.000).
- Transacciones en efectivo acumuladas por nombre de cliente, número de identificación fiscal o de archivo de información del cliente.

Dichos informes de filtrado, ya sea implementados mediante un sistema adquirido de software de un proveedor o mediante solicitudes de prestadores de servicios de información, mejorarán de manera significativa la capacidad de un banco de identificar y evaluar transacciones en efectivo poco habituales.

Registros de transferencias de fondos. La BSA exige que los bancos mantengan registros de transferencias de fondos de sumas de USD 3.000 y superiores. El control periódico de esta información puede asistir a los bancos en la identificación de patrones de actividades poco habituales. Generalmente, un control periódico de los registros de transferencias de fondos en bancos con poca actividad de transferencias de fondos es suficiente para identificar actividades poco habituales. Para los bancos con actividades de transferencias de fondos más significativas, la utilización de una hoja de cálculo o software de proveedores es una manera eficaz de revisar los patrones poco habituales en este tipo de actividades. La mayoría de los sistemas de software de proveedores incluyen informes de filtrado de actividades sospechosas estándar. Generalmente, estos informes se enfocan en la identificación de ciertas ubicaciones geográficas de mayor riesgo y en las transacciones de transferencias de fondos en dólares más importantes realizadas por personas y empresas. Cada banco debe establecer sus propios criterios de filtrado tanto de personas físicas como de empresas. Las transacciones de transferencias de fondos realizadas por quienes no son clientes y las pagaderas mediante presentación de identificación apropiada (PUPID) deben revisarse para identificar actividades poco habituales. Las actividades identificadas durante estas revisiones deben estar sujetas a una investigación adicional para garantizar que las actividades identificadas sean consistentes con el propósito declarado de la cuenta y las actividades esperadas. Cuando se identifican incoherencias, es posible que los bancos deban realizar una revisión global de las relaciones para determinar si se requiere un SAR.

Registros de instrumentos monetarios. La BSA exige que se registren las ventas de instrumentos monetarios. Dichos registros pueden ayudar al banco en la identificación de posibles estructuraciones de dinero a través de la adquisición de cheques de caja, cheques oficiales de bancos, giros postales o cheques de viajero en sumas de USD 3.000 a USD 10.000. Un control periódico de estos registros puede también ayudar a identificar compradores frecuentes de instrumentos monetarios y beneficiarios habituales. Las revisiones de actividades sospechosas deben incluir actividades durante un período extendido (30, 60 ó 90 días) y deben centrarse, entre otras cosas, en la identificación de concordancias, como compradores y beneficiarios habituales, o instrumentos monetarios con numeración consecutiva.

Supervisión de vigilancia (supervisión automatizada de cuentas)

Un sistema de supervisión de vigilancia, a veces denominado sistema de supervisión automatizado de cuentas, puede abarcar diversos tipos de transacciones y utilizar varias reglas para identificar posibles actividades sospechosas. Además, muchos se pueden adaptar con el tiempo según la actividad histórica, las tendencias o la comparación de pares internos. Por lo general, estos sistemas hacen uso de programas informáticos, desarrollados internamente o comprados a proveedores, para identificar transacciones particulares, patrones de actividades poco habituales o variaciones con respecto a las actividades esperadas. Estos sistemas pueden capturar un amplio rango de actividades de cuentas, como depósitos, extracciones, transferencias de fondos, transacciones de compensación automatizada (ACH) y cajeros automáticos (ATM), directamente del sistema de procesamiento de datos principal del banco. Los bancos grandes, que operan

en muchas ubicaciones o tienen un gran volumen de clientes de mayor riesgo generalmente utilizan sistemas de supervisión de vigilancia.

Los sistemas de supervisión de vigilancia incluyen sistemas inteligentes y basados en reglas. Los sistemas basados en reglas detectan transacciones poco comunes que no se incluyen en las "reglas" desarrolladas por el sistema o establecidas por la gerencia. Dichos sistemas pueden estar compuestos por pocas o muchas reglas, según la complejidad del producto desarrollado internamente o por un proveedor. Estas reglas se aplican utilizando una serie de filtros de transacciones o un motor de reglas. Los sistemas basados en reglas son más sofisticados que el sistema manual básico, que sólo filtra según una regla (p. ej., transacciones que superen los USD 10.000).
Los sistemas basados en reglas pueden aplicar reglas múltiples, reglas superpuestas y filtros más complejos. Por ejemplo, los sistemas basados en reglas pueden aplicar inicialmente una regla o un conjunto de criterios a todas las cuentas dentro de un banco (p. ej., todos los clientes minoristas) y, luego, aplicar un conjunto de criterios más refinado a un subconjunto de cuentas o a una categoría de riesgo de cuentas (p. ej., todos los clientes minoristas con depósitos directos). Los sistemas basados en reglas también pueden filtrar por perfiles de cuenta/clientes particulares.

Los sistemas inteligentes se adaptan y pueden filtrar transacciones, según la actividad histórica de cuentas, o comparar la actividad del cliente con un grupo de pares preestablecido u otros datos relevantes. Los sistemas inteligentes controlan las transacciones en contexto con otras transacciones y el perfil del cliente. Al hacer esto, estos sistemas amplían su base de datos de información sobre el cliente, tipo de cuenta, categoría o negocio, a medida que se almacenan más transacciones y datos en el sistema.

En relación con la supervisión de vigilancia, las capacidades y los umbrales del sistema se refieren a los parámetros o filtros utilizados por los bancos en sus procesos de supervisión. Los parámetros y filtros deben ser razonables y estar adaptados a la actividad que el banco está intentando identificar o controlar. Después de que los parámetros y filtros hayan sido desarrollados, se deben revisar antes de la implementación para identificar las deficiencias (fraudes o técnicas de lavado de dinero comunes) que es posible que no se hayan abordado. Por ejemplo, un banco puede descubrir que su filtro de fraccionamiento de efectivo se activa sólo por una transacción diaria de efectivo de más de USD 10.000. Es posible que el banco deba refinar su filtro para evitar pasar por alto posibles actividades sospechosas, ya que, a menudo, las técnicas de fraccionamiento de efectivo comunes implican transacciones que están apenas por debajo del umbral del CTR. Una vez que se hayan establecido, el banco debe revisar y probar las capacidades y los umbrales del sistema con regularidad. Este control debe centrarse en parámetros o filtros específicos para garantizar que la información que se tiene por objeto se capte de manera adecuada y que el parámetro o filtro sea adecuado para el perfil de riesgo particular del banco.

Comprender los criterios de filtrado de un sistema de supervisión de vigilancia es fundamental para analizar la eficacia de dicho sistema. Los criterios de filtrado del sistema deben desarrollarse mediante el control de productos, servicios, clientes, entidades y ubicaciones geográficas de mayor riesgo específicos. Los criterios de filtrado del sistema, incluidos las reglas y los perfiles específicos, se deben desarrollar en función de lo que es

razonable y se espera para cada tipo de cuenta. La supervisión de las cuentas meramente en función de la actividad histórica puede resultar engañosa si la actividad no concuerda con la de tipos similares de cuentas. Por ejemplo, una cuenta puede tener una actividad transaccional histórica que es sustancialmente diferente de lo que se esperaría normalmente de ese tipo de cuenta (p. ej., un negocio de cambio de cheques que deposita grandes sumas de dinero frente a la extracción de dinero para financiar el cambio de cheques).

La autoridad para establecer o cambiar los perfiles de actividad esperada debe definirse claramente y debe exigir generalmente la aprobación del funcionario de cumplimiento de la BSA o de la alta gerencia. Los controles deben garantizar el acceso limitado al sistema de supervisión. La gerencia debe documentar o ser capaz de explicar los criterios de filtrado, los umbrales utilizados y por qué son adecuados ambos según los riesgos del banco. La gerencia debe también revisar periódicamente los criterios de filtrado y los umbrales establecidos para garantizar que aún sean eficaces. Además, la eficacia y la metodología de programación del sistema de supervisión deben validarse de manera independiente para garantizar que los modelos detecten actividades potencialmente sospechosas.

Gestión de alertas

La gestión de alertas se centra en los procesos utilizados para investigar y evaluar actividades poco habituales identificadas. Los bancos deben tener en cuenta todos los métodos de identificación y deben garantizar que su programa de supervisión de actividades sospechosas incluya procesos para evaluar cualquier actividad poco habitual identificada, independientemente del método de identificación. Los bancos deben contar con políticas, procedimientos y procesos para notificar sobre las actividades poco habituales de todas las áreas del banco o rubros de la actividad comercial al personal o el departamento responsables de la evaluación de dichas actividades. En estos procedimientos, la gerencia debe establecer un proceso de derivación al superior definido y claro desde la detección inicial hasta la resolución de la investigación.

El banco debe asignar personal adecuado para la identificación, evaluación y elaboración de informes de posibles actividades sospechosas según el perfil de riesgo general del banco, así como el volumen de sus transacciones. Además, un banco debe garantizar que el personal asignado tenga los niveles de experiencia necesarios y reciba capacitación integral y continua para mantener su pericia técnica. También se debe proporcionar al personal herramientas internas y externas suficientes para permitirles investigar las actividades de manera adecuada y formular conclusiones.

Las herramientas de investigación internas incluyen, entre otras, acceso a sistemas de cuentas e información de cuentas, incluida la información de CDD y EDD. La información de CDD y EDD permitirá que los bancos determinen si la actividad poco habitual puede considerarse sospechosa. Para obtener más información, consulte la sección del esquema general principal, “Debida diligencia de los clientes”, en las páginas 69 a 71. Las herramientas de investigación externas pueden incluir herramientas de búsqueda de medios por Internet ampliamente disponibles, así como aquellas a las que se puede obtener acceso por suscripción. Después de una investigación y un análisis

minuciosos, los investigadores deben documentar las conclusiones, incluidas las recomendaciones respecto a si se debe o no presentar un SAR.

Cuando existen varios departamentos que son responsables de la investigación de actividades poco habituales (p. ej., el departamento BSA investiga actividades relacionadas con la BSA y el departamento Fraudes investiga actividades relacionadas con fraudes), las líneas de comunicación entre los departamentos deben permanecer abiertas. Esto permite que los bancos con procesos ramificados obtengan eficiencia al compartir información, disminuir el exceso de personal y garantizar que las actividades sospechosas se identifiquen, evalúen e informen.

Si es pertinente, el control y la comprensión de la supervisión de actividades sospechosas en la totalidad de las filiales, subsidiarias y rubros de la actividad de la organización pueden mejorar la capacidad de la organización bancaria de detectar actividades sospechosas y así minimizar las posibilidades de pérdidas financieras, aumento de gastos legales o de cumplimiento y riesgos que puedan afectar la reputación de dicha organización. Consulte la sección del esquema general ampliado, "Estructuras de programas de cumplimiento BSA/AML", en las páginas 179 a 185, como guía adicional.

Identificación de delitos subyacentes

Los bancos están obligados a informar actividades sospechosas que puedan incluir el lavado de dinero, las violaciones a la BSA, el financiamiento del terrorismo[61] y algunos otros delitos que superen el umbral en dólares establecido. Sin embargo, no se exige a los bancos que investiguen o confirmen los delitos subyacentes (p. ej., el financiamiento del terrorismo, el lavado de dinero, la evasión impositiva, el robo de identidad y varios tipos de fraude). La investigación es responsabilidad de las autoridades de aplicación de la ley pertinentes. Cuando se evalúan las actividades sospechosas y se presenta el SAR, los bancos deben hacer todo lo que esté a su alcance para identificar las características de la actividad sospechosa. La Parte III, sección 35, del SAR proporciona 20 características diferentes de actividades sospechosas. Aunque existe la categoría "Otros", la utilización de esta categoría se debe limitar a situaciones que no se pueden identificar, en líneas generales, dentro de las 20 características proporcionadas.

Toma de decisiones en relación con los SAR

En general, después de que se haya realizado la investigación y el análisis minuciosos, los resultados se reenvían a alguien que toma las decisiones finales (una persona particular o un comité). El banco debe contar con políticas, procedimientos y procesos para notificar sobre las actividades poco habituales de todos los rubros de la actividad comercial al

[61] Si un banco tiene conocimiento, sospecha o tiene motivos para sospechar que un cliente puede estar vinculado a una actividad terrorista contra los Estados Unidos, éste debe llamar inmediatamente a la Línea Gratuita de Emergencias Terroristas para Instituciones Financieras de la FinCEN: 866-556-3974. De la misma manera, si cualquier otro tipo de sospecha de violación requiere atención inmediata, como una operación de lavado de dinero que está en curso, el banco debe notificar a los entes bancarios federales y autoridades de aplicación de la ley pertinentes. En cualquier caso, el banco también debe presentar un SAR.

personal o el departamento responsables de la evaluación de dichas actividades. En estos procedimientos, la gerencia debe establecer un proceso de derivación al superior definido y claro desde la detección inicial hasta la resolución de la investigación.

Quien tome las decisiones, ya sea una persona particular o un comité, debe estar autorizado a tomar la decisión final de presentación del SAR. Cuando el banco tiene un comité, debe haber un proceso claramente definido para resolver las diferencias de opinión sobre las decisiones de presentación. Los bancos deben documentar las decisiones en relación con los SAR, incluido el motivo específico para presentar o no un SAR. La documentación minuciosa proporciona un registro del proceso de toma de decisiones en relación con los SAR, incluidas las decisiones finales de no presentar un SAR. Sin embargo, debido a la variedad de sistemas utilizados para identificar, informar y hacer un seguimiento de actividades sospechosas, así como el hecho de que cada decisión de informar actividades sospechosas se basará en circunstancias y hechos únicos, no se requiere ninguna forma de documentación cuando un banco decide no presentar un informe.[62]

La decisión de presentar un SAR es inherentemente subjetiva. Los inspectores deben enfocarse en si el banco cuenta con un proceso eficaz de toma de decisiones con respecto al SAR, y no, únicamente, decisiones individuales sobre éste. Los inspectores deben revisar las decisiones individuales con respecto al SAR para probar la eficacia de la supervisión, la generación de informes y el proceso de toma de decisiones con respecto al SAR. En los casos en que el banco haya establecido un proceso de toma de decisiones con respecto al SAR, haya seguido las políticas, los procedimientos y los procesos, y haya determinado no presentar un SAR, no deberá ser criticado por no presentar este informe a menos que la no presentación sea grave o exista evidencia de que se actuó de mala fe.[63]

Presentación de un SAR sobre actividades continuas

Uno de los propósitos de la presentación de los SAR es identificar las violaciones o las violaciones potenciales a la ley y notificar a las autoridades de aplicación para que inicien una investigación penal. Este objetivo se logra con la presentación de un SAR que identifique la actividad que causa preocupación. Si esta actividad continúa durante un período, dicha información debe notificarse a las autoridades de aplicación de la ley y a las agencias bancarias federales. Las pautas de la FinCEN sugieren que los bancos deben informar sobre las actividades sospechosas continuas mediante la presentación de un informe al menos cada 90 días.[64] Esta práctica notificará a las autoridades de aplicación

---

[62] Grupo de asesoría de la ley de secreto bancario, "Section 4 — Tips on SAR Form Preparation & Filing," *The SAR Activity Review — Trends, Tips & Issues* ("Sección 4: Sugerencias prácticas sobre la presentación y preparación del formulario del SAR", Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas), edición 10 de Mayo de 2006, en la página 38, en www.fincen.gov.

[63] Para obtener más información, consulte el Informe entre Agencias sobre el Cumplimiento (Apéndice R).

[64] Grupo de asesoría de la ley de secreto bancario, "Sección 5: temas y orientación" en *Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas*, edición 1 de Octubre de 2000, en la página 27, en www.fincen.gov.

de la ley sobre el carácter continuo de la actividad en su totalidad. Además, esta práctica hará que el banco recuerde que debe continuar controlando las actividades sospechosas para determinar si otras medidas pueden ser adecuadas, como que la gerencia del banco determine que es necesario finalizar una relación con el cliente o empleado que es el sujeto de la presentación.

Los bancos deben tener en cuenta que las autoridades de aplicación de la ley pueden estar interesadas en garantizar que ciertas cuentas permanezcan abiertas pese a que puedan estar relacionadas con actividades delictivas potenciales o sospechosas. Si una autoridad de aplicación de la ley solicita que un banco mantenga abierta una cuenta en particular, el banco debe pedir una solicitud por escrito. La solicitud por escrito debe indicar que la agencia ha solicitado que el banco mantenga abierta la cuenta, y el propósito y la duración de la solicitud. En último término, es el banco quien debe decidir si se debe mantener abierta una cuenta o se la debe cerrar, de acuerdo con sus propias pautas y normas.[65]

El banco debe desarrollar políticas, procedimientos y procesos indicando cuándo se deben derivar al superior los asuntos o problemas identificados como resultado de la presentación repetida de los SAR sobre cuentas. Los procedimientos deben incluir:

- Control por parte de la alta gerencia y el personal legal (p. ej., el funcionario de cumplimiento de la BSA o el comité del SAR).
- Criterios que establezcan cuándo es necesario un análisis de la relación general con el cliente.
- Criterios que establezcan si se debe cerrar la cuenta y, de ser así, cuándo.
- Criterios que establezcan cuándo se debe notificar a las autoridades de aplicación de la ley, si corresponde.

Realización y presentación de SAR

La realización y la presentación de SAR son una parte fundamental del proceso de supervisión y realización de informes de SAR. Se debe disponer de políticas, procedimientos y procesos adecuados para garantizar que los formularios de SAR se presenten de manera oportuna, estén completos y sean precisos, y que la descripción de la actividad informada, así como de los hechos en función de los que pueden presentarse los SAR, sea suficiente. Desde el 12 de Septiembre de 2009, los bancos que presentan SAR de manera electrónica pueden recibir de la FinCEN un Número de control del documento como acuse de recibo de un SAR presentado.[66]

---

[65] Consulte *Solicitudes de las autoridades de aplicación de la ley a las instituciones financieras sobre el mantenimiento de cuentas*, 13 de Junio de 2007, en www.fincen.gov.

[66] Para obtener más información, consulte http://fincen.gov/whatsnew/html/20090826.html.

Momento oportuno para presentar un SAR

Las reglamentaciones del SAR exigen que éste se presente antes de los 30 días calendario a partir de la fecha de la detección inicial de los hechos en función de los cuales puede presentarse un SAR. Si no se puede identificar un sospechoso, el período para presentar un SAR se extiende a 60 días. Es posible que las organizaciones necesiten revisar las transacciones o la actividad de la cuenta de un cliente para determinar si presentar o no un SAR. La necesidad de revisar la actividad o las transacciones de un cliente no indica necesariamente que se deba presentar un SAR. El plazo para presentar un SAR comienza cuando la organización, durante el control o debido a otros factores, conoce o tiene motivos para sospechar que la actividad o las transacciones que se controlan encuadran en una o más de las definiciones de actividad sospechosa.[67]

No debe interpretarse el significado de la frase "detección inicial" como el momento en que se destaca una transacción para su control. Existe una variedad de transacciones legítimas que pueden considerarse señales de advertencia simplemente porque no son consistentes con la actividad corriente de la cuenta del titular. Por ejemplo, una inversión en bienes inmuebles (compra o venta), la recepción de una herencia, o un regalo, puede causar que una cuenta tenga un crédito o débito significativo que no sea coherente con la actividad típica de cuenta. El sistema automatizado de supervisión de cuentas o el descubrimiento inicial de información del banco, como informes generados por el sistema, puede señalar la transacción; sin embargo, esto no debe considerarse como detección inicial de posibles actividades sospechosas. El período de 30 (ó 60) días no comenzará hasta que se realice un control adecuado y se tome una determinación de que la transacción que se está controlando es "sospechosa" según el significado del reglamento de SAR.[68]

Cuando sea posible, se recomienda realizar un control rápido de la transacción o la cuenta, lo que puede asistir en gran medida a las autoridades de aplicación de la ley. En cualquier caso, el control debe realizarse en un plazo razonable. Lo que constituye un "plazo razonable" variará según los hechos y las circunstancias del asunto en particular que se esté controlando y la eficacia de la supervisión, generación de informes y el proceso de toma de decisiones con respecto al SAR de cada banco. El factor clave es que un banco haya establecido procedimientos adecuados para revisar y analizar los

---

[67] Grupo de asesoría de la ley de secreto bancario, "Sección 5: temas y orientación" en *The SAR Activity Review — Trends, Tips & Issues* (Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas), edición 1 de Octubre de 2000, en la página 27, en www.fincen.gov.

[68] Grupo de asesoría de la ley de secreto bancario, "Section 5 — Issues and Guidance," *The SAR Activity Review – Trends, Tips & Issues* ("Sección 5: temas y orientación", Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas), edición 10 de Mayo de 2006, en la página 44, en www.fincen.gov. Para obtener ejemplos de cuándo es la fecha de detección inicial, consulte *Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas*, edición 14 de Octubre de 2008, página 38, en www.fincen.gov.

hechos y circunstancias identificados como potencialmente sospechosos, y que esos procedimientos estén documentados y se cumplan.[69]

En las situaciones que demanden inmediata atención, además de presentar oportunamente un SAR, un banco debe notificar de inmediato, por teléfono, a una "autoridad de aplicación de la ley pertinente" y, según sea necesario, a la agencia reguladora principal del banco. Para esta notificación inicial, una "autoridad de aplicación de la ley pertinente" generalmente será la oficina local de la División de Investigación Delictiva del Servicio del IRS o el FBI. La notificación a una autoridad de aplicación de la ley de una actividad sospechosa no exime a un banco de su obligación de presentar un SAR.[70]

Calidad del SAR

Los bancos deben presentar formularios del SAR que estén completos, sean exhaustivos y oportunos. Los bancos deben incluir toda la información conocida sobre sospechosos en el formulario del SAR. La importancia de la precisión de esta información no puede dejarse de resaltar. La información errónea introducida en el formulario del SAR, o una descripción incompleta o desorganizada, puede dificultar la realización de un más profundo análisis e incluso hacer que sea imposible. Sin embargo, pueden existir motivos legítimos por los que cierta información no se proporcione en un SAR, como ser que el responsable de la presentación del informe no cuente con ella. Una descripción completa y exhaustiva puede marcar la diferencia al determinar si las autoridades de aplicación de la ley comprenden con claridad la conducta descrita y su posible carácter delictivo. Debido a que la sección de descripción del SAR es la única área en la que se resume la actividad sospechosa, dicha sección, según lo indica el formulario del SAR, es "fundamental". De este modo, no describir de manera adecuada los factores que hacen que una transacción o actividad sea sospechosa menoscaba el propósito del SAR.

Por su carácter, las descripciones en el SAR son subjetivas y los inspectores generalmente no deben criticar la interpretación que hace el banco de los hechos. No obstante, los bancos deben garantizar que las descripciones en el SAR estén completas, describan exhaustivamente el alcance y el carácter de la actividad sospechosa y se incluyan dentro del formulario del SAR (p. ej., no se puede almacenar ningún anexo en la sección de descripción dentro del banco de datos de los informes sobre la BSA). Una guía más específica esta disponible en el Apéndice L ("Guía sobre calidad del SAR") para asistir a los bancos en la realización de las descripciones en el SAR y a los inspectores en la evaluación de las mismas. Además, la FinCEN pone a disposición una guía exhaustiva (p. ej., *Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative* [Guía sobre la preparación de una descripción completa y suficiente en el informe de actividades sospechosas], Noviembre de 2003, y *Suggestions for Addressing*

[69] Id.

[70] En caso de existir actividades sospechosas relacionadas con la actividad terrorista, las instituciones pueden llamar a la línea gratuita de emergencias terroristas para instituciones financieras de la FinCEN: 866-556-3974 (las 24 horas del día, los 7 días de la semana) para que faciliten la transmisión inmediata de información relevante a las autoridades pertinentes.

Common Errors Noted in Suspicious Activity Reporting [Sugerencias para abordar errores comunes identificados en la realización de informes sobre actividades sospechosas], Octubre de 2007) en www.fincen.gov/news_room/rp/sar_guidance.html.

Notificación a la junta directiva de la presentación de un SAR

Los reglamentos de los SAR de las agencias bancarias federales que supervisan los bancos exigen que éstos notifiquen a la junta directiva o al comité correspondiente que se han presentado los SAR. Sin embargo, los reglamentos no exigen que se utilice un formato de notificación en particular, por lo que los bancos pueden proceder a estructurar los respectivos formatos con flexibilidad. Por lo tanto, los bancos pueden proporcionar copias reales de los SAR a la junta directiva o al comité, pero no están obligados a hacerlo. Como alternativa, los bancos pueden optar por proporcionar resúmenes, tablas de los SAR presentados para tipos específicos de violaciones u otras formas de notificación. Independientemente del formato de notificación utilizado por el banco, la gerencia debe proporcionar información suficiente sobre su presentación del SAR a la junta directiva o el respectivo comité para cumplir con sus tareas fiduciarias.[71]

Conservación de registros del SAR y documentación respaldatoria

Los bancos deben conservar copias de los SAR y la documentación respaldatoria durante cinco años a partir de la fecha de presentación del SAR. Además, los bancos deben proporcionar toda la documentación respaldatoria de la presentación de un SAR cuando la FinCEN, una autoridad de aplicación de la ley pertinente o una agencia bancaria federal lo solicite. “Documentación respaldatoria” es todo documento o registro que ayudó a un banco a determinar que cierta actividad exigía la presentación de un SAR. No se exige ningún proceso legal para la divulgación de documentación respaldatoria a la FinCEN, una autoridad de aplicación de la ley pertinente o una agencia bancaria federal.[72]

Prohibición de la divulgación del SAR

Ningún banco, y ningún director, funcionario, empleado o agente de un banco, que informe acerca de una transacción sospechosa puede notificar a ninguna persona implicada en la transacción que la transacción ha sido informada. Por lo tanto, toda persona que haya sido citada legalmente o, de otro modo, intimada a divulgar un SAR o la información incluida en éste, excepto cuando la FinCEN, una autoridad de aplicación

---

[71] Como se indica en *The SAR Activity Review – Trends, Tips & Issues* (Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas) del Grupo de asesoría de la ley de secreto bancario, edición 2 de Junio de 2001, “En la inusual ocasión en la que la actividad sospechosa esté relacionada con un individuo de la organización, como el presidente o uno de los miembros de la junta directiva, no debe cumplirse con la política establecida que requeriría la notificación de la presentación de un SAR a dicho individuo. Las desviaciones de las políticas y procedimientos establecidos para evitar la notificación de la presentación de un SAR a un individuo sujeto a dicho SAR deben documentarse y notificarse al personal de mayor jerarquía de la organización que no esté involucrado”. Consulte www.fincen.gov.

[72] Consulte *Suspicious Activity Report Supporting Documentation* (Documentación respaldatoria del informe de actividades sospechosas), 13 de Junio de 2007, en www.fincen.gov.

de la ley o una agencia bancaria federal solicite dicha divulgación,[73] debe rehusarse a generar el SAR o proporcionar cualquier información que divulgaría que se ha preparado o presentado un SAR, citando 31 CFR 103.18(e) y 31 USC 5318(g)(2). Debe notificarse a la FinCEN y a la agencia bancaria federal del banco dicha solicitud y la respuesta del banco. Además, la FinCEN y las agencias bancarias federales consideran que los controles internos de los bancos para la presentación de los SAR deben minimizar los riesgos de divulgación.

Intercambio de los SAR con oficinas centrales y compañías de control

La guía que se aplica entre agencias clarifica que las organizaciones bancarias pueden compartir los SAR con oficinas centrales y compañías de control ubicadas en los Estados Unidos o en el extranjero.[74] Una compañía de control, según se define en la guía, incluye:

- Una sociedad de control de bancos (BHC, por sus siglas en inglés), como se define en la sección 2 de la ley de BHC.
- Una sociedad de control de asociaciones de ahorro y préstamo, como se define en la sección 10(a) de la Ley de Préstamos para Propietarios de Viviendas.
- Una compañía que tiene el poder, directo o indirecto, de orientar las políticas de gerencia de una compañía de préstamo industrial o una compañía matriz o que se encuentra en poder del 25 % o más de cualquier clase de acciones con derecho a voto de una compañía de préstamo industrial o una compañía matriz.

La guía confirma que:

- Una sucursal en los Estados Unidos o agencia de un banco extranjero puede compartir un SAR con su oficina central fuera de los Estados Unidos.

---

[73] Los ejemplos de las agencias a las cuales se les puede proporcionar un SAR o la información contenida en éste incluyen: los servicios de investigación delictiva de las fuerzas armadas; la Oficina de Control de Bebidas Alcohólicas, Tabaco y Armas de Fuego; un procurador general, fiscal de distrito o el fiscal del estado a nivel local o estatal; la Agencia Antinarcóticos; la Oficina Federal de Investigaciones; el Servicio de Impuestos Internos o agencias de supervisión tributaria a nivel estatal; la Oficina para el Control de Activos Extranjeros; un departamento de policía local o estatal; una Oficina del Fiscal en los Estados Unidos; Oficina de Inmigración y Aduana; el Servicio de Inspección Postal de Estados Unidos; y el Servicio Secreto Estadounidense. Para obtener más información, consulte Grupo de asesoría de la ley de secreto bancario, "Section 5—Issues and Guidance," *The SAR Activity Review—Trends, Tips & Issues* ("Sección 5: temas y orientación", Control de la actividad del SAR – Tendencias, sugerencias prácticas y temas), edición 9 de Octubre de 2005, página 44, en www.fincen.gov.

[74] *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies* (Guía aplicable entre agencias sobre el intercambio de informes de actividades sospechosas con oficinas centrales y compañías de control), expedida por la Red de Lucha contra Delitos Financieros, la Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro, el 20 de Enero de 2006.

- Un banco de los Estados Unidos puede compartir un SAR con compañías de control nacionales o extranjeras.

Los bancos deben establecer estrategias para proteger la confidencialidad de los SAR. La guía no menciona si un banco puede compartir un SAR con una filial que no sea una compañía de control o una oficina central. Sin embargo, para gestionar los riesgos de toda la organización, los bancos que presentan un SAR pueden divulgar a entidades dentro de su organización la información subyacente a la presentación de un SAR.

Procedimientos de Inspección

Presentación de informes de actividades sospechosas

Objetivo: *Evaluar las políticas, los procedimientos y los procesos del banco, y el cumplimiento general de las exigencias normativas y legales para la supervisión, la detección y la elaboración de informes sobre actividades sospechosas.*

Al principio, los inspectores pueden decidir establecer qué proceso sigue el banco para revisar, identificar, investigar e informar actividades sospechosas. Una vez que el inspector comprenda el proceso, debe seguir una alerta durante todo el proceso.

Identificación de actividades poco habituales

1. Revise las políticas, los procedimientos y los procesos del banco para identificar, investigar y elaborar informes sobre actividades sospechosas. Determine si incluyen lo siguiente:

   - Líneas de comunicación para la remisión de actividades poco habituales al personal apropiado.
   - Designación del individuo o los individuos responsables de identificar, investigar e informar sobre actividades sospechosas.
   - Sistemas de supervisión utilizados para identificar actividades poco habituales.
   - Procedimientos para revisar y evaluar la actividad transaccional de personas incluidas en las solicitudes de las autoridades de aplicación de la ley (p. ej., citaciones de jurados de acusación, solicitudes según la sección 314(a) o Cartas de Seguridad Nacional [NSL]) sobre actividades sospechosas. Las NSL son documentos sumamente confidenciales y, como tales, los inspectores no revisarán ni tomarán muestras de cartas específicas. En cambio, los inspectores deben evaluar las políticas, los procedimientos y los procesos para:

     – Responder a las NSL.

     – Evaluar la cuenta para identificar actividades sospechosas.

     – Presentar SAR, si fuera necesario.

     – Gestionar cierres de cuentas.

2. Revise los sistemas de supervisión del banco y la manera en que el sistema o los sistemas se adaptan al proceso general de supervisión e informe de las actividades sospechosas del banco. Realice los procedimientos de inspección adecuados que siguen. Cuando evalúen la eficacia de los sistemas de supervisión del banco, los inspectores deben considerar el perfil de riesgo general del banco (productos,

servicios, clientes, entidades y ubicaciones geográficas de mayor riesgo), el volumen de transacciones y la aptitud del personal.

Supervisión (manual) de transacciones

3. Revise los informes de supervisión de las transacciones del banco. Determine si los informes incluyen todas las áreas que plantean riesgos de lavado de dinero y financiamiento del terrorismo. Los ejemplos de estos informes incluyen: informes sobre actividades en efectivo, informes de transferencias de fondos, informes de ventas de instrumentos monetarios, informes de artículos significativos, informes de cambios significativos en el balance e informes de fondos insuficientes (NSF) e informes de extranjeros no residentes (NRA).

4. Determine si los sistemas de supervisión de transacciones del banco utilizan criterios razonables de filtrado cuya programación haya sido verificada de manera independiente. Determine si los sistemas de supervisión generan informes adecuados con una frecuencia razonable.

Supervisión (automatizada de cuentas) de vigilancia

5. Identifique los tipos de clientes, productos y servicios que estén incluidos dentro del sistema de supervisión de vigilancia.

6. Identifique la metodología del sistema para el establecimiento y la aplicación de criterios de actividades previstas o de filtrado de perfiles y para generar informes de supervisión. Determine si los criterios de filtrado del sistema son razonables.

7. Determine si la programación de la metodología ha sido validada de manera independiente.

8. Determine que los controles garantizan el acceso limitado a los sistemas de supervisión, así como la suficiente supervisión de los cambios en las presunciones.

Gestión de alertas

9. Determine si el banco cuenta con políticas, procedimientos y procesos para garantizar la generación oportuna, el control y la respuesta a los informes utilizados para identificar actividades poco habituales.

10. Determine si las políticas, los procedimientos y los procesos exigen una investigación apropiada cuando los informes de supervisión identifican actividades poco habituales.

11. Evalúe las políticas, los procedimientos y los procesos del banco para notificar sobre las actividades poco habituales de todos los rubros de la actividad comercial al personal o el departamento responsables de la evaluación de dichas actividades. El proceso debe garantizar que toda información pertinente (p. ej., las citaciones penales, las NSL y las solicitudes según la sección 314(a)) sea evaluada de manera eficaz.

12. Verifique que los niveles de personal sean suficientes para revisar informes y alertas e investigar elementos, y que el personal tenga el nivel de experiencia necesario y las

herramientas de investigación adecuadas. El volumen de las investigaciones y las alertas del sistema no se debe adaptar sólo para satisfacer los niveles de personal existentes.

13. Determine si el proceso de toma de decisiones del banco con respecto a los SAR tiene en cuenta toda la información disponible de CDD y EDD.

Toma de decisiones en relación con los SAR

14. Determine si las políticas, los procedimientos y los procesos del banco incluyen procedimientos para:

    - Documentar decisiones de no presentar un SAR.
    - Derivar problemas identificados como resultado de la repetición de presentaciones de SAR por varias cuentas.
    - Considerar el cierre de cuentas como consecuencia de actividades sospechosas continuas.

Realización y presentación de SAR

15. Determine si las políticas, los procedimientos y los procesos del banco permiten:

    - Realizar, presentar y conservar los SAR y su documentación respaldatoria.
    - Notificar los informes SAR a la junta directiva, o a un comité de dicha junta, y a la alta gerencia.
    - Compartir los SAR con las oficinas centrales y las compañías de control, según sea necesario.

Pruebas de transacciones

Las pruebas de transacciones de los sistemas de supervisión de actividades sospechosas y los procesos de elaboración de informes están destinadas a determinar si las políticas, los procedimientos y los procesos del banco están implementados de manera apropiada y eficaz. Los investigadores deben documentar los factores que utilizaron para seleccionar muestras y deben realizar una lista de las cuentas de las que sirvieron de muestra. El tamaño y la muestra deben basarse en lo siguiente:

- Las debilidades en los sistemas de supervisión de cuentas.
- El perfil de riesgo BSA/AML general del banco (p. ej., número y tipo de productos, servicios, clientes, entidades y ubicaciones geográficas de mayor riesgo).
- La calidad y el alcance del control realizado por medio de auditorías o terceros independientes.
- Los resultados de inspecciones previas.

- Las fusiones recientes, adquisiciones u otros cambios importantes en la organización.
- Las conclusiones o preguntas del control de los informes SAR del banco.

Consulte el Apéndice O ("Herramientas del inspector para las pruebas de transacciones"), como guía adicional.

16. En función de un análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de cuentas de clientes determinados para revisar lo siguiente:
    - Informes de supervisión de actividades sospechosas.
    - Información descargada sobre informes CTR.
    - Operaciones bancarias de mayor riesgo (productos, servicios, clientes, entidades y ubicaciones geográficas).
    - Actividad del cliente.
    - Citaciones recibidas por el banco.
    - Decisiones de no presentar un SAR.
17. Para los clientes seleccionados previamente, obtenga la siguiente información, si es pertinente:
    - CIP y documentación sobre la apertura de cuentas.
    - Documentación de CDD.
    - Estados financieros de dos o tres meses que cubran la relación total con el cliente y muestren todas las transacciones.
    - Puntos de la muestra comparados con la cuenta (p. ej., copias de los cheques depositados y escritos, tickets de crédito o débito, y beneficiarios y realizadores de transferencias de fondos.
    - Otra información relevante, como archivos de préstamos y correspondencia.
18. Revise las cuentas seleccionadas para detectar actividades inusuales . Si el inspector identifica actividad unusual, revise la información del cliente para verificar si dicha actividad es habitual en él (p. ej., el tipo de actividad en la que se espera que participe el cliente normalmente). Cuando se realice un control para detectar actividades poco habituales, considere lo siguiente:
    - Para clientes particulares, si la actividad es coherente con la información de CDD (p. ej., ocupación, actividad prevista de la cuenta, y origen de los fondos y de la riqueza).

- Para clientes comerciales, si la actividad es coherente con la información de CDD (p. ej., tipo de actividad comercial, tamaño, ubicación y mercado objetivo).

19. Determine si el sistema de supervisión, ya sea de transacciones o de vigilancia, de actividades sospechosas detectó la actividad que el inspector identificó como poco común.

20. Para las transacciones identificadas como poco habituales, trate dichas transacciones con la gerencia. Determine si el funcionario de la cuenta tiene conocimiento del cliente y de las transacciones poco habituales. Luego de inspeccionar los hechos disponibles, determine si la gerencia le encuentra una explicación razonable a las transacciones.

21. Determine si el banco ha fallado al identificar alguna actividad sospechosa declarable.

22. A partir de los resultados de la muestra, determine si el sistema de supervisión, ya sea de transacciones o de vigilancia, de actividades sospechosas detecta actividades sospechosas o poco habituales de manera efectiva. Identifique la causa subyacente de cualquier deficiencia en los sistemas de supervisión (p. ej., filtros poco apropiados, análisis de riesgos insuficiente o toma de decisiones inadecuada).

23. En función de un análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de las decisiones de la gerencia respecto a la investigación para determinar lo siguiente:

    - Si las decisiones de la gerencia de presentar o no presentar un informe SAR están respaldadas y son razonables.
    - Si la documentación es adecuada.
    - Si el proceso de decisión se realizó y los informes SAR son presentados de manera oportuna.

24. En función del análisis de riesgos, los informes de inspección anteriores y un control de los resultados de la auditoría del banco, tome una muestra de los SAR descargados del banco de datos de los informes sobre la BSA o los registros de los informes SAR internos del banco. Revise la calidad del contenido del SAR para analizar a lo siguiente:

    - Si los informes SAR contienen información precisa.
    - Si las descripciones en el SAR son completas y exhaustivas, y explican de manera clara la razón por la cual la actividad es considerada sospechosa.
    - Si las descripciones en el SAR del banco de datos de los informes sobre la BSA están en blanco o contienen frases como “vea el anexo”, asegurarse de que el banco no esté enviando anexos al Centro de Cómputo Empresarial de Detroit del IRS (anteriormente el Centro de Cómputos de Detroit).[75]

[75] La línea gratuita del Centro de Cómputo Empresarial de Detroit del IRS es 800-800-2877.

25. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos de cumplir con las exigencias normativas asociadas con la supervisión, detección e informe de actividades sospechosas.

Informe de Transacciones en Efectivo: Esquema General

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para el informe de transacciones de grandes volúmenes de moneda.*

Todo banco debe elaborar un Informe de transacciones de dinero (CTR) (Formulario 104 de la FinCEN) [76] (depósito, extracción, intercambio u otros pagos o transferencias) de más de USD 10.000 efectuado por el banco, a través del banco o dirigido a éste. No es necesario informar algunas transacciones en moneda, como las que incluyen a "personas exentas", agrupación que puede incluir a clientes minoristas o comerciales que cumplen con ciertos criterios específicos fijados para la exención. Consulte la sección del esquema general, "Exenciones al informe de transacciones en efectivo", en las páginas 100 a 105, como guía.

Acumulación de transacciones en efectivo

Cuando en un mismo día hábil se realizan múltiples transacciones en efectivo por un valor superior a los USD 10.000, éstas deben ser tratadas como si fueran una sola transacción, si el banco sabe que han sido realizadas por una misma persona o en nombre de ésta. Para determinar las transacciones múltiples es necesario acumular las transacciones realizadas en todo el banco. Los tipos de transacciones en efectivo que están sujetos a requisitos de informe, tanto individualmente como por acumulación, incluyen los siguientes, sin limitarse únicamente a ellos: cuentas individuales de retiro (IRA, por sus siglas en inglés), pagos de préstamos, transacciones efectuadas en cajeros automáticos (ATM), compras de certificados de depósito, depósitos y extracciones, transferencias de fondos pagadas en efectivo y compras de instrumentos monetarios. Se considera altamente recomendable que los bancos desarrollen sistemas que les permitan acumular transacciones en efectivo de toda la entidad. La gerencia debe asegurarse de que exista un sistema que permita informar de manera adecuada las transacciones en efectivo que están sujetas a las exigencias fijadas por la BSA.

Exigencias sobre el plazo de presentación y la conservación de registros

El Informe de transacciones en efectivo (CTR) debe presentarse ante la FinCEN dentro de los 15 días siguientes a la fecha de la transacción (25 días si se presenta en forma electrónica). El banco debe conservar copias de los CTR durante cinco años a partir de la fecha del informe (31 CFR 103.27 (a)(3)).

---

[76] "Moneda" significa el dinero en forma de monedas y billetes de los Estados Unidos o de cualquier otro país, siempre y cuando sea aceptado normalmente como dinero en el país que lo emitió.

Registro de CTR anteriores

Si un banco no ha presentado informes CTR sobre transacciones declarables, debe iniciar la presentación de estos y comunicarse con el Centro de Cómputo Empresarial de Detroit del IRS (anteriormente el Centro de Cómputos de Detroit)[77] para solicitar una determinación sobre la necesidad de presentar o no transacciones previas no declaradas.

[77] La línea gratuita del Centro de Cómputo Empresarial de Detroit del IRS es 800-800-2877.

Procedimientos de Inspección

Informe de transacciones en efectivo

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para el informe de transacciones de grandes volúmenes de moneda.*

1. Determine si las políticas, los procedimientos y los procesos del banco tratan de manera adecuada la preparación, presentación y conservación del CTR (Formulario 104 de la FinCEN).

2. Revise la correspondencia que el banco ha recibido del Centro de Cómputo Empresarial de Detroit del Servicio de Impuestos Internos (IRS) (anteriormente el Centro de Cómputos de Detroit) relacionada con los informes CTR incorrectos o incompletos (errores). Determine si la gerencia ha adoptado acciones correctivas, cuando sea necesario.

3. Revise el sistema de transacciones en efectivo (p. ej., cómo el banco identifica las transacciones que requieren la presentación de un CTR). Determine si el banco acumula todas o algunas transacciones en efectivo dentro del banco. Determine si el banco acumula transacciones por número de identificación fiscal (TIN), número de identificación fiscal individual (ITIN) o número de archivo de información del cliente (CIF). Además, evalúe cómo se presentan los informes CTR de los clientes que no tienen TIN o EIN.

Pruebas de transacciones

4. En función de un análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de los informes CTR presentados (copia impresa o de archivos realizados por computadora) para determinar si:

   - Los informes CTR están realizados según las instrucciones de la FinCEN.

   - Los CTR se presentaron para las transacciones de grandes volúmenes de moneda que fueron identificadas por medio de pruebas del comprobante de dinero en efectivo del cajero, sistemas automatizados de transacciones de grandes volúmenes de moneda u otros tipos de sistemas de acumulación que cubran todas las áreas significativas del banco, a menos que exista una exención al cliente.

   - Los informes CTR se realizaron y presentaron ante la FinCEN dentro de los 15 días siguientes a la fecha de la transacción (25 días si se presentaron en forma electrónica).

   - Las pruebas independientes del banco confirman la integridad y la precisión de los MIS utilizados para acumular transacciones en efectivo. Si no es así, el inspector debe confirmar la integridad y precisión de MIS. El control del

inspector debe confirmar que los cajeros no poseen la capacidad de anular los sistemas de acumulación de efectivo.

- Existen discrepancias entre los registros de CTR del banco y los CTR reflejados en la descarga del banco de datos de los informes sobre la BSA.
- El banco conserva copias de los CTR durante cinco años a partir de la fecha del informe (31 CFR 103.27 (a)(3)).

5. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos para cumplir con las exigencias normativas asociadas con el informe de transacciones en efectivo.

Exenciones al Informe de Transacciones en Efectivo: Esquema General

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para las exenciones a las exigencias del informe de transacciones en efectivo.*

Históricamente, los reglamentos del Tesoro de los Estados Unidos han reconocido el hecho de que la elaboración rutinaria de ciertos tipos de informes de transacciones de grandes volúmenes de moneda no necesariamente ayuda a las autoridades de aplicación de la ley y puede generar cargas poco razonables a los bancos. Por consiguiente, es posible que los bancos eximan a ciertos tipos de clientes de la necesidad de informar las transacciones en efectivo.

La Ley de Supresión del Lavado de Dinero de 1994 (MLSA) estableció un proceso de exención de dos fases. Bajo las exenciones de la Fase I, quedan exentas las transacciones en efectivo realizadas por bancos, oficinas y agencias gubernamentales, y empresas de suscripción pública que coticen en bolsa de valores y las subsidiarias de las mismas. Bajo las exenciones de la Fase II, quedan exentas las transacciones en efectivo realizadas por empresas más pequeñas que cumplen con ciertos criterios fijados por los reglamentos de la FinCEN.

El 5 de Diciembre de 2008, FinCEN expidió una enmienda para las reglas que rigen las exenciones del Informe de transacciones de dinero (CTR, por sus siglas en inglés)[78] Las enmiendas, entre otras cosas, eliminaron las exigencias de la designación inicial y el control anual para determinados clientes de Fase I, la exigencia de presentación bienal para los clientes exentos de Fase II y eliminó el período de espera para exentar a clientes de Fase II elegibles de otra manera al adoptar un enfoque en función del riesgo para exentar a esos clientes. El siguiente análisis refleja las exigencias normativas actualizadas.

Exenciones al CTR de Fase I (31 CFR 103.22(d)(2)(i)–(v))

Las normas de FinCEN identifican cinco categorías de entidades exentas en la Fase I:

- Los bancos, hasta donde sea pertinente según el alcance de sus operaciones nacionales.
- Las agencias o departamentos gubernamentales federales, estatales o locales.
- Cualquier entidad que ejerza autoridad gubernamental en los Estados Unidos.
- Cualquier entidad (que no sea un banco) cuyas acciones comunes o participación accionaria análoga se coticen en las bolsas de valores de Nueva York o de los Estados

[78] Consulte 73 FR 74010 (Diciembre 5, 2008).

Unidos, o hayan sido designadas como Seguridad del Mercado Nacional de NASDAQ cotizadas en la bolsa del Mercado de Acciones de NASDAQ (con algunas excepciones).

- Cualquier subsidiaria (que no sea un banco) de cualquier "entidad que cotice en bolsa", se rija bajo las leyes de Estados Unidos y cuyas acciones comunes o participación accionaria análoga sean como mínimo un 51% de propiedad de la entidad que cotiza en bolsa.

Plazo de presentación

Los bancos deben presentar un formulario de Designación de persona exenta (Formulario 110 de la FinCEN) para exentar a cada empresa de suscripción pública que cotice en bolsa de valores o subsidiaria elegible del informe de transacciones en efectivo. El formulario se debe presentar ante el Servicio de Impuestos Internos (IRS, por sus siglas en inglés) durante los 30 días siguientes a la realización de la primera transacción en efectivo que el banco desea exentar.

No es necesario que los bancos presenten un formulario de Designación de persona exenta para clientes elegibles de Fase I que sean bancos, gobiernos federales, estatales o locales o entidades que ejerzan autoridad gubernamental. Sin embargo, un banco debe tomar las mismas medidas para asegurarse la elegibilidad inicial del cliente para la exención, y documentar la base para la conclusión, que un banco razonable y prudente tomaría para protegerse de préstamos u otro fraude o pérdida basados en la identificación errónea del estado de una persona. La exención de la entidad de Fase I cubre todas las transacciones realizadas en efectivo con la entidad exenta, y no sólo las transacciones en efectivo realizadas a través de una cuenta.

Control anual

Al menos una vez al año, el banco debe revisar y verificar la información que sustenta las designaciones de empresas de suscripción pública que coticen en bolsa o subsidiarias como exentas de Fase I. Para documentar el control, se pueden utilizar informes anuales, los valores de las acciones que cotizan en bolsa obtenidos de periódicos u otra información, como medios de comunicación electrónicos. No es necesario que los bancos confirmen la elegibilidad continua para la exención de los clientes de Fase I que son bancos, agencias gubernamentales o entidades que ejercen autoridad gubernamental.

Exenciones al CTR de Fase II (31 CFR 103.22(d)(2) (vi)–(vii))

Las empresas que no encuadran en ninguna de las categorías de la Fase I pueden estar exentas bajo la Fase II si califican como "empresas no enlistadas" o como "clientes que pagan nómina".

Empresas no enlistadas

Una "empresa no enlistada" se define como una empresa comercial, según el alcance de sus operaciones nacionales y únicamente con respecto a las transacciones realizadas a través de sus cuentas exentas, que: (i) ha mantenido una cuenta de transacción en el banco que realiza exención durante al menos dos meses o antes de que transcurra el período de dos meses si el banco realiza un análisis basado en el riesgo de ese cliente que le permita formar y documentar una convicción razonable de que el cliente tiene un propósito comercial legítimo para llevar a cabo transacciones de grandes volúmenes de dinero con frecuencia; (ii) con frecuencia[79] efectúa transacciones en efectivo con el banco por un valor superior a USD 10.000; y (iii) ha sido constituida u organizada bajo las leyes de los Estados Unidos o de algún estado de los Estados Unidos, o está registrada y es elegible para realizar negocios en ese país o un estado de éste.

Empresas que no califican

Ciertas empresas no son elegibles para ser consideradas empresas no elistadas exentas (31 CFR 103.22(d)(5)(viii)). Dichas empresas no elegibles se definen como empresas dedicadas principalmente a una o más de las siguientes actividades específicas:

- Servir como institución financiera o agente de una institución financiera de cualquier tipo.
- Compraventa de vehículos automotores de cualquier tipo, así como de embarcaciones, aviones, maquinaria agrícola o casas móviles.
- Ejercicio del derecho, la contabilidad o la medicina.
- Subasta de bienes.
- Alquiler o manejo de embarcaciones, autobuses o aviones.
- Prestación de servicios de intermediación de casas de empeño.
- Participación en cualquier clase de juego de azar (que no sean apuestas "pari-mutuel" licenciadas realizadas en pistas de carreras).
- Participación en servicios de asesoría sobre inversiones o servicios de banca de inversión.
- Prestación de servicios de intermediación en operaciones relacionadas con bienes inmuebles.
- Participación en actividades relacionadas con títulos de seguros y cierre de operaciones que impliquen bienes inmuebles.

[79] FinCEN ha observado que, para fines de 31 CFR 103.22(d)(2)(vi)(B): "[los bancos] pueden designar a un cliente elegible de alguna otra forma para la exención de la Fase II después de que el cliente haya llevado a cabo, en el transcurso de un año, cinco o más transacciones de efectivo declarables." Consulte 73 FR 74010, 74014 (5 de Diciembre de 2008).

- Participación en actividades realizadas por sindicatos.
- Participación en cualquier otra actividad que pueda ocasionalmente indicar la FinCEN.

Las entidades que realicen múltiples actividades de negocios pueden calificar para la exención como empresas no enlistadas, siempre y cuando más del 50% de sus ingresos brutos anuales[80] se deriven de una o más de las actividades comerciales no elegibles enumeradas en la normativa.

Un banco debe considerar y mantener materiales u otra información de respaldo que le permita corroborar que la decisión de exentar al cliente del informe de transacciones en efectivo se basó en una determinación razonable de que el cliente deriva no más del 50% de sus ingresos brutos anuales de actividades comerciales no elegibles. Dicha determinación razonable se debe basar en el entendimiento del carácter del negocio del cliente, el propósito de las cuentas del cliente y la actividad real o anticipada en esas cuentas.[81]

Clientes que pagan nómina

Los "clientes que pagan nómina" se definen únicamente con respecto a las extracciones realizadas para pagar la nómina desde cuentas existentes cubiertas por la exención y son personas que: (i) han mantenido una cuenta de transacción en el banco que realiza exención durante al menos dos meses o antes de que transcurra el período de dos meses si el banco realiza un análisis basado en el riesgo de ese cliente que le permita formar y documentar una convicción razonable de que el cliente tiene un propósito comercial legítimo para llevar a cabo transacciones de grandes volúmenes de dinero con frecuencia; (ii) operan empresas que regularmente realizan extracciones por más de USD 10.000 para pagar a sus empleados de los Estados Unidos en esa moneda; y (iii) han sido constituidas u organizadas bajo las leyes de los Estados Unidos o de algún estado de los Estados Unidos, o está registrada y es elegible para realizar negocios en ese país o un estado de éste.

---

[80] Con frecuencia surgen interrogantes en la determinación de los "ingresos brutos" de las actividades de juego de azar, tales como las ventas de lotería. La FinCEN ha establecido que para los fines de determinar si un negocio deriva más del 50% de sus ingresos brutos provenientes de actividades de juego de azar, el término ingresos brutos incluye el monto de dinero realmente obtenido como ingresos por un negocio a través de una actividad particular, en lugar del volumen de ventas de las actividades realizadas por el negocio. Por ejemplo, si un negocio participa en ventas de lotería, los "ingresos brutos" derivados de esta actividad serían el monto de dinero que ese negocio realmente obtiene de las ventas de lotería, en lugar del monto de dinero que obtiene en nombre del sistema de lotería del Estado o destinado al mismo. Consulte el Dictamen FinCEN 2002-1, www.fincen.gov.

[81] Para obtener información adicional, consulte Guidance on Supporting Information Suitable for Determining the Portion of a Business Customer's Annual Gross Revenues that is Derived from Activities Ineligible for Exemption from Currency Transaction Reporting Requirements (Guía sobre información de respaldo adecuada para determinar la parte de los ingresos brutos anuales del cliente de un negocio que deriva de actividades que no califican para la exención de las exigencias para la generación de informes de transacciones de moneda) (FIN-2009-G001) (27 de Abril de 2009), en www.fincen.gov.

Plazo de presentación

Luego de decidir exentar a un cliente de Fase II, el banco debe presentar un formulario de designación de persona exenta ante el IRS en el transcurso de los 30 días siguientes a la realización de la primera transacción en efectivo que el banco planea exentar.

Control anual

Al menos una vez al año el banco deberá revisar y verificar la información que sustenta cada designación de persona exenta de Fase II. El banco debe documentar el control anual. Por otra parte, para ser coherente con este control anual, el banco debe revisar y verificar cuando menos anualmente que la gerencia efectivamente supervise las cuentas de Fase II para la detección de transacciones sospechosas.

Protección legal contra la no presentación de los CTR

Las normas (31 CFR 103.22(d)(7)) proporcionan una protección legal al determinar que un banco no se hará responsable por no presentar un CTR debido a una transacción en efectivo por parte de un cliente exento, a menos que el banco proporcione deliberadamente información falsa o incompleta o tenga motivos para creer que el cliente no cumple con los requisitos para ser considerado un cliente exento. Si no se tiene conocimiento o información específica que indique que un cliente ya no cumple con los requisitos para ser considerado exento, el banco tiene derecho a una protección legal contra sanciones civiles en la medida que continúe tratando al cliente como exento hasta la fecha en que se realice el control anual de clientes.

Efecto sobre otras exigencias normativas

Los procedimientos de exención no tienen efecto alguno en la exigencia que tienen los bancos de presentar los Informes de Actividades Sospechosas (SAR, por sus siglas en inglés) o en las exigencias con respecto a la gestión de otros registros. Por ejemplo, el hecho de que un cliente sea una persona exenta no tiene efecto alguno en la obligación de un banco de conservar los registros de transferencias de fondos de dicho cliente, o de conservar los registros relacionados con la venta de instrumentos monetarios a dicho cliente.

Si un banco ha otorgado exenciones a cuentas de manera inadecuada, puede revocar dichas exenciones formalmente mediante la presentación del Formulario 110 de la FinCEN y marcar el cuadro “Exención revocada” o revocar informalmente la exención mediante la presentación de CTR del cliente. En cualquier caso, el banco debe iniciar la presentación de los CTR y comunicarse con el Centro de Cómputo Empresarial de Detroit del IRS (anteriormente conocido como el Centro de Cómputos de Detroit)[82] para solicitar una determinación sobre la necesidad de presentar o no el informe de las transacciones en efectivo previas no declaradas.

[82] La línea gratuita del Centro de Cómputo Empresarial de Detroit del IRS es 800-800-2877.

Se puede encontrar más información sobre el proceso de exención de transacciones en efectivo en el sitio web de FinCEN en www.fincen.gov.

Procedimientos de Inspección

Exenciones al informe de transacciones en efectivo

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para las exenciones a las exigencias del informe de transacciones en efectivo.*

1. Determine si el banco hace uso del proceso de exención del Informe de transacciones en efectivo (CTR). Si lo utiliza, determine si las políticas, los procedimientos y los procesos de las exenciones del CTR son adecuadas.

Exenciones de fase I (31 CFR 103.22(d)(2)(i)–(v))

2. Determine si el banco presenta el formulario de Designación de persona exenta (Formulario 110 de la FinCEN) en el IRS para exentar, según sean elegibles, a empresas de suscripción pública que coticen en bolsa y sus subsidiarias de la presentación de un CTR, según se define en 31 CFR 103.22. El formulario debe presentarse dentro de los 30 días a partir de la primera transacción declarable a la que se le otorgó la exención.

3. Analice si se implementa una diligencia continua, debida y razonable, incluidos los controles anuales exigidos para determinar si una empresa de suscripción pública que cotice en bolsa o subsidiaria continúa siendo elegible para ser considerada exenta bajo las exigencias normativas. La gerencia debe documentar de manera adecuada las determinaciones sobre exención (p. ej., con el valor actual de las acciones en la bolsa de valores obtenido de periódicos y la cantidad de cheques rechazados consolidados de la entidad).

Exenciones de fase II (31 CFR 103.22(d)(2)(vi)–(vii))

Según el reglamento, la definición de persona exenta incluye las "empresas no enlistadas" y los "clientes que pagan nómina", según se define en 31 CFR 103.22(d)(2)(vi)–(vii). No obstante, varias empresas continúan sin cumplir con los requisitos para la exención; consulte 31 CFR 103.22(d)(5)(viii) y la sección del esquema general "Exenciones al informe de transacciones en efectivo" de este manual.

4. Determine si el banco presenta el formulario de Designación de persona exenta ante el IRS para exentar a un cliente, según lo identifique la gerencia, de la presentación de un CTR.

5. Determine si el banco mantiene documentación para respaldar que las "empresas no enlistadas" que ha designado como exentas de la presentación de un CTR no reciban más del 50% de los ingresos brutos de actividades comerciales que no cumplen con los requisitos.

6. Analice si se implementa debida diligencia continua y razonablemente, incluidos los controles anuales exigidos para determinar si un cliente cumple con los requisitos

para ser considerado persona exenta de la presentación de un CTR. Los clientes deben cumplir con los siguientes requisitos para la exención según el reglamento:

- Efectuar transacciones en efectivo frecuentes[83] que superen los USD 10.000 (en el caso de los clientes que pagan nómina, las extracciones regulares para pagar en moneda a los empleados nacionales).
- Haberse incorporado u organizado bajo las leyes de los Estados Unidos o un estado de los Estados Unidos, o estar registrado y cumplir con los requisitos para hacer negocios dentro de los Estados Unidos o uno de sus estados.
- Mantener una cuenta de transacciones en el banco durante al menos dos meses (o antes de que transcurra el período de dos meses si el banco ha realizado un análisis basado en el riesgo de ese cliente que le permita formar y documentar una convicción razonable de que el cliente tiene un propósito comercial legítimo para llevar a cabo transacciones de grandes volúmenes de dinero con frecuencia).

Pruebas de transacciones

7. En función del análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de formularios de Designación de persona exenta del banco para comprobar el cumplimiento con las exigencias normativas (p. ej., sólo se exentan las empresas que cumplen con los requisitos, y se mantiene una documentación de respaldo adecuada).
8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos para cumplir con las exigencias normativas asociadas con las exenciones al informe de transacciones en efectivo.

---

[83] FinCEN ha observado que, al interpretar la frase "con frecuencia" para fines de 31 CFR 103.22(d)(2)(vi)(B): "[los bancos] pueden designar un cliente elegible de alguna otra forma para la exención de la Fase II después de que el cliente haya llevado a cabo, en el transcurso de un año, cinco o más transacciones de efectivo declarables." Consulte 73 FR 74010, 74014 (5 de Diciembre de 2008).

Intercambio de Información: Esquema General

Objetivo: *Evaluar el cumplimiento de la institución financiera con las exigencias normativas y legales para los "Procedimientos Especiales de Intercambio de Información para Impedir las Actividades Terroristas y de Lavado de Dinero" (Solicitudes de información según la sección 314).*

El 26 de Septiembre de 2002, entraron en vigencia los reglamentos definitivos (31 CFR 103.100 y 31 CFR 103.110) que implementaban la sección 314 de la Ley PATRIOTA de EE. UU. Los reglamentos establecieron procedimientos para el intercambio de información para impedir las actividades terroristas y de lavado de dinero. El 5 de Febrero de 2010, FinCEN enmendó los reglamentos para permitir a las agencias de aplicación de la ley estatales, locales y a determinadas agencias de aplicación de la ley extranjeras acceder al programa de intercambio de información.[84]

Intercambio de información entre las autoridades de aplicación de la ley y las instituciones financieras: Sección 314(a) de la Ley PATRIOTA de EE. UU. (31 CFR 103.100)

Una agencia federal, local o extranjera[85] de aplicación de la ley que investiga actividades terroristas y de lavado de dinero puede pedir que la FinCEN solicite, en su nombre, cierta información de una institución financiera o un grupo de instituciones financieras. La agencia de aplicación de la ley debe proporcionar una certificación por escrito a la FinCEN avalando que existe evidencia creíble de participación o sospecha fundada de participación en actividades terroristas y de lavado de dinero respecto a cada persona física, entidad u organización sobre la cual la agencia de aplicación de la ley está recabando información. La agencia de aplicación de la ley también debe proporcionar identificadores específicos, como la fecha de nacimiento y el domicilio, que permitirían que una institución financiera se diferencie entre nombres comunes o similares. Al recibir una certificación por escrito completa de parte una agencia de aplicación de la ley, la FinCEN puede exigir que una institución financiera realice una búsqueda en sus registros para determinar si mantiene o ha mantenido cuentas para cualquier persona física, entidad u organización específica, o ha participado en transacciones con cualquiera de los mismos.

---

[84] Consulte 75 FR 6560 (Febrero 10, 2010).

[85] Una agencia extranjera de aplicación de la ley debe proceder de una jurisdicción que sea parte del Acuerdo de Asistencia Jurídica Mutua entre los Estados Unidos y la Unión Europea. Íd. en 6560-61.

Exigencias sobre la búsqueda

Al recibir una solicitud de información,[86] una institución financiera debe realizar una búsqueda única en sus registros para identificar las cuentas o transacciones de la persona identificada como sospechosa. A menos que se establezca lo contrario en una solicitud de información, las instituciones financieras deben realizar una búsqueda en sus registros para verificar las cuentas actuales, las mantenidas durante los 12 meses precedentes y las transacciones efectuadas fuera de una cuenta por la persona identificada como sospechosa o en nombre de ésta durante los seis meses precedentes. La institución financiera debe realizar una búsqueda en sus registros e informar a la FinCEN de cualquier coincidencia positiva dentro de los 14 días, a menos que se especifique lo contrario en la solicitud de información.

En marzo de 2005, la FinCEN comenzó a publicar listas de sospechosos según la sección 314(a) a través del Sistema seguro de intercambio de información de 314(a) basado en la Web. Cada dos semanas, o con más frecuencia si se envía una solicitud de emergencia, los puntos de contacto designados por la institución financiera recibirán notificaciones de la FinCEN sobre las nuevas publicaciones en el sitio web seguro de la FinCEN. El punto de contacto podrá acceder a la lista de sospechosos según la sección 314(a) actual (y a una anterior) y descargar los archivos en varios formatos para realizar búsquedas. Las instituciones financieras deben informar acerca de todas las coincidencias positivas a través del Sistema seguro de intercambio de información (SISS, por sus siglas en inglés). A partir del 2 de Junio de 2008, FinCEN ha suspendido la transmisión vía fax de las listas de sospechosos según la sección 314(a) a instituciones financieras. Las instituciones financieras a las que FinCEN cesó la transmisión de las listas de sospechosos según la sección 314(a) vía fax que obtienen acceso a Internet deben tomar medidas para comenzar a recibir las listas de sospechosos según la sección 314(a) a través del SISS.

La FinCEN ha proporcionado a las instituciones financieras Instrucciones generales y Preguntas frecuentes (FAQ, por sus siglas en inglés) relacionadas con el proceso de la sección 314(a). A menos que se establezca lo contrario en una solicitud de información, las instituciones financieras deben realizar búsquedas en los registros especificados en las Instrucciones generales.[87] Las Instrucciones generales o FAQ están disponibles para las instituciones financieras en el SISS[88]

---

[86] Si la solicitud enumera varios sospechosos, a menudo se denomina “lista 314(a)”.

[87] Por ejemplo, con respecto a las transferencias de fondos, las “Instrucciones generales” indican que, a menos que las instrucciones de una solicitud según la 314(a) específica indiquen lo contrario, se exige que los bancos realicen búsquedas en registros de transferencias de fondos mantenidos según 31 CFR 103.33, para determinar si la persona identificada como sospechosa fue un originador/transmisor de una transferencia de fondos en la que el banco fue la institución financiera del originador/transmisor, o un beneficiario/receptor de una transferencia de fondos en la que el banco fue la institución financiera del beneficiario/receptor.

[88] También puede comunicarse de manera gratuita con la FinCEN al 800-949-2732 para obtener las Instrucciones generales y las FAQ.

Si una institución financiera identifica cualquier cuenta o transacción, debe informar a la FinCEN que encontró una coincidencia. No se debe proporcionar detalles a la FinCEN más que el hecho de que la institución financiera encontró una coincidencia. No es necesario informar una respuesta negativa. Una institución financiera puede proporcionar las listas de sospechosos según la sección 314(a) a un prestador de servicios externo o proveedor para que realice o facilite las búsquedas en los registros siempre y cuando la institución tome las medidas necesarias, a través del uso de un acuerdo o procedimientos, para garantizar que el tercero proteja y mantenga la confidencialidad de la información.

Según las FAQ disponibles en el SISS, si una institución financiera que recibe listas de sospechosos según la sección 314(a) a través del SISS no realiza o no completa las búsquedas en una o más solicitudes de información recibidas durante los 12 meses anteriores, debe obtener de inmediato estas solicitudes anteriores de la FinCEN y realizar una búsqueda retroactiva en sus registros.[89] No se exige a una institución financiera realizar búsquedas retroactivas en conexión con las solicitudes de intercambio de información transmitidas más de 12 meses antes de la fecha en la que descubre que no realizó ni completó las búsquedas de solicitudes de información anteriores. Además, no se le exige a una institución financiera buscar registros creados después de la fecha de la solicitud de información original, cuando realiza búsquedas retroactivas.

Restricciones de uso y confidencialidad

Las instituciones financieras deben desarrollar e implementar políticas, procedimientos y procesos exhaustivos para responder a las solicitudes según la sección 314(a). El reglamento restringe el uso de la información proporcionada en la solicitud según la sección 314(a) (31 CFR 103.100(b)(2)(iv)). Una institución financiera puede usar la información para presentarla ante la FinCEN, para determinar si es necesario establecer o mantener una cuenta o participar en una transacción, o para contribuir en el cumplimiento de BSA/AML. Aunque la lista de sospechosos según la sección 314(a) se puede usar para determinar si es necesario establecer o mantener una cuenta, la FinCEN disuade firmemente a las instituciones financieras de usarla como el único factor para tomar una decisión al respecto, a menos que la solicitud indique específicamente lo contrario. A diferencia de las listas de la Oficina de Control de Activos Extranjeros (OFAC, por sus siglas en inglés), las listas de sospechosos según la sección 314(a) no son “listas de observación” permanentes. De hecho, las listas de sospechosos según la sección 314(a) generalmente se relacionan con consultas únicas y no se actualizan ni corrigen si se cancela una investigación, se rechaza un proceso judicial o se exonera a un sospechoso. Además, los nombres no corresponden a personas condenadas o inculpadas; sino más bien, el sospechoso según la 314(a) sólo necesita ser “sospechoso según una valoración

[89] La institución financiera se debe comunicar con la Oficina del programa 341 de FinCEN vía correo electrónico a sys314a@fincen.gov para obtener solicitudes de información anteriores. Si la institución financiera descubre una coincidencia positiva mientras realiza la búsqueda retroactiva, debe comunicarse con la Oficina del programa 314 de manera gratuita al 800-949-2732 y seleccionar la opción 2. Las instituciones financieras deben responder con coincidencias positivas en el transcurso de los 14 días de recibir una solicitud de información anterior; sin embargo, si una búsqueda retroactiva no arroja coincidencias positivas, no se requiere ninguna otra acción.

razonable" en función de evidencia creíble que demuestre su participación en actos terroristas o lavado de dinero. Por otra parte, la FinCEN aconseja que la inclusión en la lista de sospechosos según la sección 314(a) no debe constituir el único factor para determinar si es necesario presentar un Informe de actividades sospechosas (SAR, por sus siglas en inglés). Las instituciones financieras deben establecer un proceso para determinar si debe presentarse un SAR y cuándo debe presentarse. Consulte la sección del esquema general, "Informes de actividades sospechosas" en las páginas 73 a 89, como guía.

Las medidas tomadas de conformidad con la información proporcionada en una solicitud de la FinCEN no surten efectos sobre las obligaciones de una institución financiera de cumplir con todas las reglas y reglamentos de la OFAC ni de responder a cualquier proceso legal. Además, las medidas tomadas en respuesta a una solicitud no eximen a una institución financiera de su obligación de presentar un SAR y de notificar de inmediato a la autoridad de aplicación de la ley, si fuera necesario, según la normativa vigente.

Una institución financiera no puede divulgar a ninguna persona que no sea la FinCEN, la agencia reguladora principal de la institución o la agencia de aplicación de la ley en cuyo nombre la FinCEN solicita la información, el hecho de que la FinCEN ha solicitado u obtenido información. Una institución financiera debe designar uno o más puntos de contacto para recibir solicitudes de información. La FinCEN ha indicado que un grupo de instituciones financieras afiliadas puede establecer un punto de contacto para distribuir la lista de sospechosos según la sección 314(a) para responder a las solicitudes. Sin embargo, las listas de sospechosos según la sección 314(a) no se pueden compartir con ninguna oficina, sucursal o filial extranjera (a menos que la solicitud especifique lo contrario) y dichas listas no se pueden compartir con filiales o subsidiarias de sociedades de control bancarias, si las filiales o subsidiarias no son consideradas instituciones financieras según se describe en 31 USC 5312(a)(2).

Cada institución financiera debe mantener procedimientos adecuados para proteger la seguridad y confidencialidad de las solicitudes de la FinCEN. Los procedimientos para garantizar la confidencialidad se considerarán adecuados si la institución financiera aplica procedimientos similares a los que ha establecido para cumplir con la sección 501 de la Ley Gramm–Leach–Bliley (15 USC 6801) para la protección de la información personal no pública de sus clientes. Las instituciones financieras pueden llevar un registro de todas las solicitudes según la sección 314(a) y de cualquier coincidencia positiva identificada e informada a la FinCEN.

Documentación

Además, es fundamental contar con documentación que pueda demostrar que se realizaron todas las búsquedas exigidas. En el caso de aquellas listas de sospechosos según la sección 314(a) recibidas vía fax antes del 2 de Junio de 2008, el banco puede conservar copias de la portada de la solicitud con aval de la institución financiera que asegure que los registros se verificaron, junto con la fecha de la búsqueda y los resultados de ésta (p. ej., positivos o negativos). Para las coincidencias positivas con las listas de sospechosos recibidas vía fax, se deben conservar copias del formulario enviado a la FinCEN y la documentación respaldatoria. Para aquellas instituciones que utilizan el

SISS de la sección 314(a) basado en la Web, los bancos pueden imprimir un documento de autoverificación de la búsqueda para cada transmisión de listas de sospechosos según la sección 314(a). Además, se puede imprimir una Lista de Respuestas de Sospechosos con propósitos de documentación. La Lista de respuestas de sospechosos muestra la cantidad total de respuestas positivas enviadas a la FinCEN con respecto a esa transmisión, la fecha de la transmisión, la fecha de presentación, y el número de referencia y nombre del sospechoso que arrojó un resultado positivo. Si la institución financiera opta por mantener copias de las solicitudes según la sección 314(a), no debe ser criticada por su decisión, siempre y cuando las preserve y proteja su confidencialidad de manera adecuada. Las auditorías deben incluir una evaluación del cumplimiento de estas pautas dentro de su campo de aplicación.

La FinCEN actualiza regularmente una lista de transmisiones de solicitudes de búsqueda recientes, que incluye información sobre la fecha de transmisión, el número de referencia y la cantidad de sospechosos listados en la transmisión.[90] Los banqueros e inspectores pueden revisar esta lista para verificar que se hayan recibido las solicitudes de búsqueda. Cada banco se debe comunicar con su agencia reguladora principal si necesita orientación para obtener la lista de sospechosos según la sección 314(a) y para actualizar la información de contacto.[91]

Intercambio de información voluntario: sección 314(b) de la Ley PATRIOTA de EE. UU. (31 CFR 103.110)

La Sección 314(b) exhorta a las instituciones financieras[92] y asociaciones de instituciones financieras ubicadas en los Estados Unidos a compartir información para identificar e informar sobre actividades que pueden estar relacionadas con actividades terroristas o de lavado de dinero. Esta sección también proporciona protección específica contra la responsabilidad civil.[93] Para beneficiarse de esta protección legal estatutaria contra la

[90] Esta lista, denominada "Law Enforcement Information Sharing with the Financial Industry" (Intercambio de Información de las Autoridades de Aplicación Pertinentes con la Industria Financiera), está disponible en la página "Sección 314(a)" del sitio web de FinCEN. Esta lista contiene información sobre cada solicitud de búsqueda transmitida desde el 4 de Enero de 2005, y se actualiza luego de cada transmisión.

[91] Visite el sitio web de FinCEN en www.fincen.gov/statutes_regs/patriot/pdf/poc_change_314a.pdf, para consultar la información de contacto de la sección 314(a) para cada agencia reguladora principal.

[92] 31 CFR 103.110 generalmente define "institución financiera" como cualquier institución financiera descrita en 31 USC 5312(a)(2), a la que se le exige que establezca y mantenga un programa de cumplimiento BSA/AML.

[93] FinCEN ha indicado que una institución financiera que participe del programa de la sección 314(b) puede compartir información relacionada con las transacciones que la institución sospecha que pueden involucrar ingresos de una o más actividades ilegales específicas (SUA, por sus siglas en inglés) y dicha institución aún permanecerá dentro de la protección legal de la sección 314(b) contra la responsabilidad civil. La información relacionada con las actividades ilegales específicas se puede compartir adecuadamente dentro de la protección legal de la 314(b) en la medida en que la institución financiera sospeche que la transacción puede involucrar los ingresos de una o más actividades ilegales específicas y el propósito del intercambio de información permitido bajo la regla de la 314(b) es identificar e informar actividades de las que la institución financiera sospeche que puedan *involucrar posibles* actividades terroristas o lavado de dinero.

responsabilidad, una institución financiera o una asociación debe notificar a la FinCEN su intención de participar en el intercambio de información y que ha establecido y mantendrá procedimientos adecuados para proteger la seguridad y confidencialidad de la información. La falta de cumplimiento de las exigencias de 31 CFR 103.110 derivará en la pérdida de la protección legal para el intercambio de información y puede causar una violación de las leyes de privacidad u otras normativas.

Si una institución financiera opta por participar voluntariamente en la sección 314(b), debe desarrollar e implementar políticas, procedimientos y procesos para compartir y recibir información.

Una notificación para compartir información es efectiva durante un año.[94] La institución financiera debe designar un punto de contacto para recibir y proporcionar información. Una institución financiera debe establecer un proceso para enviar y recibir solicitudes de intercambio de información. Además, una institución financiera debe tomar medidas razonables para verificar que la otra institución financiera o asociación de instituciones financieras con la que tiene la intención de compartir información también haya enviado a la FinCEN la notificación necesaria. La FinCEN proporciona a las instituciones financieras participantes acceso a una lista de otras instituciones financieras participantes y la información de contacto relacionada.

Si una institución financiera recibe dicha información de otra institución financiera, también debe limitar el uso de la información y mantener su seguridad y confidencialidad (31 CFR 103.110(b)(4)). Dicha información puede utilizarse sólo para identificar y, cuando sea conveniente, informar sobre actividades terroristas o de lavado de dinero; para determinar si se debe establecer o mantener una cuenta; para participar en una transacción; o para asistir en el cumplimiento de la BSA. Los procedimientos para garantizar la confidencialidad se considerarán adecuados si la institución financiera aplica procedimientos similares a los que ha establecido para cumplir con la sección 501 de la Ley Gramm–Leach–Bliley (15 USC 6801) para la protección de la información personal no pública de sus clientes. La protección legal no se aplica al intercambio de información con instituciones radicadas en el extranjero. Además, la sección 314(b) no autoriza a una institución financiera a compartir un SAR ni divulgar la existencia o inexistencia de éste. Si una institución financiera comparte información bajo la sección 314(b) sobre el contenido de un informe SAR preparado o presentado, la información que se comparte debe limitarse a la información sobre el cliente y las transacciones subyacentes. Una institución financiera debe usar la información obtenida bajo la sección 314(b) para determinar si debe presentar un SAR, pero la intención de preparar o presentar un SAR no se puede compartir con otra institución financiera. Las instituciones financieras deben establecer un proceso para determinar si debe presentarse un SAR y cuándo debe presentarse.

Consulte *Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act,* (Guía sobre el campo de intercambio de información permisible cubierto por la protección legal de la sección 314(b) de la ley PATRIOTA de EE. UU.) FIN-2009-G002 (16 de Junio de 2009) en www.fincen.gov**.**

[94] Las instrucciones sobre el envío de un formulario de notificación (inicial o renovación) están disponibles en el sitio web de la FinCEN, www.fincen.gov.

Las medidas tomadas de conformidad con la información obtenida mediante el proceso de intercambio de información voluntario no tienen efecto en las obligaciones de una institución financiera de responder a cualquier proceso legal. Además, las medidas tomadas en respuesta a la información obtenida mediante este proceso no eximen a una institución financiera de su obligación de presentar un SAR y de notificar de inmediato a la autoridad de aplicación de la ley, si fuera necesario según la normativa vigente.

Procedimientos de Inspección

Intercambio de información

Objetivo: *Evaluar el cumplimiento de la institución financiera con las exigencias normativas y legales para los "Procedimientos Especiales de Intercambio de Información para Impedir las Actividades Terroristas y de Lavado de Dinero" (Solicitudes de información según la sección 314).*

Intercambio de información entre las autoridades de aplicación de la ley y las instituciones financieras (Sección 314(a))

1. Verifique que la institución financiera reciba actualmente las solicitudes según la sección 314(a) de parte de la FinCEN o de parte de una institución financiera afiliada que sirva de punto de contacto de la institución financiera en cuestión. Si la institución financiera no recibe las solicitudes de información[95] o los cambios en la información de contacto, la institución financiera debe actualizar su información de contacto con su ente regulador principal según las instrucciones disponibles en www.fincen.gov.

2. Verifique que la institución financiera cuente con políticas, procedimientos y procesos suficientes para documentar el cumplimiento, mantener los controles internos suficientes, proporcionar capacitación continua y probar de manera independiente su cumplimiento con 31 CFR 103.100, que implementa la sección 314(a) de la Ley PATRIOTA de EE. UU. Como mínimo, los procedimientos deben lograr lo siguiente:

   - Designar un punto de contacto para recibir solicitudes de información.
   - Garantizar que la confidencialidad de la información solicitada esté protegida.
   - Establecer un proceso para responder a las solicitudes de la FinCEN.
   - Establecer un proceso para determinar si debe presentarse un SAR y cuándo.

3. Determine si las políticas, los procedimientos y los procesos de búsqueda que la institución financiera utiliza para responder a las solicitudes según la sección 314(a) son exhaustivos y cubren todos los registros identificados en las Instrucciones generales para dichas solicitudes. Las Instrucciones generales incluyen realizar búsquedas en

[95] A partir del 2 de Junio de 2008, FinCEN ha suspendido la transmisión vía fax de las listas de sospechosos según la sección 314(a) a instituciones financieras. Las instituciones financieras a las que FinCEN cesó la transmisión de las listas de sospechosos según la sección 314(a) vía fax que obtienen acceso a través de Internet deben tomar medidas para comenzar a recibir las listas de sospechosos según la sección 314(a) a través del Sistema seguro de intercambio de información de la 314(a) basado en la Web.

cuentas mantenidas por el sujeto en cuestión durante los 12 meses precedentes y las transacciones efectuadas dentro de los últimos seis meses. Las instituciones financieras tienen 14 días desde la fecha de transmisión de la solicitud para responder a un Formulario de información sobre sospechosos según la sección 314(a).

4. Si la institución financiera utiliza los servicios de un proveedor externo para realizar o facilitar las búsquedas, determine si se dispone de un acuerdo o de procedimientos para garantizar la confidencialidad.

5. Examine los controles internos de la institución financiera y determine si la documentación con la que cuentan para demostrar el cumplimiento con las solicitudes según la sección 314(a) es adecuada. Por ejemplo, esta documentación puede incluir lo siguiente:

   - Copias de las solicitudes según la sección 314(a).
   - Un registro que almacena los números de referencia e incluye una columna donde se puede avalar.
   - Para las listas de sospechosos según la sección 314(a) recibidas vía fax antes del 2 de Junio de 2008, copias de la portada de las solicitudes con aval de la institución financiera que asegure que los registros se verificaron, junto con la fecha de la búsqueda y los resultados de ésta (p. ej., positivos o negativos).
   - Copias de los documentos de la autoverificación de la búsqueda generada por el SISS.
   - Para las coincidencias positivas, se deben conservar copias del formulario enviado a la FinCEN (p. ej., Listas de Respuestas de Sospechosos generadas por el SISS) y la documentación respaldatoria.

Intercambio de información voluntario (Sección 314(b))

6. Determine si la institución financiera ha decidido compartir información voluntariamente. Si es así, verifique que la institución financiera haya presentado un formulario de notificación en la FinCEN y que proporcione una fecha de vigencia para el intercambio de información que sea dentro de los 12 meses anteriores.

7. Verifique que la institución financiera cuente con políticas, procedimientos y procesos para compartir información y recibir la información compartida, según lo especifica 31 CFR 103.110 (que implementa la sección 314(b) de la Ley PATRIOTA de EE.UU.).

8. Las instituciones financieras que optan por compartir información voluntariamente deben contar con políticas, procedimientos y procesos para documentar el cumplimiento, mantener los controles internos adecuados, proporcionar capacitación continua y probar de manera independiente su cumplimiento con 31 CFR 103.110. Como mínimo, los procedimientos deben:

   - Designar un punto de contacto para recibir y proporcionar información.

- Garantizar la protección y confidencialidad de la información recibida y solicitada.
- Establecer un proceso para enviar y responder a solicitudes, incluso para garantizar que otras partes con las que la institución financiera tiene la intención de compartir información (incluidas las filiales) hayan presentado la notificación adecuada.
- Establecer procedimientos para determinar si debe presentarse un SAR y cuándo.

9. Si la institución financiera comparte información con otras entidades y no cumple con los procedimientos descritos en 31 CFR 103.110(b), notifique a los inspectores que controlan las normas sobre privacidad.

10. Mediante una revisión de la documentación de la institución financiera (incluido el análisis de cuenta) de una muestra de la información compartida y recibida, evalúe cómo hizo la institución financiera para determinar si se requería la presentación de un SAR. No se exige que la institución financiera presente los SAR sólo en función de la información obtenida mediante el proceso de intercambio de información voluntario. De hecho, la información obtenida mediante el proceso de intercambio de información voluntario puede permitir que la institución financiera determine que no se requiere la presentación de un SAR con respecto a transacciones que inicialmente pueden haber parecido sospechosas. La institución financiera debe haber tenido en cuenta la actividad de cuenta al determinar si se requería la presentación de un SAR.

Pruebas de transacciones

11. En función de un análisis de riesgos, los informes de inspección previos, y un control de los resultados de la auditoría de la institución financiera, seleccione una muestra de las coincidencias positivas o búsquedas recientes para determinar si se han cumplido las siguientes exigencias:

    - Las políticas, los procedimientos y los procesos de la institución financiera le permiten buscar todos los registros identificados en las Instrucciones generales para las solicitudes según la sección 314(a). Dichos procesos pueden ser electrónicos, manuales o ambos.
    - La institución financiera busca registros apropiados para cada solicitud de información recibida. Para las coincidencias positivas:
        - Verifique que se haya proporcionado una respuesta a la FinCEN dentro del plazo designado (31 CFR 103.100(b)(2)(ii)).
        - Revise la documentación de la institución financiera (incluido el análisis de cuenta) para evaluar cómo hizo la institución financiera para determinar si se requería la presentación de un SAR. No se exige que las instituciones financieras presenten los SAR sólo en función de una coincidencia con un individuo identificado; en cambio, debe tomarse en cuenta la actividad de la cuenta para determinar si se requiere la presentación de un SAR.

- La institución financiera utiliza información únicamente en la manera permitida y para los propósitos permitidos, y mantiene dicha información segura y confidencial (31 CFR 103.100(b)(2)(iv)). (Esta exigencia puede verificarse mediante una conversación con la gerencia).

12. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos para cumplir con las exigencias normativas asociadas al intercambio de información.

Gestión de Registros de Compraventa de Instrumentos Monetarios: Esquema General

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales de registro de información necesaria para la compraventa de instrumentos monetarios por montos en moneda entre USD 3.000 y USD 10.000 inclusive. Esta sección abarca las exigencias normativas según lo establece la BSA. Consulte las secciones ampliadas de este manual para conocer análisis y procedimientos adicionales relacionados con los riesgos específicos de lavado de dinero en las compraventas de instrumentos monetarios.*

Los bancos venden una variedad de instrumentos financieros (p. ej., cheques de bancos o giros, que incluyen giros en moneda extranjera, giros postales, cheques de caja y cheques de viajeros) a cambio de moneda. La compra de estos instrumentos por montos inferiores a los USD 10.000 es una práctica común empleada por quienes lavan dinero, para evadir las exigencias de informe que aplican para las transacciones de grandes volúmenes de moneda. Una vez que el efectivo fue convertido en instrumento, los delincuentes generalmente lo depositan en cuentas abiertas en otros bancos para facilitar el movimiento de los fondos a través del sistema de pagos. En muchos casos, las personas involucradas no poseen cuentas en el banco que les vende los instrumentos.

Identificación del comprador

Bajo 31 CFR 103.29, los bancos están obligados a verificar la identidad de quienes compran instrumentos monetarios a cambio de efectivo por valores entre USD 3.000 y USD 10.000 inclusive, y llevar registros de dichas ventas.

Los bancos pueden verificar si el comprador de los instrumentos monetarios es titular de una cuenta de depósito con la información de identificación que posee el banco en sus registros, o puede verificar la identidad del comprador viendo algún documento de identidad del comprador que contenga el nombre y la dirección del cliente, y que sea reconocido por la comunidad financiera como medio de identificación válido para el pago de cheques a quienes no son clientes. El banco debe obtener información adicional de los compradores que no posean cuentas de depósito. El método empleado para verificar la identidad del comprador debe quedar registrado.

Identificación admisible

El Dictamen Administrativo 92-1 expedido por el Tesoro de los Estados Unidos indica la forma en que los bancos pueden verificar la identidad de clientes de edad avanzada o discapacitados que no posean los documentos de identidad comúnmente aceptables. Un banco puede aceptar una tarjeta del Seguro Social, de Medicare o Medicaid conjuntamente con alguna otra forma de identificación que incluya el nombre y la dirección del cliente. Esa identificación adicional incluye recibos de pago de servicios públicos, recibos de pago de impuestos o la tarjeta de inscripción en el padrón del elector. Las formas alternas de identificación que decida aceptar un banco deben ser incluidas en sus políticas, procedimientos y procesos formales.

Compras simultáneas

Las compras simultáneas de una misma clase de instrumento o de instrumentos de clases diferentes por un valor total de USD 3.000 o más se deben tratar como una sola compra. Las compras múltiples realizadas en un mismo día hábil por valor de USD 3.000 o más se deben acumular y tratar como una sola compra, si el banco tiene conocimiento de las mismas.

Compras indirectas en efectivo de instrumentos monetarios

Los bancos pueden implementar una política que exija a los clientes titulares de cuentas de depósito que deseen adquirir instrumentos monetarios por un valor entre USD 3.000 y USD 10.000 en efectivo, que primero depositen el monto respectivo en sus cuentas de depósito. No existe nada en la BSA ni en los reglamentos de ejecución que prohíba a los bancos instituir una política de este tipo.

Sin embargo, la FinCEN considera[96] que cuando un cliente compra un instrumento monetario por un monto entre USD 3.000 y USD 10.000 con fondos que ya ha depositado en su cuenta de depósito, la transacción sigue estando sujeta a las exigencias de gestión de registros establecidas en 31 CFR 103.29. Esta exigencia se aplica tanto si la transacción se realiza de conformidad con las políticas establecidas por el banco, como si se realiza a solicitud del cliente. Generalmente, cuando un banco vende instrumentos monetarios a clientes titulares de cuentas de depósito, los bancos ya tienen la mayor parte de la información que se requiere según 31 CFR 103.29, lograda durante el curso normal de sus negocios.

Exigencias con respecto a la gestión y conservación de registros

Según 31 CFR 103.29, los registros de ventas de los bancos deben incluir, como mínimo, la siguiente información:

- Si el comprador **es titular de una cuenta de depósito** en el banco:
  - Nombre del comprador.
  - Fecha de la compra.
  - Tipos de instrumentos adquiridos.
  - Número de serie de cada uno de los instrumentos adquiridos.
  - Monto en dólares de cada instrumento adquirido en efectivo.

[96] Guidance on Interpreting Financial Institution Policies in Relation to Recordkeeping Requirements (Guía para la interpretación de las políticas de las instituciones financieras sobre exigencias con respecto a la conservación de los registros) de la FinCEN bajo 31 CFR 103.29, Noviembre de 2002, www.fincen.gov.

  - Información específica de identificación, si es pertinente.[97]

- Si el comprador no es titular de una cuenta de depósito en el banco:
  - Nombre y dirección del comprador.
  - Número de Seguro Social o un número de identificación de extranjero del comprador.
  - Fecha de nacimiento del comprador.
  - Fecha de la compra.
  - Tipos de instrumentos adquiridos.
  - Número de serie de cada uno de los instrumentos adquiridos.
  - Monto en dólares de cada instrumento adquirido.
  - Información específica de identificación para verificar la identidad del comprador (p. ej., estado que expide la licencia de conducir y número de la misma).

Si el comprador no brinda la información requerida en el momento de la transacción o ésta no se obtiene de los registros previamente verificados del mismo banco, se debe rechazar la transacción. Los registros de ventas de instrumentos monetarios deben guardarse durante cinco años y estar disponibles para consulta por parte de las agencias apropiadas mediante solicitud.

---

[97] El banco debe verificar que la persona sea titular de una cuenta de depósito o verificar la identidad de dicha persona. La verificación puede hacerse mediante una tarjeta de firma u otro tipo de archivo o registro del banco, siempre que el nombre y la dirección del cliente titular de la cuenta de depósito hayan sido verificados previamente y la información haya sido registrada en la tarjeta de firma u otro archivo o registro, o mediante examen del documento normalmente aceptado en la comunidad bancaria que contenga el nombre y la dirección del comprador. Si la identidad del titular de la cuenta de depósito no ha sido verificada con anterioridad, el banco debe registrar la información concreta de identificación (p. ej., el estado que expidió la licencia de conducir así como el número de la licencia) del documento examinado.

Procedimientos de Inspección

Gestión de registros de compraventa de instrumentos monetarios

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales de registro de información necesaria para la compraventa de instrumentos monetarios por montos en moneda entre USD 3.000 y USD 10.000 inclusive. Esta sección abarca las exigencias normativas según lo establece la BSA. Consulte las secciones ampliadas de este manual para conocer análisis y procedimientos adicionales relacionados con los riesgos específicos de lavado de dinero en las compraventas de instrumentos monetarios.*

1. Determine si el banco mantiene los registros exigidos (en un sistema manual o automatizado) para las ventas de cheques del banco o giros, que incluyen giros en moneda extranjera, cheques de caja, giros postales y cheques de viajeros a cambio de efectivo por valores de entre USD 3.000 y USD 10.000, inclusive, a compradores titulares de cuentas de depósito en el banco.

2. Determine si las políticas, los procedimientos y los procesos del banco permiten las ventas de instrumentos monetarios en efectivo a compradores que no son titulares de cuentas de depósito en el banco (que no son depositantes).

   - De ser así, determine si el banco mantiene los registros exigidos para las ventas de los instrumentos monetarios a quienes no son depositantes.

   - Si no está permitido, determine si el banco permite las ventas en casos de excepción.

Pruebas de transacciones

3. En función de un análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de los instrumentos monetarios vendidos a cambio de efectivo por valores entre U$S 3.000 y U$S 10.000, inclusive, para determinar si el banco obtiene, verifica y conserva los registros exigidos para garantizar el cumplimiento con las exigencias normativas.

4. A partir de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos de cumplir con las exigencias normativas asociadas con la compraventa de instrumentos monetarios.

5. En función de la conclusión anterior y los riesgos asociados con la actividad del banco en esta área, continúe con los procedimientos de inspección de la sección ampliada, si fuera necesario.

Gestión de Registros de Transferencias de Fondos: Esquema General

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para las transferencias de fondos. Esta sección abarca las exigencias normativas según lo establecido en la BSA. Consulte las secciones ampliadas de este manual para conocer análisis y procedimientos relacionados con los riesgos específicos de lavado de dinero en las actividades de transferencia de fondos.*

Los sistemas de transferencias de fondos permiten la transferencia instantánea de fondos, ya sean transferencias nacionales como transnacionales. Por consiguiente, estos sistemas pueden presentar un método atractivo para ocultar el origen de los fondos derivados de actividades ilegales. La BSA fue enmendada por la Ley Annunzio-Wylie Contra el Lavado de Dinero de 1992, con el objetivo de facultar al Tesoro de los Estados Unidos y a la Junta de Reserva Federal para reglamentar las transferencias de fondos tanto nacionales como internacionales.

En 1995 el Tesoro de los Estados Unidos y la Junta de Gobernadores del Sistema de Reserva Federal expidieron una reglamentación definitiva sobre las exigencias de gestión de registros respecto a órdenes de pago emitidas por bancos (31 CFR 103.33).[98] La reglamentación exige que cada banco que participe en transferencias de fondos[99] obtenga y conserve cierta información sobre las transferencias de fondos realizadas por valor de USD 3.000 o más.[100] La información que es necesario obtener y conservar depende del papel que ejerza el banco en la transferencia de fondos concreta (banco del remitente, banco intermediario o banco del beneficiario).[101] Las exigencias también pueden variar si el remitente o el beneficiario es cliente reconocido del banco, y si la orden de pago se hace personalmente o de otra forma.

---

[98] 31 CRF 103.33(e) es la regla que rige los registros que llevan los bancos y 31 CFR 103.33(f) impone exigencias similares a las instituciones financieras no bancarias que participan en transferencias de fondos. Los procedimientos establecidos en la sección del esquema general principal únicamente tratan las reglas que deben aplican bancos según 31 CFR 103.33(e).

[99] La transferencia de fondos se define en 31 CRF 103.11. Las transferencias de fondos que se rigen por la Ley de Transferencia Electrónica de Fondos de 1978, así como todas las demás transferencias de fondos realizadas a través de cámaras de compensación automáticas, cajeros automáticos o sistemas de puntos de venta, están excluidas de esta definición y quedan exentas de los requisitos establecidos en 31 CFR 103.33(e), (f) y (g).

[100] 31 CRF 103.33(e)(6) establece excepciones a las exigencias para las transferencias de fondos. Las transferencias de fondos en las que el remitente y el beneficiario son la misma persona y el banco del primero y del segundo son el mismo banco, no están sujetas a las exigencias de registro que se aplican a las transferencias de fondos. Además, se crean excepciones a las exigencias de registro de transferencias de fondos cuando tanto el remitente como el beneficiario son: bancos; una subsidiaria nacional de entera propiedad de un banco constituido en los Estados Unidos; un agente o comisionista de valores; una subsidiaria nacional de entera propiedad de un agente o comisionista de valores; los Estados Unidos; un gobierno estatal o local; o una agencia o dependencia del gobierno federal, estatal o local.

[101] Estos términos están definidos bajo 31 CFR 103.11.

También en 1995 el Tesoro de los Estados Unidos expidió una norma definitiva en la que se exige que todas las instituciones financieras incluyan cierta información en las órdenes de transmisión de transferencias de fondos efectuadas por un valor de USD 3.000 o más (31 CFR 103.33).[102] Esta exigencia es conocida en general como la "*Travel Rule*".

Obligaciones del banco del remitente

Exigencias en cuanto a la gestión de registros

Por cada orden de pago por valor de USD 3.000 o más en la que un banco acepte participar en carácter de banco del remitente, dicho banco debe obtener y guardar los siguientes registros (31 CFR 103.33(e)(1)(i)):

- Nombre y dirección del remitente.
- Monto de la orden de pago.
- Fecha de la orden de pago.
- Instrucciones de pago.
- Identidad de la institución del beneficiario.
- De los siguientes elementos, los mismos que se reciban con la orden de pago:
    - Nombre y dirección del beneficiario.
    - Número de cuenta del beneficiario.
    - Cualquier otra identificación específica del beneficiario.

Exigencias adicionales en cuanto a la gestión de registros para clientes no reconocidos

Si el remitente no es un cliente reconocido del banco, es necesario obtener y retener la información mencionada arriba. Además, el banco del remitente debe obtener y conservar otra información, según la orden de pago se emita o no personalmente.

Órdenes de pago emitidas personalmente

Si la orden de pago se emite personalmente, el banco del remitente debe verificar la identidad de la persona que emite la orden antes de aceptarla. Si acepta la orden, la institución financiera del remitente debe obtener y conservar los siguientes registros:

---

[102] La regla se aplica tanto a bancos como a instituciones no bancarias (31 CFR 103.33(g)). Debido a su mayor alcance, la *Travel Rule* emplea términos de mayor cobertura tales como "orden de transmisión" en lugar de "orden de pago" e "institución financiera del transmisor" en lugar de "banco remitente". Los términos más amplios incluyen aquellos que son específicos de los bancos.

- Nombre y dirección de quien emite la orden.
- Tipo de identificación controlada.
- Número del documento de identificación (p. ej., licencia de conducir).
- Número de identificación fiscal (TIN) de la persona (p. ej., el número de Seguro Social [SSN] o número de identificación del empleador [EIN]) o, si éstos no están disponibles, el número de identificación extranjera o del pasaporte y país de expedición, o una anotación indicando la ausencia de dicho documento. Si el banco del remitente sabe que la persona que emite la orden de pago no es el remitente, dicho banco debe obtener y registrar el TIN del remitente (por ej., el SSN o el EIN) o, si éstos no están disponibles, el número de identificación extranjera o del pasaporte y país que lo expidió, o una anotación indicando la ausencia de dicho documento.

Órdenes de pago no emitidas personalmente

Si la orden de pago no se emite personalmente, el banco del remitente debe obtener y conservar los siguientes registros:

- Nombre y dirección de quien emite la orden de pago.
- Número de identificación fiscal (TIN) de la persona (p. ej., el número de Seguro Social [SSN] o número de identificación del empleador [EIN]) o, si éstos no están disponibles, el número de identificación extranjera o del pasaporte y país de expedición, o una anotación indicando la ausencia de dicho documento y una copia o registro que indique el medio de pago (p. ej., transacción por medio de cheque o tarjeta de crédito) de la transferencia de fondos. Si el banco del remitente sabe que la persona que emite la orden de pago no es el remitente, dicho banco debe obtener y registrar el TIN del remitente (por ej., el SSN o el EIN) o, si éstos no están disponibles, el número de identificación extranjera o del pasaporte y país que lo expidió, o una anotación indicando la ausencia de dicho documento.

Localización de la información

La información conservada debe ser localizable mediante referencia al nombre del remitente. Cuando el remitente es un cliente reconocido del banco y dispone de una cuenta que utiliza para transferencias de fondos, la información conservada también debe ser localizable por número de cuenta (31 CFR 103.33(e)(4)). Los registros deben mantenerse durante un período de cinco (5) años.

Exigencias de la *Travel Rule*

Para las transmisiones de fondos de USD 3.000 o más, la institución financiera del transmisor debe incluir la siguiente información en la orden de transmisión, en el momento en que dicha orden se envía a la entidad financiera receptora (31 CFR 103.33(g)(1)):

- Nombre del transmisor y, si el pago se ordena desde una cuenta, el número de la cuenta del transmisor.
- Dirección del transmisor.
- Monto de la orden de transmisión.
- Fecha de la orden de transmisión.
- Identidad de la institución financiera del receptor.
- De los siguientes elementos, los mismos que se reciban con la orden de transmisión:
  - Nombre y dirección del receptor.
  - Número de cuenta del receptor.
  - Cualquier otra identificación específica del receptor.
- El nombre y la dirección o el identificador numérico de la institución financiera del transmisor.

La *Travel Rule* no dispone de exigencias en cuanto a la gestión de registros.

Obligaciones de las instituciones intermediarias

Exigencias en cuanto a la gestión de registros

El banco debe conservar un registro de cada orden de pago por valor de USD 3.000 o más en la que acepte participar como banco intermediario.

Exigencias de la *Travel Rule*

La institución financiera intermediaria debe incluir la siguiente información respecto a las transmisiones de fondos de USD 3.000 o más, si dicha información fue recibida de parte del remitente de una orden de transmisión en el momento en que en dicha orden se envió a la entidad financiera receptora (31 CFR 103.33(g)(2)):

- Nombre y número de cuenta del transmisor.
- Dirección del transmisor.
- Monto de la orden de transmisión.
- Fecha de la orden de transmisión.
- Identidad de la institución financiera del receptor.
- De los siguientes elementos, los mismos que se reciban con la orden de transmisión:
  - Nombre y dirección del receptor.

  - Número de cuenta del receptor.
  - Cualquier otra identificación específica del receptor.
- El nombre y la dirección o el identificador numérico de la institución financiera del transmisor.

Las instituciones financieras intermediarias deben transmitir toda la información recibida de la institución financiera del transmisor o la institución financiera anterior, pero no están obligadas a obtener la información que no haya sido suministrada por la institución financiera del transmisor o la institución financiera anterior.

Obligaciones del banco del beneficiario

Exigencias en cuanto a la gestión de registros

El banco debe conservar un registro de cada orden de pago por valor de USD 3.000 o más en que acepte participar como banco del beneficiario.

Si el beneficiario no es un cliente reconocido del banco, la entidad del beneficiario debe conservar la siguiente información por cada pago emitido por valor de USD 3.000 o más.

Fondos a ser entregados personalmente

Si los fondos se entregan personalmente al beneficiario o a su representante o agente, la institución debe verificar la identidad de la persona que recibe los fondos y conservar un registro con la siguiente información:

- Nombre y dirección.
- Tipo de documento controlado.
- Número del documento de identificación.
- El TIN de la persona, o, si éste no está disponible, el número de identificación extranjera o del pasaporte y país de expedición, o una anotación en el registro indicando la ausencia de dicho documento.
- Si la institución tiene conocimiento de que la persona que recibe los fondos no es el beneficiario, debe obtener y conservar un registro del nombre y la dirección del beneficiario, así como de la identificación del beneficiario.

Fondos que no se entregan personalmente

Si los fondos no se entregan personalmente, la institución debe conservar una copia del cheque u otro instrumento empleado para efectuar el pago, o debe registrar la información relativa al instrumento. La institución debe también registrar el nombre y la dirección de la persona a la cual éste ha sido enviado.

Localización de la información

La información conservada debe ser localizable mediante referencia al nombre del beneficiario. Cuando el beneficiario es un cliente reconocido del banco y dispone de una cuenta que utiliza para transferencias de fondos, la información conservada también debe ser localizable por número de cuenta (31 CFR 103.33(e)(4)).

No existen exigencias relativas a la *Travel Rule* para los bancos beneficiarios.

Abreviaturas y direcciones

Aunque la *Travel Rule* no permite usar nombres codificados o seudónimos, sí permite usar nombres abreviados, nombres que reflejen distintas cuentas de una corporación (por ej., Cuenta de nómina de XYZ) y nombres comerciales o adoptados para un negocio ("opera comercialmente bajo el nombre de") o nombres de las divisiones o departamentos que no estén formalmente constituidos y que formen parte de un negocio.

Dirección del cliente

El término "dirección" tal como se emplea en (31 CFR 103.33(g) no está definido. Las pautas previamente emitidas por la FinCEN habían sido interpretadas como contrarias al uso de la dirección postal en las órdenes de transmisión, cuando la institución financiera del transmisor conocía la dirección real. Sin embargo, en la notificación del *Registro Federal* del 28 de Noviembre de 2003,[103] la FinCEN expidió una interpretación reglamentaria que sostiene que la *Travel Rule* debe permitir el uso de las direcciones postales, incluidos apartados postales, en el campo de dirección del transmisor de órdenes de transmisión, en ciertas circunstancias.

La interpretación reglamentaria sostiene que, para los fines de 31 CFR 103.33(g), el término "dirección" significa la dirección real del transmisor o la dirección del transmisor registrada en el archivo automatizado CIF de la entidad financiera (por ejemplo, una dirección postal que incluye un número de apartado postal), siempre y cuando la institución mantenga la dirección del transmisor[104] en sus registros y dicha dirección sea localizable si lo solicitan las autoridades de aplicación de la ley.

---

[103] 68 FR 66708 (23 de Noviembre de 2003).

[104] De conformidad con 31 CFR 103.121 para los fines de la *Travel Rule* una "dirección" significa lo siguiente: en el caso de una persona, una dirección residencial o comercial, un Apartado postal del ejército o Apartado postal de la marina, o la dirección residencial o comercial del familiar más cercano u otra persona de contacto, para quienes no cuentan con una dirección residencial o comercial. Para las personas que no son personas físicas (por ejemplo, corporaciones, asociaciones o fideicomisos), la "dirección" es la sede principal de los negocios, oficina local u otra ubicación física. Sin embargo, si bien 31 CFR 103.121 se aplica únicamente a nuevos clientes que han abierto cuentas a partir del 1 de Octubre de 2003, y exceptúa las transferencias de fondos de la definición de "cuenta", en el caso de los bancos la *Travel Rule* se aplica a todas las transmisiones de fondos por valor de USD 3.000 o más, sin importar si el transmisor es un cliente para los fines de 31 CFR 103.121.

Procedimientos de Inspección

Gestión de registros de transferencias de fondos

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para las transferencias de fondos. Esta sección abarca las exigencias normativas según lo establecido en la BSA. Consulte las secciones ampliadas de este manual para conocer análisis y procedimientos relacionados con los riesgos específicos de lavado de dinero en las actividades de transferencia de fondos.*

1. Verifique que el banco obtenga y mantenga los registros adecuados para garantizar el cumplimiento de 31 CFR 103.33(e).

2. Verifique que el banco transmita información sobre pagos según lo exige 31 CFR 103.33(g) ("*Travel Rule*").

3. Verifique que el banco presente CTR cuando el efectivo se reciba o distribuya en una transferencia de fondos que supere los USD 10.000 (31 CFR 103.22).

4. Si el banco envía transferencias de fondos a instituciones en otros países o recibe dichas transacciones de instituciones en otros países, especialmente aquellas sujetas a leyes de secreto y privacidad estrictas, analice si el banco cuenta con políticas, procedimientos y procesos para determinar si las sumas, la frecuencia de la transferencia y los países de origen o destino son consistentes con el tipo de negocio u ocupación del cliente.

Pruebas de transacciones

5. En función del análisis de riesgos, los informes de inspección anteriores, y el control de los resultados de la auditoría del banco, seleccione una muestra de las transferencias de fondos en las que la participación sea en carácter de banco del remitente, banco intermediario y banco del beneficiario para garantizar que la institución obtenga, mantenga o transmita la información requerida, según el papel que ejerza en la transferencia.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, procedimientos y procesos de cumplir con las exigencias normativas asociadas a las transferencias de fondos.

7. En función de la conclusión anterior y los riesgos asociados con la actividad del banco en esta área, continúe con los procedimientos de inspección de la sección ampliada, si fuera necesario.

Debida Diligencia y Gestión de Registros de Cuentas Corresponsales Extranjeras: Esquema General

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para cuentas corresponsales de bancos fantasmas extranjeros, gestión de registros de cuentas corresponsales extranjeras y programas de debida diligencia para detectar e informar acerca de actividades sospechosas y de lavado de dinero. Consulte las secciones ampliadas del manual para conocer análisis y procedimientos de inspección relacionados con los riesgos específicos de lavado de dinero en las cuentas corresponsales extranjeras.*

Uno de los objetivos centrales de la Ley PATRIOTA de EE. UU. fue proteger el acceso al sistema financiero estadounidense exigiendo ciertos registros y programas de debida diligencia para las cuentas corresponsales extranjeras. Además, la Ley PATRIOTA de EE. UU. prohíbe las cuentas en bancos fantasmas extranjeros. Las cuentas corresponsales extranjeras, como se indica en los informes de investigaciones anteriores del Senado de los Estados Unidos,[105] constituyen una puerta de acceso al sistema financiero estadounidense. Esta sección del manual abarca las exigencias normativas establecidas en las secciones 312, 313, y 319(b) de la Ley PATRIOTA de EE. UU. y en los reglamentos de ejecución de 31 CFR 103.175, 103.176, 103.177 y 103.185. En las secciones ampliadas se incluyen análisis y procedimientos adicionales con respecto a los riesgos específicos de lavado de dinero en las actividades de bancos corresponsales extranjeros, como envíos de efectivo en grandes cantidades, actividad de depósitos vía maletines/bolsos, giros en dólares estadounidenses y cuentas empleadas para pagos.

Prohibición con respecto a bancos fantasmas extranjeros y gestión de registros de cuentas corresponsales extranjeras

En relación con 31 CFR 103.177 y 103.185, una "cuenta corresponsal" es una cuenta establecida por un banco a fin de que un banco extranjero reciba depósitos o realice pagos u otros desembolsos en nombre del banco extranjero o para encargarse de otras transacciones financieras relacionadas con el banco extranjero. Una "cuenta" significa cualquier relación formal comercial o bancaria establecida para prestar servicios regulares, realizar negociaciones y otras transacciones financieras. Incluye una cuenta corriente, depósitos en cajas de ahorro u otra cuenta de activos o transacción y una cuenta de crédito u otra concesión de crédito (31 CFR 103.175(d)). Las cuentas mantenidas por

[105] *Correspondent Banking: A Gateway for Money Laundering*. (Bancos corresponsales. Una puerta de acceso para el lavado de dinero). Consulte la Sesión 107-84 del Senado, llevada a cabo el 1, 2 y 6 de Marzo de 2001. El informe aparece en la página 273 del volumen 1 de los registros de sesiones y está titulado *Role of U.S. Correspondent Banking in International Money Laundering* (Papel de los bancos corresponsales de Estados Unidos en el lavado de dinero internacional).

bancos extranjeros para instituciones financieras amparadas por la reglamentación no constituyen "cuentas corresponsales" sujetas a este reglamento.[106]

Bajo 31 CFR 103.177, se prohíbe que un banco establezca, mantenga, administre o gestione una cuenta corresponsal en los Estados Unidos para un banco fantasma extranjero o en nombre de éste. Un banco fantasma extranjero se define como un banco extranjero sin presencia física en ningún país.[107] Sin embargo, una excepción permite que un banco mantenga una cuenta corresponsal para un banco fantasma extranjero que sea una filial regulada.[108] 31 CFR 103.177 también exige que un banco tome medidas razonables para garantizar que cualquier cuenta corresponsal establecida, mantenida, administrada o gestionada en los Estados Unidos para un banco extranjero no esté siendo utilizada por éste para prestar servicios bancarios indirectamente a bancos fantasmas extranjeros.

Certificaciones

Un banco que mantiene una cuenta corresponsal en los Estados Unidos para un banco extranjero debe mantener registros en los Estados Unidos que identifiquen a los propietarios de cada banco extranjero.[109] Un banco también debe registrar el nombre

---

[106] 71 FR 499. La FinCEN ha emitido una guía interpretativa, Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment (Aplicación de reglamentaciones de cuentas corresponsales a la presentación de instrumentos negociables recibidos por parte de una institución financiera para el pago), FIN-2008-G001 (30 de Enero de 2008), que se encuentra en www.fincen.gov, y que establece, "En el transcurso normal de los negocios, una institución financiera cubierta puede recibir instrumentos negociables para el pago por parte de una institución financiera extranjera con la cual mantiene una relación de corresponsalía. . . La FinCEN no ve la presentación de transacción por transacción de un instrumento negociable a una institución de pago extranjera (ya sea directamente o a través de una institución de compensación) como el establecimiento de una relación comercial o bancaria formal por parte de una institución financiera cubierta con propósitos de cumplir con la reglamentación de cuentas corresponsales".

[107] "Presencia física" significa un centro de operaciones que:

- Esté mantenido por un banco extranjero.
- Esté ubicado en un domicilio social fijo (que no sea una dirección electrónica o un apartado postal únicamente) en un país en el que la institución financiera extranjera esté autorizada a llevar a cabo actividades bancarias, en cuya ubicación la institución financiera extranjera:
- Emplee una o más personas a tiempo completo.
- Mantenga registros operativos relacionados con sus actividades bancarias.
- Esté sujeto a inspecciones por parte de la autoridad bancaria que expidió la licencia a la institución financiera extranjera para realizar actividades bancarias.

[108] Una "filial regulada" es un banco fantasma que está afiliado a una institución de depósito, cooperativa de crédito o banco extranjero que mantiene una presencia física en los Estados Unidos o en otra jurisdicción. El banco fantasma afiliado regulado también debe estar sujeto a supervisión por la autoridad bancaria que regula la entidad afiliada.

[109] Para minimizar las responsabilidades de la gestión de registros, no se exige información sobre propiedad a las instituciones financieras que presentan el formulario FR Y-7 *(Informe Anual de las Organizaciones Bancarias Extranjeras)* en la Reserva Federal o para aquellas instituciones financieras que cotizan en la Bolsa de Valores. "Que cotizan en la Bolsa de Valores" se refiere a acciones que cotizan en la bolsa de

y dirección real de una persona que resida en los Estados Unidos y que esté autorizada y haya aceptado ser el agente que acepte notificaciones de demandas.[110] Bajo 31 CFR 103.185, un banco debe generar estos registros dentro de los siete días de recibir una solicitud por escrito de parte de un funcionario de una autoridad federal de aplicación de la ley.

El Tesoro de los Estados Unidos, en colaboración con la industria y agencias bancarias y autoridades de aplicación de la ley federales, elaboró un "proceso de certificación" para ayudar a los bancos en el cumplimiento con las disposiciones sobre gestión de registros. Este proceso incluye formularios de certificación y recertificación. Aunque no se exige que los bancos usen estos formularios, un banco será "considerado en cumplimiento" con el reglamento si obtiene un formulario de certificación completo de parte del banco extranjero y recibe una recertificación antes o cuando se cumple el tercer aniversario de la ejecución de la certificación inicial o previa.[111]

Cierre de cuentas

El reglamento contiene también disposiciones específicas en cuanto al momento en que los bancos deben obtener la información requerida o cerrar las cuentas corresponsales. Los bancos deben obtener certificaciones (o recertificaciones) u obtener la información requerida de algún otro modo dentro de los 30 días calendario de la fecha en que se establece la cuenta y al menos una vez cada tres años a partir de entonces. Si el banco no puede obtener la información requerida, debe cerrar todas las cuentas corresponsales del banco extranjero dentro de un plazo comercialmente razonable.

Verificación

Un banco debe revisar las certificaciones para verificar que sean razonables y precisas. Si en cualquier momento un banco conoce, sospecha o tiene motivos para sospechar que cualquier información contenida en una certificación (o recertificación) o cualquier otra información de la que se vale ya no es correcta, el banco debe solicitar que el banco extranjero verifique o corrija dicha información o debe tomar otras medidas adecuadas para cerciorarse de su precisión. Por lo tanto, los bancos deben revisar las certificaciones para verificar que no existan problemas potenciales que puedan requerir más controles, como el uso de apartados postales o direcciones de reenvío. Si el banco no ha obtenido la información correcta o necesaria dentro de los 90 días, debe cerrar la cuenta dentro de un plazo comercialmente razonable. Durante este plazo, el banco no debe permitir que el banco extranjero establezca nuevas situaciones financieras o ejecute transacciones a

---

valores o en un mercado legal organizado que esté regulado por una autoridad de valores extranjera según lo define la sección 3(a)(50) de la Ley del Mercado de Valores de 1934.

[110] "Notificación de demanda" significa que el agente está dispuesto a aceptar documentos legales tales como citaciones, en nombre del banco extranjero.

[111] Consulte la Guía de la FinCEN FIN-2006-G003, *Frequently Asked Questions, Foreign Bank Recertifications under 31 CFR 103.177* (Preguntas Frecuentes, Recertificaciones de Bancos Extranjeros bajo 31 CFR 103.177), 3 de Febrero de 2006, en www.fincen.gov.

través de la cuenta, que no sean las necesarias para cerrarla. Además, un banco no debe establecer ninguna otra cuenta corresponsal para el banco extranjero hasta haber obtenido la información requerida.

Un banco también debe conservar el original de cualquier documento proporcionado por un banco extranjero, o de lo contrario, el original o una copia de cualquier documento del que se valga en relación con el reglamento, durante al menos cinco años luego de la fecha en la que el banco ya no mantenga ninguna cuenta corresponsal para el banco extranjero.

Citaciones

Bajo la sección 319(b) de la Ley PATRIOTA de EE. UU., el Secretario del Departamento del Tesoro de los Estados Unidos puede expedir una citación o auto de comparecencia a cualquier banco extranjero que mantenga una cuenta corresponsal en los Estados Unidos para obtener los registros relacionados con esa cuenta, incluidos los registros mantenidos en el exterior, o para obtener registros relacionados con el depósito de fondos en el banco extranjero. Si el banco extranjero no puede cumplir con la citación o iniciar el procedimiento judicial para impugnar dicha citación penal, el Secretario del Departamento del Tesoro de los Estados Unidos o el Procurador General de Estados Unidos (consulta mutua previa), puede, mediante notificación por escrito, ordenar que un banco cese su relación con un banco corresponsal extranjero. Si un banco no cesa la relación con el banco corresponsal dentro de los diez días a partir de la recepción de la notificación, puede estar sujeto a una sanción civil monetaria de hasta USD 10.000 por día hasta que cese la relación con el banco corresponsal.

Solicitudes de registros AML por parte de reguladores federales

Además, a solicitud de su regulador federal, un banco debe proporcionar o poner a disposición registros relacionados con el cumplimiento AML del banco o uno de sus clientes, dentro de las 120 horas desde el momento en que se recibió la solicitud (31 USC 5318 (k)(2)).

Programa de debida diligencia especial para cuentas corresponsales extranjeras

La sección 312 de la Ley PATRIOTA de EE. UU. agregó la subsección (i) a 31 USC 5318 de la BSA. Esta subsección exige que cada institución financiera estadounidense que establezca, mantenga, administre o gestione una cuenta corresponsal en los Estados Unidos para una institución financiera extranjera tome ciertas medidas AML para dichas cuentas. Además, la sección 312 de la Ley PATRIOTA de EE. UU. especifica normas adicionales aplicables a las cuentas corresponsales mantenidas para ciertos bancos extranjeros.

El 4 de Enero de 2006, la FinCEN publicó un reglamento definitivo (31 CFR 103.176) que implementa las disposiciones de debida diligencia de 31 USC 5318(i)(1). Posteriormente, el 9 de agosto de 2007, publicó una enmienda para ese reglamento definitivo que implementa las disposiciones de debida diligencia especial de

31 USC 5318(i)(2) con respecto a las cuentas corresponsales establecidas o mantenidas para ciertos bancos extranjeros.

Debida diligencia general

31 CFR 103.176(a) exige que los bancos establezcan un programa de debida diligencia que incluya procedimientos, controles y políticas adecuados, específicos, en función del riesgo y, cuando sea necesario, especiales que hayan sido razonablemente diseñados para permitir que el banco detecte e informe, continuamente, cualquier actividad de lavado de dinero de la que sospeche o tenga conocimiento llevada a cabo a través de o que implique cualquier cuenta corresponsal establecida, mantenida, administrada o gestionada por un banco de los Estados Unidos para una institución financiera extranjera[112] ("cuenta corresponsal extranjera").

Las políticas, los procedimientos y los controles de debida diligencia deben incluir cada uno de los siguientes:

- Determinar si cada una de tales cuentas corresponsales extranjeras está sujeta a debida diligencia especial (consulte "Debida diligencia especial" a continuación).
- Analizar los riesgos de lavado de dinero presentados por cada una de las cuentas corresponsales extranjeras.
- Aplicar procedimientos y controles en función del riesgo razonablemente diseñados a cada cuenta corresponsal extranjera para detectar e informar actividades de lavado de dinero de las que se sospeche o se tenga conocimiento, incluido un control periódico de la actividad de la cuenta corresponsal suficiente para determinar la coherencia de la misma con información obtenida acerca del tipo, propósito y actividad prevista de la cuenta.

Análisis de riesgos de instituciones financieras extranjeras. El programa de debida diligencia general del banco debe incluir políticas, procedimientos y procesos para analizar los riesgos planteados por sus clientes de instituciones financieras extranjeras. Los recursos de un banco están dirigidos más adecuadamente a aquellas cuentas que

[112] El término "institución financiera extranjera" según se define en 31 CFR 103.175(h) generalmente incluye:

- Un banco extranjero.
- Una sucursal en el extranjero u oficina de un banco estadounidense, agentes de valores y comisionistas del mercado de futuros financieros, asesores financieros o agente colocador de fondos comunes de inversión.
- Cualquier otra persona organizada bajo una ley extranjera que, de encontrarse en los Estados Unidos, sería un agente de valores y comisionista del mercado de futuros financieros, asesor financiero o agente colocador de fondos comunes de inversión.
- Cualquier persona organizada bajo la ley extranjera que esté involucrada en el negocio de intercambio de moneda o en el envío de dinero o pueda ser identificada con alguna de estas actividades.

plantean un mayor riesgo de lavado de dinero. El programa de debida diligencia del banco debe hacer posible el análisis de riesgos de cuentas corresponsales extranjeras teniendo en cuenta todos los factores relevantes, incluidos, según sea pertinente:

- El carácter de los negocios de la institución financiera extranjera y los mercados a los que presta servicios.
- El tipo, el propósito y la actividad prevista de la cuenta corresponsal extranjera.
- El carácter y duración de la relación del banco con la institución financiera extranjera (y, de ser pertinente, con cualquier filial de ésta).
- El régimen AML y de supervisión de la jurisdicción que expidió la autorización para funcionar o licencia a la institución financiera extranjera y, en la medida que esa información con respecto a dicha jurisdicción esté razonablemente disponible, de la jurisdicción en la que cualquier compañía propietaria de la institución financiera extranjera está constituida o autorizada a funcionar.
- Información conocida por el banco o razonablemente disponible acerca del registro AML de la institución financiera extranjera, incluida información pública en guías estándar de la industria, periódicos y publicaciones importantes.

No se exige que los bancos evalúen todos los factores anteriores en cada cuenta corresponsal.

Supervisión de cuentas corresponsales extranjeras. Como parte de la debida diligencia continua, los bancos deben revisar periódicamente sus cuentas corresponsales extranjeras. La supervisión no implicará, en situaciones normales, el escrutinio de cada transacción que se efectúe dentro de la cuenta, pero, en su lugar, debe implicar un control de la cuenta que sea suficiente para garantizar que el banco pueda determinar si el carácter y volumen de la actividad de cuenta es generalmente coherente con la información en cuanto al propósito y la actividad prevista de la misma, y para garantizar que el banco pueda identificar de manera adecuada las transacciones sospechosas.

Un programa de debida diligencia eficaz hará posible una variedad de medidas de debida diligencia, en función del análisis de riesgos que el banco realice de cada cuenta corresponsal extranjera. Por lo tanto, el punto de partida de un programa de debida diligencia eficaz debe ser una estratificación del riesgo de lavado de dinero de cada cuenta corresponsal extranjera en función del control de los factores de riesgo relevantes por parte del banco (como aquellos identificados anteriormente) para determinar qué cuentas pueden exigir medidas más profundas. El programa de debida diligencia debe identificar los factores de riesgo que requerirían que la institución lleve a cabo más escrutinios o supervisiones de una cuenta en particular. Como la debida diligencia es un proceso continuo, un banco debe tomar medidas para garantizar que los perfiles de cuenta sean actuales y la supervisión se establezca en función del riesgo. Los bancos deben tener en cuenta si los perfiles de riesgo deben ajustarse o la actividad sospechosa debe informarse cuando ésta no sea coherente con el perfil.

Debida diligencia especial

31 CFR 103.176(b) exige que los bancos establezcan políticas, procedimientos y controles de debida diligencia especial en función del riesgo cuando establezcan, mantengan, administren o gestionen una cuenta corresponsal en los Estados Unidos para ciertos bancos extranjeros (según se identifica en 31 CFR 103.176(c)) operando bajo uno o más de los siguientes:

- Una licencia bancaria extraterritorial.[113]
- Una licencia bancaria expedida por un país extranjero que ha sido designado como no cooperante con los principios o procedimientos AML internacionales por un grupo u organización intergubernamental de la que los Estados Unidos sea miembro y con cuya designación esté de acuerdo el representante de Estados Unidos del grupo u organización.[114]
- Una licencia bancaria expedida por un país extranjero que ha sido designado por el Secretario del Tesoro como destinatario de medidas especiales debido al peligro de lavado de dinero.

Si dicha cuenta se establece o mantiene, 31 CFR 103.176(b) exige que el banco establezca políticas, procedimientos y controles de debida diligencia especial para garantizar que el banco, como mínimo, tome medidas razonables para:

- Determinar, respecto a cualquier banco extranjero cuyas acciones no cotizan en la Bolsa de Valores, la identidad de sus propietarios y el carácter y alcance del interés de cada uno de ellos.[115]
- Llevar a cabo un escrutinio especial de dicha cuenta para protegerse contra el lavado de dinero y para identificar e informar de cualquier transacción sospechosa según la normativa vigente. Este escrutinio especial se lleva a cabo para reflejar el análisis de riesgos de la cuenta y debe incluir, según sea pertinente:

---

[113] La ley PATRIOTA de EE. UU. (31 USC 5318(i)(4)(A) y 31 CFR 103.175(k)) define una licencia bancaria extraterritorial como un licencia para realizar actividades bancarias que, como condición de la licencia, prohíbe a la entidad licenciataria realizar dichas actividades con ciudadanos de la jurisdicción que expidió la licencia o en la moneda local de tal jurisdicción.

[114] El Grupo de Acción Financiera (FATF, por sus siglas en inglés) es la única organización intergubernamental de la cual Estados Unidos es miembro que ha designado países como no cooperantes con los principios internacionales contra el lavado de dinero. Estados Unidos ha estado de acuerdo con todas las designaciones del FATF hasta la fecha.

[115] Un "propietario" es cualquier persona que posee directa o indirectamente, controla o tiene derecho al 10% de los votos o más, de cualquier clase de valores de un banco extranjero (31 CFR 103.176(b)(3)). "Que cotizan en la Bolsa de Valores" se refiere a las acciones que cotizan en la bolsa de valores o en un mercado legal organizado que esté regulado por una autoridad de valores extranjera según lo define la sección 3(a)(50) de la Ley del Mercado de Valores de 1934 (15 USC 78c(a)(50)) (31 CFR 103.176(b)(3)).

  - La obtención y consideración de información relacionada con el programa contra el lavado de dinero del banco extranjero para analizar el riesgo de lavado de dinero que plantea la cuenta corresponsal del banco extranjero.
  - La supervisión de transacciones hacia la cuenta corresponsal, desde dicha cuenta o a través de ella, de una manera razonablemente diseñada para detectar las actividades sospechosas y de lavado dinero.
  - La obtención de información del banco extranjero sobre la identidad de cualquier persona con autoridad para efectuar transacciones a través de cualquier cuenta corresponsal que sea una cuenta empleada para pagos, y sobre las fuentes y el usufructuario de fondos u otros activos de la cuenta empleada para pagos.

- Determinar si el banco extranjero para el cual se mantiene la cuenta corresponsal a su vez mantiene cuentas corresponsales para otros bancos extranjeros que utilizan la cuenta corresponsal del banco extranjero y, de ser así, tome medidas razonables para obtener información relevante para analizar y mitigar los riesgos de lavado de dinero asociados con las cuentas corresponsales del banco extranjero para otros bancos extranjeros, incluida, de ser razonable, la identidad de dichos bancos extranjeros.

Además de esas categorías de bancos extranjeros identificados en el reglamento como entidades que requieren debida diligencia especial, puede ser conveniente que los bancos tomen medidas de debida diligencia adicionales con respecto a las instituciones financieras extranjeras identificadas mediante la aplicación del programa de debida diligencia general del banco como entidades que plantean un mayor riesgo de lavado de dinero. Dichas medidas pueden incluir alguno o todos los elementos de debida diligencia mejorada establecidos en el reglamento, según sea pertinente dependiendo de los riesgos planteados por la cuenta corresponsal extranjera específica.

Como también se indicó en la sección anterior sobre debida diligencia general, los recursos de un banco están dirigidos más adecuadamente a aquellas cuentas que plantean un riesgo de lavado de dinero más significativo. Consecuentemente, cuando se exige que un banco establezca (o de otro modo éste determina que es necesario establecer) debida diligencia especial con respecto a una cuenta corresponsal extranjera, el banco puede tener en cuenta los factores de análisis de riesgos tratados en la sección sobre debida diligencia general al determinar el alcance de la debida diligencia especial que será necesaria y adecuada para mitigar los riesgos planteados. Particularmente, el régimen de supervisión y contra el lavado de dinero de la jurisdicción que expidió la autorización para funcionar o licencia a la institución financiera extranjera, puede resultar en especial relevante en la determinación que realice el banco sobre el carácter y alcance de los riesgos planteados por una cuenta corresponsal extranjera y el alcance de la debida diligencia especial que se aplicará.

Procedimientos especiales cuando no se puede aplicar debida diligencia

Las políticas, los procedimientos y los controles de debida diligencia de un banco establecidos de conformidad con 31 CFR 103.176 deben incluir procedimientos que deberán seguirse en circunstancias en las que no pueda aplicarse adecuada debida diligencia o debida diligencia especial con respecto a una cuenta corresponsal extranjera, inclusive cuando el banco deba:

- Negarse a abrir la cuenta.
- Suspender actividades transaccionales.
- Presentar un SAR.
- Cerrar la cuenta.

Procedimientos de Inspección

Debida diligencia y gestión de registros de cuentas corresponsales extranjeras

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para cuentas corresponsales de bancos fantasmas extranjeros, gestión de registros de cuentas corresponsales extranjeras y programas de debida diligencia para detectar e informar acerca de actividades sospechosas y de lavado de dinero. Consulte las secciones ampliadas del manual para conocer análisis y procedimientos de inspección relacionados con los riesgos específicos de lavado de dinero en las cuentas corresponsales extranjeras.*

1. Determine si el banco participa en relaciones bancarias con corresponsales extranjeros.

Prohibición con respecto a bancos fantasmas extranjeros y gestión de registros de cuentas corresponsales extranjeras

2. Si es así, revise las políticas, procedimientos y procesos del banco. Como mínimo, las políticas, los procedimientos y los procesos deben lograr lo siguiente:

   - Prohibir negociaciones con bancos fantasmas extranjeros y especificar la parte responsable de obtener, actualizar y gestionar certificaciones o información para cuentas corresponsales extranjeras.
   - Identificar cuentas corresponsales extranjeras y encargarse del envío, seguimiento, recepción y control de las solicitudes de certificación o información.
   - Evaluar la calidad de la información recibida en respuesta a las solicitudes de certificación o información.
   - Determinar si debe presentarse un SAR y cuándo.
   - Mantener suficientes controles internos.
   - Proporcionar capacitación continua.
   - Realizar pruebas independientes del cumplimiento del banco con 31 CFR 103.177.

3. Determine si el banco tiene archivos de la certificación actual o información actual (que incluya de otro modo la información contenida en la certificación) para cada cuenta corresponsal extranjera que ayude a determinar si el banco corresponsal extranjero es o no un banco fantasma extranjero (31 CFR 103.177(a)).

4. Si el banco tiene sucursales en el extranjero, determine si ha tomado medidas razonables para garantizar que ninguna cuenta corresponsal mantenida para sus sucursales en el extranjero se utilice para prestar servicios bancarios indirectamente a bancos fantasma extranjeros.

Programa de debida diligencia especial para cuentas corresponsales extranjeras

5. Determine si el banco ha establecido un programa de debida diligencia general que incluya políticas, procedimientos y controles apropiados, específicos, en función del riesgo, y cuando sea necesario, especiales, para cuentas corresponsales establecidas, mantenidas, administradas o gestionadas en los Estados Unidos para instituciones financieras extranjeras ("cuentas corresponsales extranjeras"). El programa de debida diligencia general se debe aplicar a cada cuenta corresponsal extranjera. Verifique que las políticas, los procedimientos y los controles de debida diligencia incluyan:

   - La posibilidad de determinar si toda cuenta corresponsal extranjera está sujeta a debida diligencia especial (31 CFR 103.176(a)(1)).
   - El análisis de los riesgos de lavado de dinero presentados por la cuenta corresponsal extranjera (31 CFR 103.176(a)(2)).
   - La aplicación de procedimientos y controles en función del riesgo a cada cuenta corresponsal extranjera diseñados de manera razonable para detectar e informar de actividades de lavado de dinero de las que se sospeche o tenga conocimiento, incluido un control periódico de la actividad de la cuenta corresponsal suficiente para determinar la coherencia con la información obtenida acerca del tipo, propósito y actividad prevista de la cuenta (31 CFR 103.176(a)(3)).

6. Revise las políticas, los procedimientos y los procesos de debida diligencia que rigen el análisis de riesgos BSA/AML de las cuentas corresponsales extranjeras (31 CFR 103.176(a)(2)). Verifique que el programa de debida diligencia del banco considere los siguientes factores, según sea pertinente, como criterios en el análisis de riesgos:

   - El carácter de los negocios de la institución financiera extranjera y los mercados a los que presta servicios.
   - El tipo, el propósito y la actividad prevista de la cuenta corresponsal extranjera.
   - El carácter y duración de la relación del banco con la institución financiera extranjera y cualquiera de sus filiales.
   - El régimen AML y de supervisión de la jurisdicción que expidió la autorización para funcionar o licencia a la institución financiera extranjera y, en la medida que esa información con respecto a dicha jurisdicción esté razonablemente disponible, de la jurisdicción en la que cualquier compañía propietaria de la institución financiera extranjera está constituida o autorizada a funcionar.

- La información conocida o razonablemente al alcance del banco respecto al registro AML de la institución financiera extranjera.

7. Garantice que el programa está razonablemente diseñado para:
   - Detectar e informar, continuamente, acerca de actividades de lavado de dinero de las que se sospeche o tenga conocimiento.
   - Realizar controles periódicos de la actividad de las cuentas corresponsales para determinar la coherencia con la información obtenida acerca del tipo, propósito y actividad prevista de la cuenta.
8. Para los bancos extranjeros que estén sujetos a debida diligencia especial, evalúe los criterios que el banco estadounidense utiliza para protegerse contra el lavado de dinero, e informar acerca de actividades sospechosas relacionadas con toda cuenta corresponsal mantenida por dichos bancos extranjeros. Verifique que los procedimientos de debida diligencia especial se apliquen a cada cuenta corresponsal establecida por los bancos extranjeros que operan bajo:
   - Una licencia bancaria extraterritorial.
   - Una licencia bancaria expedida por un país extranjero que ha sido designado como no cooperante con los principios o procedimientos AML internacionales por un grupo u organización intergubernamental de la que los Estados Unidos sea miembro y con cuya designación esté de acuerdo el representante de Estados Unidos del grupo u organización.
   - Una licencia bancaria expedida por un país extranjero que ha sido designado por el Secretario del Tesoro como un país que requiere medidas especiales debido al peligro de AML.
9. Revise las políticas, procedimientos y procesos del banco y determine si incluyen medidas razonables para llevar a cabo un escrutinio especial de cuentas corresponsales extranjeras para protegerse contra el lavado de dinero y para identificar e informar toda transacción sospechosa de acuerdo con la normativa vigente (31 CFR 103.176(b)(1)). Verifique que este escrutinio especial refleje el análisis de riesgos de cada cuenta corresponsal extranjera que esté sujeta a dicho escrutinio e incluya, según sea pertinente:
   - La obtención y consideración de información relacionada con el programa contra el lavado de dinero del banco extranjero para analizar el riesgo de lavado de dinero planteado por la cuenta corresponsal del banco extranjero (31 CFR 103.176(b)(1)(i)).
   - La supervisión de transacciones hacia la cuenta corresponsal, desde dicha cuenta o a través de ella, de una manera razonablemente diseñada para detectar las actividades sospechosas y de lavado de dinero (31 CFR 103.176(b)(1)(ii)).
   - La obtención de información del banco extranjero sobre la identidad de cualquier persona con autoridad para efectuar transacciones a través de cualquier cuenta

corresponsal que sea una cuenta empleada para pagos, y sobre las fuentes y el usufructuario de fondos u otros activos de la cuenta empleada para pagos (31 CFR 103.176(b)(1)(iii)).

10 Revise las políticas, los procedimientos y los procesos del banco para determinar si los bancos corresponsales extranjeros sujetos a debida diligencia especial mantienen cuentas corresponsales para otros bancos extranjeros, y, de ser así, determine si las políticas, los procedimientos y los procesos del banco incluyen medidas razonables para obtener información relevante que ayude a analizar y mitigar los riesgos de lavado de dinero asociados a las cuentas corresponsales del banco corresponsal extranjero para otros bancos extranjeros. Esta información incluye, según sea pertinente, la identidad de esos bancos extranjeros (31 CFR 103.176(b)(2)).

11. Determine si las políticas, procedimientos y procesos exigen que el banco tome medidas razonables para identificar a cada uno de los propietarios con derecho al 10% de los votos o más sobre cualquier clase de valores de un banco corresponsal extranjero que no cotice en la bolsa de valores para el cual aquel banco abra o mantenga una cuenta sujeta a debida diligencia especial. Para dichas cuentas, evalúe las políticas, los procedimientos y los procesos del banco para determinar el interés de cada uno de tales propietarios (31 CFR 103.176(b)(3)).

Pruebas de transacciones

Prohibición con respecto a bancos fantasmas extranjeros y gestión de registros de cuentas corresponsales extranjeras

12. En función de un análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de cuentas de bancos extranjeros. De la muestra seleccionada, determine lo siguiente:

- Si las certificaciones e información de las cuentas están completas y son razonables.
- Si el banco tiene documentación adecuada para demostrar que no presta servicios indirectamente ni mantiene cuentas para bancos fantasmas extranjeros.
- Respecto a los cierres de cuenta, si se realizaron dentro de un período razonable y la relación no se volvió a establecer sin motivos suficientes.
- Si existen solicitudes de información respecto a cuentas corresponsales extranjeras por parte de alguna autoridad federal de aplicación de la ley. De ser así, cerciórese de que las solicitudes hayan sido cumplidas oportunamente.

- Si el banco recibió alguna notificación oficial para cerrar cuentas de instituciones financieras extranjeras.[116] Si es así, cerciórese de que las cuentas hayan sido cerradas dentro de los diez días hábiles.
- Si el banco conserva, durante cinco años desde la fecha de cierre de la cuenta, el original de todo documento proporcionado por una institución financiera extranjera, así como el original o una copia de cualquier documento válido relacionado con cualquier auto de comparecencia o citación de la institución financiera extranjera emitida bajo 31 CFR 103.185.

Programa de debida diligencia especial para cuentas corresponsales extranjeras

13. De una muestra seleccionada, determine si el banco sigue coherentemente sus políticas, procedimientos y procesos de debida diligencia para cuentas corresponsales extranjeras. Puede ser necesario expandir la muestra para incluir cuentas corresponsales mantenidas para instituciones financieras extranjeras que no sean bancos extranjeros (como transmisores de dinero o casas de cambio), según sea pertinente.

14. De la muestra original, determine si el banco ha implementado procedimientos de debida diligencia especial para bancos extranjeros que operan bajo:

    - Una licencia bancaria extraterritorial.
    - Una licencia bancaria emitida por un país extranjero que haya sido designado como no cooperante con los procedimientos o principios internacionales AML.
    - Una licencia bancaria expedida por un país extranjero que ha sido designado por el Secretario del Tesoro como un país que requiere medidas especiales debido al peligro de AML.

15. De una muestra de las cuentas que están sujetas a debida diligencia especial, verifique que el banco haya tomado medidas razonables, según sus políticas, procedimientos y procesos, para:

    - Determinar, respecto a cualquier banco extranjero cuyas acciones no coticen en la bolsa de valores, la identidad de cada uno sus propietarios con derecho al 10% de los votos o más sobre cualquier clase de valores de un banco, y el carácter y grado de la participación accionaria de tales propietarios.
    - Realizar un escrutinio especial de cualquier cuenta mantenida por dichos bancos para protegerse contra el lavado de dinero e informar actividades sospechosas.

[116] Las notificaciones oficiales para cerrar cuentas de instituciones financieras extranjeras deben ser firmadas por el Secretario del Tesoro o el Procurador General de los Estados Unidos (31 CFR 103.185(d)).

- Determinar si dicho banco extranjero proporciona cuentas corresponsales a otros bancos extranjeros y, de ser así, obtener información necesaria para analizar y mitigar riesgos de lavado de dinero asociados con cuentas corresponsales del banco extranjero para otros bancos extranjeros. La información deberá incluir, según sea pertinente, la identidad de esos bancos extranjeros.

16. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos para cumplir con las exigencias normativas asociadas con la gestión de registros y debida diligencia de cuentas corresponsales extranjeras.
17. En función de la conclusión anterior y los riesgos asociados con la actividad del banco en esta área, continúe con los procedimientos de inspección de la sección ampliada, si fuera necesario.

Programa de Debida Diligencia de la Banca Privada (Ciudadanos no Estadounidenses): Esquema General

Objetivo: *Analizar el cumplimiento del banco con las exigencias normativas y legales para implementar políticas, procedimientos y controles a fin de detectar e informar de actividades sospechosas y de lavado de dinero a través de cuentas de banca privada establecidas, administradas o mantenidas para ciudadanos no estadounidenses. Consulte las secciones ampliadas del manual para conocer análisis y procedimientos de inspección relacionados con los riesgos específicos de lavado de dinero asociados con la banca privada.*

La banca privada puede definirse en términos generales como la prestación de servicios financieros personalizados a clientes adinerados. La sección 312 de la Ley PATRIOTA de EE. UU. agregó la subsección (i) a 31 USC 5318 de la BSA. Esta subsección exige que cada institución financiera estadounidense que establezca, mantenga, administre o gestione una cuenta de banca privada en los Estados Unidos para un ciudadano no estadounidense tome ciertas medidas AML respecto a dichas cuentas. En particular, los bancos deben establecer políticas, procedimientos y controles apropiados, específicos y, cuando sea necesario, de debida diligencia especial, razonablemente diseñados para permitirles detectar e informar instancias de lavado de dinero efectuadas a través de esas cuentas. Además, la sección 312 exige un escrutinio especial para detectar y, si corresponde, informar transacciones que puedan implicar ingresos derivados de corrupción extranjera depositados en cuentas de banca privada que son solicitadas o mantenidas por políticos extranjeros de alto nivel o en nombre de éstos y por los miembros más cercanos de su familia y su círculo inmediato de colaboradores. El 4 de Enero de 2006, la FinCEN publicó un reglamento definitivo (31 CFR 103.178) que implementa las exigencias aplicables a la banca privada de 31 USC 5318(i).

El esquema general principal y los procedimientos de inspección establecidos en esta sección están destinados a evaluar el programa de debida diligencia del banco relacionado con las cuentas de banca privada ofrecidas a ciudadanos no estadounidenses. En los procedimientos de inspección ampliada "Banca privada", en las páginas 316 a 317, se incluyen procedimientos adicionales para áreas de riesgo específicas de la banca privada.

Cuentas de banca privada

A los fines de 31 CFR 103.178, una "cuenta de banca privada" es una cuenta (o una combinación de cuentas) mantenida en un banco que satisface los tres criterios siguientes:

- Exige un depósito acumulado de fondos mínimo u otros activos de no menos de USD 1.000.000.

- Está establecida en nombre o en beneficio de uno o más ciudadanos no estadounidenses que sean propietarios directos o usufructuarios[117] de la cuenta.

- Esté asignada o administrada, en parte o en su totalidad, por un funcionario, empleado o agente del banco que actúa como contacto entre la institución financiera objeto de la normativa y el propietario directo o usufructuario de la cuenta.

Con relación a la exigencia de depósito mínimo, "una cuenta de banca privada" es una cuenta (o combinación de cuentas) que *exige* un depósito mínimo de no menos de USD 1.000.000. Un banco puede ofrecer un amplio rango de servicios que reciba el nombre genérico de banca privada, y aun cuando algunos (o cualquier combinación o todos) de los servicios de banca privada del banco no *exigen* un depósito mínimo de no menos de USD 1.000.000, estas relaciones deben estar sujetas a un mayor nivel de debida diligencia bajo el programa de cumplimiento BSA/AML en función del riesgo del banco, pero no están sujetas a 31 CFR 103.178. Consulte la sección del esquema general ampliado, "Banca Privada", en las páginas 310 a 315, como guía.

Programa de debida diligencia

Un banco debe establecer y mantener un programa de debida diligencia que incluya políticas, procedimientos y controles que estén razonablemente diseñados para detectar e informar cualquier actividad sospechosa o de lavado de dinero de la que se sospeche o tenga conocimiento llevada a cabo a través de cualquier cuenta de banca privada para un ciudadano no estadounidense que esté establecida, mantenida, administrada o gestionada en los Estados Unidos por el banco. El programa de debida diligencia debe garantizar que, como mínimo, el banco tome medidas razonables para cumplir con las siguientes exigencias:

- Confirmar la identidad de todos los propietarios nominales o usufructuarios de una cuenta de banca privada.

- Confirmar si el propietario nominal o usufructuario de alguna cuenta de banca privada es una figura política extranjera de alto nivel.

- Confirmar el origen o los orígenes de los fondos depositados en una cuenta de banca privada y el propósito y uso previsto de la cuenta.

- Revisar la actividad de la cuenta para garantizar que sea coherente con la información obtenida acerca de la fuente de los fondos del cliente y con el propósito y uso previsto de la cuenta declarados, y presentar un SAR, según corresponda, para informar cualquier actividad sospechosa o de lavado de dinero de la que se sospeche

[117] "Usufructuario" de una cuenta es una persona que tiene un nivel de control sobre los fondos o activos depositados en la cuenta, o es titular de los mismos, de tal manera que, desde una perspectiva práctica, permita a la persona controlar, gestionar o dirigir la cuenta directa o indirectamente. La habilidad de financiar la cuenta o el derecho a los fondos de la cuenta por sí solo, sin embargo, sin la correspondiente autoridad para controlar, gestionar o dirigir la cuenta (como en el caso de un beneficiario menor de edad), no convierte a la persona en usufructuario (31 CFR 103.175(b)).

o tenga conocimiento llevada a cabo con destino a una cuenta de banca privada, desde una cuenta de banca privada o a través de ella.

Análisis de riesgos de cuentas de banca privada para ciudadanos no estadounidenses

El carácter y la extensión de la debida diligencia realizada en cuentas de banca privada para ciudadanos no estadounidenses varían en función del cliente y dependiendo de la presencia de factores de riesgo potencial. Aplicar una debida diligencia más exhaustiva, por ejemplo, puede ser apropiado para clientes nuevos, clientes que operan en jurisdicciones con controles AML débiles, o cuyos fondos se transmiten desde dichas jurisdicciones o a través de ellas. También puede ser apropiado respecto a clientes cuyos rubros de actividad comercial estén basados principalmente en moneda (p. ej., casinos o casas de cambio). La debida diligencia también debe ser acorde con el tamaño de la cuenta. Las cuentas con relativamente más depósitos y activos deben estar sujetas a una debida diligencia mayor. Además, si el banco en algún momento entra en conocimiento de información que pone en duda la información previa, será apropiado establecer debida diligencia adicional.

Confirmación del origen de los fondos y supervisión de la actividad de la cuenta

Los bancos que proporcionan servicios de banca privada por lo general obtienen información importante sobre sus clientes, que incluye el propósito para el cual el cliente establece la cuenta de banca privada. Esta información puede ser un valor de referencia sobre las actividades de la cuenta que permita al banco detectar mejor cualquier actividad sospechosa y analizar situaciones donde pueda ser necesaria verificación adicional respecto al origen de los fondos. No se espera que los bancos, en el curso ordinario de los negocios, verifiquen el origen de cada depósito colocado en cada cuenta de banca privada. Sin embargo, deben supervisar los depósitos y las transacciones cuando sea necesario para garantizar que la actividad sea coherente con la información que el banco ha recibido sobre el origen de los fondos del cliente y el propósito declarado y uso previsto de la cuenta. Dicha supervisión facilitará la identificación de las cuentas que requieran un escrutinio adicional.

Escrutinio especial de las cuentas de banca privada para políticos extranjeros de alto nivel

Para los propósitos de las cuentas de banca privada bajo 31 CFR 103.175(r), el reglamento define el término “político extranjero de alto nivel” incluyendo uno o más de los siguientes:

- Un actual o ex:
  - Funcionario de alto nivel de un órgano ejecutivo, legislativo, judicial, administrativo o militar de un gobierno extranjero (haya sido elegido o no).

  - Miembro de alto nivel de un partido político extranjero importante.
  - Ejecutivo de alto nivel de una empresa comercial que sea propiedad de un gobierno extranjero.[118]

- Una corporación, negocio, u otra entidad que haya sido constituida por dicho individuo o para su beneficio.
- Un familiar cercano de dicho individuo (incluidos cónyuge, padres, hermanos, hijos, y padres y hermanos del cónyuge).
- Una persona pública y comúnmente conocida por su íntima asociación respecto al funcionario de alto nivel (o cuya asociación sea conocida por el banco relevante).

Los políticos extranjeros de alto nivel definidos anteriormente con frecuencia se conocen como "personalidades sujetas a exposición política" o PEP, por sus siglas en inglés. Consulte la sección del esquema general ampliado "Personalidades sujetas a exposición política" en las páginas 329 a 333, como guía, particularmente con respecto a la debida diligencia en cuentas mantenidas para PEP que no cumplen con la definición normativa de "cuenta de banca privada" establecida en 31 CFR 103.175(o).

Para las cuentas de banca privada respecto a las cuales una figura política extranjera de alto nivel sea propietaria nominal o usufructuaria, el programa de debida diligencia del banco debe incluir un escrutinio especial diseñado razonablemente para detectar e informar transacciones que puedan implicar ingresos derivados de corrupción extranjera. El término "ingresos derivados de corrupción extranjera" se refiere a cualquier activo o propiedad que adquiera una figura política extranjera de alto nivel, se adquiera a través de ella o en su nombre, ya sea a través de malversación, hurto o apropiación indebida de fondos públicos, la apropiación ilegal de propiedad de un gobierno extranjero, o a través de actos de cohecho o extorsión. Incluye también cualquier otra propiedad en la que cualquiera de dichos activos se haya transformado o convertido.[119] En los casos en los que un banco presenta un SAR relacionado a una transacción que puede involucrar los

[118] A los propósitos de esta definición, los términos "funcionario de alto nivel" o "ejecutivo de alto nivel" significan una persona con autoridad sustancial sobre la política, las operaciones o el uso de los recursos que son propiedad del gobierno.

[119] Las señales de advertencia adicionales respecto a las transacciones que pueden relacionarse con los ingresos por corrupción extranjera están enumeradas en la *Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption* (Guía de escrutinio mejorado para transacciones que puedan involucrar a los funcionarios extranjeros por corrupción), emitida por el Tesoro de los Estados Unidos, la Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Oficina del Interventor Monetario, la Oficina de Supervisión de Instituciones de Ahorro y el Departamento de Estado, Enero de 2001.

[119] Consulte FIN-2008-G005, *Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption* (Guía para las instituciones financieras sobre la presentación de informes de actividades sospechosas con respecto a los ingresos derivados de corrupción extranjera) 17 de Abril de 2008, disponible en www.fincen.gov.

ingresos derivados de corrupción extranjera, la FinCEN ha indicado que los bancos deben incluir el término "corrupción extranjera" en la parte narrativa del SAR. [120]

El escrutinio mejorado de las cuentas de banca privada para políticos extranjeros de alto nivel debe basarse en el riesgo. Las medidas razonables para realizar un escrutinio especial pueden incluir la consulta de información disponible públicamente sobre el país de origen del cliente, la comunicación con sucursales del banco estadounidense que opere en el país de origen del cliente para obtener información adicional sobre el mismo y el entorno político y la realización de un escrutinio mayor de la historia laboral y las fuentes de ingreso del cliente. Por ejemplo, las transferencias de fondos desde una cuenta gubernamental a la cuenta personal de un funcionario de gobierno con autoridad de firma sobre la cuenta gubernamental pueden generar sospecha del banco de posible corrupción política. Además, si un control del banco de fuentes de noticias importantes indica que el cliente puede estar o está involucrado en corrupción política, el banco debe revisar la cuenta del cliente para detectar actividad poco habitual.

Identificación de políticos extranjeros de alto nivel

Se exige que los bancos establezcan políticas, procedimientos y controles que incluyan medidas razonables para confirmar la condición de político extranjero de alto nivel de una persona. Los procedimientos deben exigir la obtención de información respecto al empleo y otras fuentes de ingresos, y el banco debe recabar información directamente del cliente respecto a su posible condición de político extranjero de alto nivel. El banco debe también verificar las referencias, según sea pertinente, para determinar si el individuo tiene o ha tenido previamente un puesto político de alto nivel o es un íntimo asociado de un político extranjero de alto nivel. Además, el banco debe hacer todo lo posible para revisar las fuentes públicas de información con respecto al cliente.

Los bancos que apliquen procedimientos de debida diligencia razonables según 31 CFR 103.178 pueden no ser siempre capaces de identificar a las personas que califican como políticos extranjeros de alto nivel, y, en particular, a sus colaboradores cercanos, y por lo tanto no poder aplicar un escrutinio especial a todas sus cuentas. Si el programa de debida diligencia del banco está razonablemente diseñado para tomar esta determinación, y el banco administra este programa de manera eficaz, el banco debería generalmente ser capaz de detectar, informar y tomar medidas adecuadas cuando se sospeche que existe lavado de dinero en relación con estas cuentas, aun en los casos en que no haya podido identificar al titular de la cuenta como político extranjero de alto nivel que requiera un escrutinio especial.

---

[120] Consulte la carta informativa FIN-2008-G005, *Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption* (Guía para las instituciones financieras sobre la presentación informes de actividades sospechosas relacionadas con los fondos provenientes de corrupción extranjera), del 17 de Abril de 2008, disponible en www.fincen.gov.

Procedimientos especiales cuando no se puede aplicar debida diligencia

Las políticas, procedimientos y controles de debida diligencia de un banco establecidos de conformidad con 31 CFR 103.178(a) deben incluir procedimientos especiales para cuando la apropiada debida diligencia no se pueda aplicar. Estos procedimientos especiales deben incluir los casos en que el banco deba:

- Negarse a abrir la cuenta.
- Suspender actividades transaccionales.
- Presentar un SAR.
- Cerrar la cuenta.

Procedimientos de Inspección

Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)

Objetivo: *Analizar el cumplimiento del banco con las exigencias normativas y legales para implementar políticas, procedimientos y controles a fin de detectar e informar de actividades sospechosas y de lavado de dinero a través de cuentas de banca privada establecidas, administradas o mantenidas para ciudadanos no estadounidenses. Consulte las secciones ampliadas del manual para conocer análisis y procedimientos de inspección relacionados con los riesgos específicos de lavado de dinero asociados con la banca privada.*

1. Determine si el banco ofrece cuentas de banca privada de acuerdo con la definición normativa de una cuenta de banca privada. Una cuenta de banca privada significa una cuenta (o cualquier combinación de cuentas) mantenida en una institución financiera cubierta por el reglamento que satisface los tres criterios siguientes:

   - Exige un depósito acumulado de fondos mínimo u otros activos de no menos de USD 1.000.000 (31 CFR 103.175(o)(1)).
   - Está establecida en nombre o en beneficio de uno o más ciudadanos no estadounidenses que sean propietarios directos o usufructuarios de la cuenta (31 CFR 103.175(o)(2)).
   - Está asignada, administrada o gestionada por, en parte o en su totalidad, un funcionario, empleado o agente del banco que actúa como coordinador entre el banco y el propietario directo o usufructuario de la cuenta (31 CFR 103.175(o)(3)).

   La reglamentación definitiva refleja la definición legal que se encuentra en la Ley PATRIOTA de EE. UU. Si una cuenta satisface los dos últimos criterios de la definición de cuenta de banca privada que se describen anteriormente, pero la institución no exige un saldo mínimo de USD 1.000.000, la cuenta no califica como cuenta de banca privada bajo esta norma. Sin embargo, la cuenta está sujeta a los controles internos y debida diligencia en función del riesgo incluidos en el programa de cumplimiento BSA/AML general de la institución.[121]

2. Determine si el banco ha implementado políticas, procedimientos y controles de debida diligencia para cuentas de banca privada establecidas, mantenidas, administradas o gestionadas en los Estados Unidos por el banco para ciudadanos no estadounidenses. Determine si las políticas, los procedimientos y los controles están razonablemente diseñados para detectar e informar cualquier actividad sospechosa o de lavado de dinero de la que se sospeche o tenga conocimiento llevada a cabo a través de cualquier cuenta de banca privada o que involucre esta clase de cuenta.

[121] Consulte los procedimientos de inspección ampliada, “Banca privada” y “Personalidades sujetas a exposición política” (PEP), en las páginas 316 a 317 y 334 a 335, respectivamente, como guía.

3. Revise las políticas, los procedimientos y los procesos del banco para analizar si el programa de debida diligencia del banco incluye medidas razonables para:

   - Confirmar la identidad de los propietarios nominales o usufructuarios de una cuenta de banca privada (31 CFR 103.178(b)(1)).
   - Confirmar si cualquier propietario nominal o usufructuario de una cuenta de banca privada es una figura política extranjera de alto nivel (31 CFR 103.178(b)(2)).
   - Confirmar la fuente o las fuentes de fondos depositados en la cuenta de banca privada y el propósito y uso previsto de la cuenta de banca privada para ciudadanos no estadounidenses (31 CFR 103.178(b)(3)).
   - Revise la actividad de la cuenta para asegurarse de que sea coherente con la información obtenida acerca de la fuente de los fondos del cliente y con el propósito y uso previsto de la cuenta declarados, según sea necesario, para protegerse del lavado de dinero e informar de cualquier actividad sospechosa o de lavado de dinero de la que se sospeche o tenga conocimiento llevada a cabo con destino a una cuenta de banca privada para ciudadanos no estadounidenses, desde una de tales cuentas o a través de ella (31 CFR 103.178(b)(4)).

4. Revise las políticas, los procedimientos y los procesos del banco para llevar a cabo un escrutinio especial para analizar si fueron razonablemente diseñados para detectar e informar transacciones que puedan involucrar ingresos derivados de corrupción extranjera[122] de los que una figura política extranjera de alto nivel[123] sea propietaria nominal o usufructuaria (31 CFR 103.178(c)(1)).

Pruebas de transacciones

5. En función del análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de archivos de clientes para determinar si el banco ha confirmado la identidad de los propietarios nominales o usufructuarios de cuentas de banca privada para ciudadanos no

[122] El término "ingresos derivados de corrupción extranjera" se refiere a cualquier activo o propiedad que adquiera una figura política extranjera de alto nivel, se adquiera a través de ella o en su nombre, ya sea a través de malversación, hurto o apropiación indebida de fondos públicos, la apropiación ilegal de propiedad de un gobierno extranjero, o a través de actos de cohecho o extorsión. Incluye también cualquier otra propiedad en la que cualquiera de dichos activos se haya transformado o convertido (31 CFR 103.178(c)(2)).

[123] La norma definitiva define a una figura política extranjera de alto nivel como: un funcionario de alto nivel que fue o es miembro de un órgano ejecutivo, legislativo, judicial, militar o administrativo de un gobierno extranjero, haya sido o no elegido para esa función; un miembro de alto nivel de un partido político extranjero importante; o un ejecutivo de alto nivel de una empresa comercial que sea propiedad de un gobierno extranjero. La definición también incluye una corporación, negocio u otra entidad formada por dicho individuo o en su beneficio. Los ejecutivos de alto nivel son individuos con autoridad sustancial sobre la política, las operaciones o el uso de los recursos que son propiedad del gobierno. También se incluye en la definición de funcionario político extranjero de alto nivel a los familiares cercanos de dichos individuos, y las personas que son pública y comúnmente conocidas por su íntima asociación respecto a la figura política extranjera de alto nivel.

estadounidenses y la fuente de los fondos depositados en tales cuentas. De la muestra seleccionada determine lo siguiente:

- Si los procedimientos del banco cumplen con las políticas internas y las exigencias legales.
- Si el banco ha cumplido sus procedimientos que rigen el análisis de riesgos de las cuentas de banca privada para ciudadanos no estadounidenses.
- Si el banco realiza un escrutinio especial de las cuentas de banca privada de las cuales las figuras políticas extranjeras de alto nivel son propietarias nominales o usufructuarias, coherente con su política, sus directrices normativas y exigencias legales.

6. En función de los procedimientos de inspección llevados a cabo, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos de cumplir con las exigencias normativas asociadas a programas de debida diligencia de banca privada.
7. En función de la conclusión anterior y los riesgos asociados con la actividad del banco en esta área, continúe con los procedimientos de inspección de la sección ampliada, si fuera necesario.

Medidas Especiales: Esquema General

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para las medidas especiales expedidas bajo la sección 311 de la Ley PATRIOTA de EE. UU.*

La sección 311 de la Ley PATRIOTA de EE. UU. incluyó 31 USC 5318A a la BSA, que autoriza al Secretario del Tesoro de los Estados Unidos a exigir a las instituciones financieras nacionales y agencias financieras nacionales tomar ciertas medidas especiales respecto a las jurisdicciones extranjeras, las instituciones financieras extranjeras, las clases de transacciones internacionales o tipos de cuentas de interés principal con relación al lavado de dinero. La sección 311 proporciona al Secretario del Tesoro una variedad de opciones que se pueden adaptar para tratar específicamente los peligros de financiamiento del terrorismo y de lavado de dinero. La sección 311 se implementa mediante varias ordenanzas y reglamentos que se incorporaron a 31 CFR 103.[124] Según se estipula en la sección 311, una ordenanza puede imponer ciertas medidas especiales sin notificación pública y derecho a audiencia previa, pero dichas ordenanzas deben tener una duración limitada y deben expedirse junto con una Notificación sobre Reglamentaciones Propuestas.

La sección 311 establece un proceso que el Secretario del Tesoro debe seguir e identifica las agencias federales a las que éste debe consultar antes de decidir si una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta es de interés principal con respecto al lavado de dinero. La ley también proporciona procedimientos similares, incluidos factores y exigencias de consulta, para seleccionar las medidas especiales específicas que se impondrán contra una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta que sea de interés principal con respecto al lavado de dinero.

Es importante tener en cuenta que, aunque una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta pueda ser designada como de interés principal con respecto al lavado de dinero en una ordenanza expedida junto con una Notificación sobre Reglamentaciones Propuestas, las medidas especiales de duración ilimitada sólo pueden imponerse mediante una reglamentación definitiva expedida luego de que se emita una notificación y se otorgue el derecho a audiencia.

Tipos de medidas especiales

Las siguientes cinco medidas especiales pueden imponerse individualmente, en conjunto o en cualquier combinación:

---

[124] Las notificaciones sobre reglamentaciones propuestas y reglamentación definitiva que acompañan la determinación de ser "de interés principal con respecto al lavado de dinero" y la imposición de medidas especiales de conformidad con la sección 311 de la Ley PATRIOTA de EE. UU., están disponibles en el sitio web de FinCEN, www.fincen.gov.

Gestión de registros y presentación de informes de ciertas transacciones financieras

Bajo la primera medida especial, es posible que se exija a los bancos que mantengan registros o presenten informes, o ambos, acerca de la cantidad de transacciones acumuladas o los detalles concretos de cada transacción con respecto a una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta que sea de interés principal con respecto al lavado de dinero. La ley contiene exigencias mínimas con respecto a la información de esos registros e informes, y permite que el Secretario del Tesoro imponga exigencias adicionales.

Información relacionada con el usufructo

Bajo la segunda medida especial, es posible que se exija a los bancos que tomen medidas razonables y prácticas, según lo determina el Secretario del Tesoro, para obtener y conservar información sobre el usufructo de cualquier cuenta abierta o mantenida en los Estados Unidos por un ciudadano extranjero (que no sea una entidad extranjera cuyas acciones estén sujetas a exigencias con respecto a la presentación de informes públicos o estén registradas o se coticen en una bolsa de valores o un mercado regulado), o un representante de dicho ciudadano extranjero, que involucre una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta que sea de interés principal con respecto al lavado de dinero.

Información sobre ciertas cuentas empleadas para pagos

Bajo la tercera medida especial, a los bancos que abren o mantienen una cuenta empleada para pagos en los Estados Unidos que involucre una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta que sea de interés principal con respecto al lavado de dinero se les puede exigir (i) que identifiquen a cada cliente (y representante) al que se le permita utilizar la cuenta o cuyas transacciones se envíen a través de la cuenta y (ii) que obtengan información sobre cada cliente (y representante) que sea comparable sustancialmente a la que el banco obtiene en el transcurso normal de los negocios sobre sus clientes que residen en los Estados Unidos.[125]

Información sobre ciertas cuentas corresponsales

Bajo la cuarta medida especial, a los bancos que abren o mantienen una cuenta corresponsal en los Estados Unidos que involucre una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta que sea de interés principal con respecto al lavado de dinero se les puede exigir: (i) que identifiquen a cada cliente (y representante) al que se le permita utilizar la cuenta o cuyas transacciones se envíen a través de la cuenta y (ii) que obtengan información sobre cada cliente (y representante) que sea comparable

[125] Consulte la sección del esquema general ampliado, “Cuentas empleadas para pagos”, en las páginas 221 a 223, como guía.

sustancialmente a la que una institución de depósito de los Estados Unidos obtiene en el transcurso normal de los negocios sobre sus clientes que residen en los Estados Unidos.[126]

Prohibiciones o condiciones con respecto a la apertura o mantenimiento de ciertas cuentas corresponsales o empleadas para pagos

Bajo la quinta, y más firme, medida especial, es posible que a los bancos se les prohíba abrir o mantener en los Estados Unidos cualquier cuenta corresponsal o empleada para pagos para una institución financiera extranjera o en nombre de ésta, si la cuenta involucra una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta que sea de interés principal con respecto al lavado de dinero. La imposición de esta medida puede prohibir a los bancos estadounidenses establecer, mantener, administrar o gestionar en dicho país una cuenta corresponsal o empleada para pagos para cualquier institución financiera de una jurisdicción extranjera específica o en nombre de cualquiera de dichas instituciones. Esta medida también puede aplicarse a instituciones financieras extranjeras específicas y a sus subsidiarias.

Los reglamentos que implementan estas prohibiciones pueden exigir a los bancos que controlen sus registros de cuentas para determinar si mantienen alguna cuenta directamente para dichas entidades o en nombre de ellas. Además de las prohibiciones directas, es posible que a los bancos se les:

- Prohíba proporcionar deliberadamente acceso indirecto a las entidades específicas mediante sus otras relaciones bancarias.
- Exija notificar a los titulares de cuentas corresponsales que no deben proporcionar a la entidad específica acceso a la cuenta mantenida en el banco estadounidense.
- Exija que tomen medidas razonables para identificar cualquier uso indirecto de sus cuentas por parte de la entidad específica.

Guía sobre medidas especiales

Las ordenanzas y reglamentos que implementan las medidas especiales específicas tomadas bajo la sección 311 de la Ley PATRIOTA de EE. UU. no son estáticas; se pueden expedir o revocar con el transcurso del tiempo a medida que el Secretario del Tesoro determine que la jurisdicción, institución, clase de transacciones o tipo de cuenta en cuestión ya no es de interés principal con respecto al lavado de dinero. Además, las medidas especiales impuestas contra una jurisdicción, institución, clase de transacciones o tipo de cuenta pueden variar de aquellas impuestas en otras situaciones. Los inspectores también deben tener en cuenta que una ordenanza o norma que imponga una medida

[126] Consulte la sección del esquema general principal, "Debida diligencia y gestión de registros de cuentas corresponsales extranjeras", en las páginas 130 a 138, y la sección del esquema general ampliado, "Cuentas corresponsales (extranjeras)", en las páginas 204 a 207, como guía.

especial puede establecer un estándar de debida diligencia que los bancos deberán aplicar para cumplir con la medida especial específica.

Consecuentemente, este manual no describe medidas especiales definitivas específicas, ya que toda lista rápidamente se vuelve obsoleta. Los inspectores que controlen el cumplimiento de esta sección deben visitar el sitio web de la FinCEN en www.fincen.gov para obtener información actual sobre las medidas especiales definitivas. Los inspectores sólo deben realizar sus inspecciones teniendo en cuenta aquellas medidas especiales que sean definitivas y no aquellas que hayan sido propuestas.

Procedimientos de Inspección

Medidas especiales

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para las medidas especiales expedidas bajo la sección 311 de la Ley PATRIOTA de EE. UU.*

1. Determine el grado en que el banco lleva a cabo actividades bancarias internacionales y las jurisdicciones extranjeras en las que el banco realiza transacciones y actividades, con especial énfasis en los bancos corresponsales extranjeros y las cuentas empleadas para pagos.

2. Según corresponda, determine si el banco ha establecido políticas, procedimientos y procesos para responder a medidas especiales específicas impuestas por la FinCEN que sean aplicables a sus operaciones. Evalúe la aptitud de las políticas, los procedimientos y los procesos para detectar cuentas o transacciones con jurisdicciones, instituciones financieras o transacciones sujetas a medidas especiales definitivas.

3. Determine, mediante conversaciones con la gerencia y el control de la documentación del banco, si éste ha establecido pautas en respuesta a las medidas especiales definitivas.

Pruebas de transacciones

4. Determine todas las medidas especiales definitivas expedidas por la FinCEN bajo la sección 311 que sean aplicables al banco (visite www.fincen.gov).

5. Para cualquiera de los primeros cuatro tipos de medidas especiales, determine si el banco obtuvo, registró o comunicó la información exigida por cada medida especial en particular.

6. Respecto a la quinta medida especial (prohibición), determine si el banco cumplió con las prohibiciones o restricciones exigidas por cada medida especial en particular y cumplió con cualquier otra pauta exigida por las medidas especiales.

7. Según sea necesario, realice una búsqueda en los sistemas de información de gestión (MIS, por sus siglas en inglés) del banco y en otros registros adecuados, de cuentas o transacciones con jurisdicciones, instituciones financieras, o transacciones sujetas a las medidas especiales definitivas.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos de cumplir con las exigencias normativas asociadas con las medidas especiales.

Presentación de Informes de Cuentas de Banco y Financieras en un Banco del Extranjero: Esquema General

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para la presentación de informes de cuentas de banco y financieras en un banco del extranjero.*

Cada persona[127] (incluido un banco) sujeta a la jurisdicción de los Estados Unidos con intereses financieros o autoridad de firma sobre un banco, valores u otras cuentas financieras en un país extranjero debe presentar un Informe de cuentas bancarias y financieras extranjeras (FBAR, por sus siglas en inglés) (TD F 90-22.1) ante el IRS si el valor acumulado de estas cuentas financieras supera los USD 10.000 en cualquier momento durante el año calendario.[128] Como se aclara en el formulario del FBAR revisado, publicado por el IRS en Octubre de 2008 y que se debe usar después del 31 de Diciembre de 2008, el término "cuenta financiera" generalmente incluye, entre otras cosas, cuentas en las que los activos se mantienen en un fondo combinado y el propietario de la cuenta mantiene una participación accionaria en el fondo (p. ej., un fondo común), así como cuentas de tarjeta prepagadas y tarjeta de débito.

El 7 de Agosto de 2009, el IRS emitió la Notificación 2009-62, que indicaba que el IRS pretendía emitir reglamentos que aclaren aún más la aplicabilidad de las exigencias del FBAR a los ciudadanos estadounidenses con sólo autoridad de firma sobre (pero no intereses financieros) una cuenta financiera extranjera, así como a ciudadanos estadounidenses con intereses financieros o autoridad de firma sobre fondos combinados extranjeros. Por consiguiente, con respecto a estos dos tipos de cuentas financieras extranjeras, el IRS extendió la fecha límite para la presentación del FBAR para ciudadanos estadounidenses para el 2008 y años calendarios anteriores hasta el 30 de Junio de 2010.

---

[127] Según se define en 31 CFR 103.11(z), el término "persona" se refiere a una persona física, una corporación, una sociedad, un fideicomiso o estado, una sociedad anónima, una asociación, un sindicato, una sociedad conjunta u otro grupo u organización no incorporado, una tribu indígena (según se define el término en la Ley Regulatoria del Juego Indio) y todas las entidades consideradas personas jurídicas. Las instrucciones para el FBAR establecen además que el término "ciudadano estadounidense" significa un ciudadano o residente de los Estados Unidos o una persona que se encuentra dentro de los Estados Unidos y hace negocios en dicho país. El IRS ha indicado que generalmente una persona no se considera que "se encuentra dentro de los Estados Unidos y hace negocios en dicho país" a menos que esa persona lleve a cabo negocios dentro de los Estados Unidos de manera regular y continua. Consulte *FAQs Regarding Report of Foreign Bank and Financial Accounts (FBAR)* (Preguntas frecuentes relacionadas con el Informe de cuentas bancarias y financieras extranjeras [FBAR]), 12 de Febrero de 2009, www.irs.gov/businesses/small/article/0,,id=148845,00.html#UPS1. Además, en el Anuncio 2009-51, 2009-25 I.R.B. 1105, emitido el 5 de Junio de 2009, el IRS indicó que había suspendido temporalmente la exigencia de presentación del FBAR para personas que no sean ciudadanos, residentes o entidades domésticas estadounidenses.

[128] 31 CFR 103.24.

Un banco debe presentar este formulario para sus propias cuentas que encuadren en esta definición; además, es posible que se obligue al banco a presentar estos formularios para cuentas de clientes en las que tenga intereses financieros o sobre las cuales tenga autoridad de firma u otra.

Se debe presentar un FBAR ante el comisionado del IRS el 30 de Junio, o antes de esa fecha, de cada año calendario para las cuentas financieras extranjeras cuyo valor acumulado supere los USD 10.000 en cualquier momento durante el año calendario anterior.

Procedimientos de Inspección

Presentación de informes de cuentas de banco y financieras en un banco del extranjero

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para la presentación de informes de cuentas de banco y financieras en un banco del extranjero.*

1. Determine si el banco tiene intereses financieros o autoridad de firma u otra forma de autorización sobre un banco, valores, o cualquier otra cuenta financiera en un país extranjero, y si se le exige al banco presentar un formulario del Informe de cuentas bancarias y financieras extranjeras (FBAR) (TD F 90-22.1) para cuentas de clientes, incluidas cuentas fiduciarias, en las que el banco tenga intereses financieros o sobre la cual tenga autoridad de firma u otra autoridad.

2. Si procede, revise las políticas, los procedimientos y los procesos del banco para presentar informes anuales.

Pruebas de transacciones

3. En función de un análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione una muestra de las cuentas para determinar si el banco ha completado, enviado y conservado de manera adecuada las copias de los formularios del FBAR.

4. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos de cumplir con las exigencias normativas asociadas con los FBAR.

Presentación de Informes sobre el Transporte Internacional de Moneda o Instrumentos Monetarios: Esquema General

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para la presentación de informes sobre envíos internacionales de moneda o instrumentos monetarios.*

Toda persona[129] (incluido un banco) que físicamente transporte o envíe por correo o de otra forma moneda o instrumentos monetarios por un valor superior a los USD 10.000 en un solo envío dirigido hacia el extranjero o hacia los Estados Unidos (y toda persona que genere de dicho transporte o envío por correo o de otra forma) debe presentar un Informe sobre el transporte internacional de moneda o instrumentos monetarios (CMIR, por sus siglas en inglés) (Formulario de FinCEN 105).[130] El CMIR se debe presentar ante un funcionario de la Oficina de Aduanas y Protección de las Fronteras correspondiente o ante el comisionado de la Aduana en el momento de ingresar o salir de los Estados Unidos. Cuando una persona reciba moneda o instrumentos monetarios por un monto superior a los USD 10.000 en un mismo envío, que hayan sido enviados desde cualquier lugar fuera de los Estados Unidos, se debe presentar un CMIR ante la Oficina de Aduanas y Protección de las Fronteras adecuada o ante el comisionado de Aduana dentro de los 15 días siguientes a la recepción de los instrumentos (a menos que ya se haya presentado un informe). El informe debe ser realizado por la persona que solicita la transferencia de moneda o instrumentos monetarios o en nombre de la misma. Sin embargo, no se exige que los bancos presenten este informe si el envío se realiza por medio del servicio postal o transporte público.[131] Además, un banco comercial o compañía fiduciaria organizada bajo las leyes de los Estados Unidos o cualquiera de sus estados no tiene la obligación de informar los envíos de moneda o instrumentos monetarios realizados por vía terrestre, si los remite o recibe un cliente establecido que tiene una relación de depósito con el banco

[129] Según se define en 31 CFR 103.11(z), el término "persona" se refiere a una persona física, una corporación, una sociedad, un fideicomiso o estado, una sociedad anónima, una asociación, un sindicato, una sociedad conjunta u otro grupo u organización no incorporado, una tribu indígena (según se define el término en la Ley Regulatoria del Juego Indio) y todas las entidades consideradas personas jurídicas.

[130] Únicamente la persona que recibe, transporta, envía por correo o de otra forma, o la que genera o intenta generar dicha recepción, el transporte o envío por correo o de otra forma, está obligada a presentar el CMIR. Ninguna otra persona tiene la obligación de presentar un CMIR. Por lo tanto, si un cliente ingresa al banco y declara haber recibido o transportado moneda en un monto acumulado superior a los USD 10.000 desde un lugar ubicado fuera de los Estados Unidos y desea depositar dicho monto en su cuenta, el banco no tiene obligación de presentar un CMIR a nombre del cliente (Dictamen Administrativo 88-2 expedido por el Tesoro).

[131] Por otra parte, los bancos deben presentar el CMIR para informar sobre envíos de moneda o instrumentos monetarios a oficinas en el extranjero cuando esos envíos los realice directamente personal del banco, como en el caso de envíos de moneda hechos por empleados del banco en los que se usan vehículos de su propiedad.

y si el banco concluye razonablemente que los montos no exceden lo que corresponde a las prácticas comunes del negocio, industria o profesión del cliente en cuestión.

La gerencia debe implementar políticas, procedimientos y procesos aplicables a la presentación de los CMIR. La gerencia debe revisar el transporte internacional de moneda e instrumentos monetarios y determinar si la actividad del cliente es habitual y se acostumbra en el tipo de actividad comercial. En el caso de que no sea así, se debe considerar la presentación de un SAR.

Procedimientos de Inspección

Presentación de informes sobre el transporte internacional de moneda o instrumentos monetarios

Objetivo: *Evaluar el cumplimiento del banco con las exigencias normativas y legales para la presentación de informes sobre envíos internacionales de moneda o instrumentos monetarios.*

1. Determine si el banco ha trasladado físicamente (o ha hecho que se traslade), enviado por correo u otro medio, moneda u otros instrumentos monetarios por un valor superior a USD 10.000 en un mismo envío hacia afuera de los Estados Unidos, o si el banco ha recibido moneda u otros instrumentos monetarios por un valor superior a USD 10.000, en un mismo envío, que hayan sido trasladados físicamente, enviados por correo u otro medio hacia adentro de los Estados Unidos.

2. Si procede, revise las políticas, los procedimientos y los procesos del banco para presentar un Informe sobre el transporte internacional de moneda o instrumentos monetarios (CMIR) (Formulario 105 de la FinCEN) por cada envío de moneda u otros instrumentos monetarios por un valor superior a USD 10.000 hacia afuera o hacia adentro de los Estados Unidos (excepto por los envíos realizados por correo postal, transporte público u otro medio de transporte exceptuado de la presentación de CMIR).

Pruebas de transacciones

3. En función del análisis de riesgos, los informes de inspección previos y un control de los resultados de la auditoría del banco, seleccione una muestra de las transacciones realizadas luego de la inspección previa para determinar si el banco ha completado, enviado y conservado de manera adecuada las copias de los formularios del CMIR.

4. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la capacidad de las políticas, los procedimientos y los procesos de cumplir con las exigencias normativas asociadas a los CMIR.

5. En función de la conclusión anterior y los riesgos asociados con la actividad del banco en esta área, continúe con los procedimientos de inspección de la sección ampliada, si fuera necesario.

Oficina de Control de Activos Extranjeros: Esquema General

Objetivo: *Evaluar el programa de cumplimiento en función del riesgo del banco según la Oficina de Control de Activos Extranjeros (OFAC) para analizar si es adecuado al riesgo del banco según la OFAC, teniendo en cuenta sus productos, servicios, clientes, entidades, transacciones y ubicaciones geográficas.*

La OFAC es una oficina del Tesoro de los Estados Unidos que administra e impone sanciones económicas y comerciales basadas en la política exterior estadounidense y sus objetivos de seguridad nacional; dichas sanciones están dirigidas a países extranjeros, terroristas y narcotraficantes internacionales, y a aquellos que participen en actividades relacionadas con la proliferación de armas de destrucción masiva.

La OFAC actúa según las facultades especiales otorgadas al Presidente en tiempos de guerra y emergencia nacional, así como bajo la autorización otorgada por legislación específica para imponer controles a las transacciones y congelar activos que estén bajo la jurisdicción estadounidense. Muchas de las sanciones se basan en mandatos de Naciones Unidas y otros mandatos internacionales, son multilaterales en cuanto a su campo de aplicación, y suponen estrecha cooperación con gobiernos de países aliados. Otras sanciones protegen exclusivamente intereses de los Estados Unidos. El Secretario del Tesoro le ha delegado a la OFAC la responsabilidad de desarrollar, promulgar y administrar los programas de sanciones de los EE. UU.[132]

El 9 de Noviembre de 2009, la OFAC emitió una reglamentación final denominada *Economic Sanctions Enforcement Guidelines* (Pautas de aplicación de sanciones económicas) para proporcionar orientación a personas sujetas a sus reglamentos. El documento explica los procedimientos que la OFAC sigue en la determinación de la respuesta adecuada respecto de aplicación para violaciones aparentes a sus reglamentos. Algunas respuestas respecto de la aplicación pueden ocasionar la emisión de una sanción civil que, según el programa de sanciones afectado, puede representar hasta USD 250.000 por violación o el doble de la cantidad de una transacción, el importe que sea mayor. Las Pautas describen los diversos

[132] Ley de Comercio con el Enemigo (TWEA, por sus siglas en inglés), 50 USC App 1-44; Ley de Poderes de Emergencia Económica Internacional (IEEPA, por sus siglas en inglés), 50 USC 1701 *et seq*.; Ley sobre Antiterrorismo y Pena de Muerte Efectiva (AEDPA, por sus siglas en inglés), 8 USC 1189, 18 USC 2339B; Ley de Participación de las Naciones Unidas (UNPA, por sus siglas en inglés), 22 USC 287c; Ley sobre Democracia Cubana (CDA, por sus siglas en inglés), 22 USC 6001-10; Ley de Libertad y Solidaridad Democrática con Cuba (Ley *Libertad*), 22 USC 6021-91; Ley de Comercio de Diamantes Limpios, Pub L. No. 108-19; Ley de Designación de Personas Claves del Narcotráfico Extranjero (Ley *Kingpin*) 21 USC 1901-1908,8 USC 1182; Ley de Libertad y Democracia en Birmania de 2003, Pub. L. No. 108-61, 117 Stat. 864 (2003); Ley de Apropiaciones de Operaciones Extranjeras, Financiación de Exportaciones y Programas Relacionados, Sec 570 de Pub. L. No. 104-208, 110 Stat. 3009-116 (1997); Ley de Sanciones a Irak, Pub. L. No. 101-513, 104 Stat. 2047-55 (1990); Ley de Cooperación en la Seguridad Internacional y el Desarrollo, 22 USC 2349 aa8-9; Ley de Reforma a las Sanciones Comerciales y Mejoramiento de la Exportación de 2000, Título IX, Pub. L, No. 106-387 (28 de Octubre de 2000).

factores que la OFAC toma en cuenta al tomar determinaciones respecto de la aplicación, especialmente la aptitud de un programa de cumplimiento en vigencia dentro de una institución para garantizar el cumplimiento con los reglamentos de la OFAC.[133]

Todas las personas de EE. UU.,[134] incluidos los bancos, las sociedades de control de bancos y las subsidiarias no bancarias estadounidenses deben cumplir con los reglamentos de la OFAC.[135] Las agencias bancarias federales evalúan los sistemas de cumplimiento con la OFAC para garantizar que todos los bancos sujetos a su supervisión cumplan con las sanciones.[136] A diferencia de la BSA, las normativas emitidas por la OFAC se aplican no sólo a los bancos estadounidenses y sus sucursales nacionales, agencias estadounidenses e instituciones bancarias internacionales, sino también a sus sucursales extranjeras, y con frecuencia a sus oficinas y subsidiarias en el exterior. Generalmente, los reglamentos exigen lo siguiente:

- Bloquear cuentas y otras propiedades de los países, entidades y personas físicas específicadas.
- Prohibir o rechazar el comercio y las transacciones financieras sin licencia con países, entidades y personas físicas específicadas.

Transacciones bloqueadas

La ley estadounidense exige bloquear activos y cuentas de un país, entidad o persona especificado por la OFAC cuando dichas propiedades estén ubicadas en los Estados Unidos, estén en manos de personas físicas o entidades estadounidenses, o comiencen a estar en posesión o bajo el control de personas físicas o entidades estadounidenses. Por ejemplo, si una transferencia de fondos proviene de un sitio extraterritorial y está siendo encausada a través de un banco de EE. UU. a un banco en el exterior, y la OFAC ha designado a alguien a dicha la transacción, la transacción se debe ser bloqueada. La definición de activos y propiedad es amplia y se define específicamente en cada programa de sanción. Activos y propiedad incluye cualquier cosa de valor directo,

---

[133] Consulte 73 FR 57593 (9 de Noviembre de 2009) para obtener información adicional (también disponible en www.treas.gov/ofac).

[134] Todas las personas de EE. UU. deben cumplir con los reglamentos de la OFAC, incluidos todos los ciudadanos estadounidenses y extranjeros que sean residentes permanentes, sin importar dónde estén ubicadas, todas las personas y entidades que estén dentro de los Estados Unidos, todas las entidades constituidas en los EE.UU. y sus sucursales extranjeras. En el caso de ciertos programas, como los que están dirigidos a Cuba y Corea del Norte, las subsidiarias extranjeras de propiedad de empresas estadounidenses o que están controladas por éstas también deben cumplir con dichos reglamentos. Ciertos programas también exigen el cumplimiento por parte de personas extranjeras que posean bienes de origen estadounidense.

[135] Se brinda información adicional en *Foreign Assets Control Regulations for the Financial Community* (Reglamentos de Control de Activos Extranjeros para la Comunidad Financiera), disponible en el sitio web de la OFAC, www.treas.gov/offices/enforcement/ofac.

[136] 31 CFR capítulo V.

indirecto, presente, futuro o contingente (incluidos todos los tipos de transacciones bancarias). Los bancos deben bloquear las transacciones que:

- Han sido efectuadas por una persona o entidad bloqueada o en su nombre;
- Se realizan para una entidad bloqueada o a través de la misma; o
- Están vinculadas a una transacción en la cual tiene intereses una persona o entidad bloqueada.

Por ejemplo, si un banco estadounidense recibe instrucciones de hacer un pago por transferencia de fondos que encuadre en una de estas categorías, debe ejecutar la orden de pago y colocar los fondos en una cuenta bloqueada.[137] No es posible cancelar o enmendar las órdenes de pago una vez que un banco estadounidense las recibe sin una autorización de la OFAC.

Transacciones prohibidas

En algunos casos, se puede prohibir una transacción subyacente sin que haya ningún interés bloqueable en la transacción (es decir, la transacción no se debe aceptar, pero la OFAC no requiere bloquear los activos). En estos casos, la transacción simplemente se rechaza, (es decir, no se procesa). Por ejemplo, los Reglamentos de Sanciones a Sudán prohíben las transacciones que apoyen actividades comerciales realizadas en Sudán. Por lo tanto, los bancos estadounidenses tendrían que rechazar las transferencias de fondos entre dos compañías que no sean Ciudadanos especialmente designados o personas bloqueadas (SDN, por sus siglas en inglés) que efectúan una exportación a una compañía en Sudán que tampoco es una SDN. Debido a que las Sanciones a Sudán sólo exigen bloquear transacciones con el Gobierno de Sudán o las SDN, no habría intereses bloqueables en los fondos entre las dos compañías. Sin embargo, debido a que las transacciones constituirían un apoyo a la actividad comercial de Sudán, lo cual está prohibido, los bancos estadounidenses no están autorizados a procesar la transacción y deberán simplemente rechazarla.

Es importante tener en cuenta que el régimen de la OFAC que establece prohibiciones respecto a ciertos países, entidades y personas es diferente y está separado de las disposiciones que contiene el Programa de identificación de clientes (CIP) de la BSA (31 CFR 103.121), que exige a los bancos comparar las cuentas nuevas con las listas del gobierno en las que se consignan los nombres de quienes se sospecha o se sabe que son terroristas u organizaciones terroristas, dentro de un plazo razonable luego de la apertura de la cuenta. Las listas de la OFAC no han sido designadas como listas del gobierno para los propósitos de la norma del CIP. Consulte la sección del esquema general principal, "Programa de identificación de clientes", en las páginas 57 a 64, como guía adicional. Sin embargo, las exigencias de la OFAC se derivan de otras leyes que no están limitadas al

[137] Una cuenta bloqueada es una cuenta segregada que gana intereses (a una tasa comercial razonable), la cual retiene la propiedad del cliente hasta que el objetivo es retirado de la lista, el programa de sanciones es revocado, o el cliente obtiene una licencia de la OFAC que autoriza la liberación de la propiedad.

terrorismo, y las sanciones de la OFAC son aplicables a las transacciones, además de aplicarse a las relaciones de cuenta.

Licencias de la OFAC

Por medio de un proceso de expedición de licencias, la OFAC tiene autoridad para permitir ciertas transacciones que están prohibidas por sus reglamentos. La OFAC puede emitir una licencia para practicar una transacción que de otro modo estaría prohibida, cuando concluye que la transacción no debilita los objetivos de las políticas estadounidenses del programa de sanciones del que se trata, o que está justificada de algún otro modo por cuestiones relativas a objetivos de seguridad nacional o política exterior de los Estados Unidos. La OFAC también puede otorgar licencias generales que autoricen ciertas categorías de transacciones, como permitir cargos razonables por servicios a las cuentas bloqueadas, sin necesidad de una autorización en cada caso por parte de la OFAC. Estas licencias pueden encontrarse en los reglamentos de cada programa de sanciones (31 CFR, Capítulo V [Reglamentos]) y se puede acceder a ellas en el sitio web de la OFAC. Antes de procesar transacciones que pueden estar sujetas a una licencia general, los bancos deben verificar que dichas transacciones cumplan con los criterios relevantes de la licencia general.[138]

Las licencias específicas se emiten para cada caso.[139] Una licencia específica es un documento emitido por escrito por la OFAC en el que se autoriza una transacción o conjunto de transacciones específicas. Para recibir una licencia específica, la persona o entidad que desea realizar la transacción debe enviar una solicitud a la OFAC. Si la transacción se ajusta a la política exterior de EE. UU. bajo algún programa en particular, se otorgará la licencia. Si el cliente de un banco afirma poseer una licencia específica, el banco debe verificar que la transacción cumple con los términos de la licencia y debe obtener y conservar una copia de la licencia que la autoriza.

Presentación de informes a la OFAC

Los bancos deben informar todos los bloqueos a la OFAC dentro de los 10 días de ocurrido el hecho, y cada año, al 30 de Septiembre, respecto a esos activos bloqueados (desde el 30 de Junio).[140] Una vez bloqueados los activos o los fondos, deben colocarse en una cuenta bloqueada. Las transacciones prohibidas que sean rechazadas también deben ser informadas a la OFAC dentro de los 10 días de ocurrido el hecho.

Los bancos deben conservar registros completos y precisos de cada transacción rechazada durante un mínimo de cinco años después de la fecha de la transacción. Se deben llevar

---

[138] La información sobre las licencias está disponible en el sitio web de la OFAC www.treas.gov/offices/enforcement/ofac, o por teléfono si llama al 202-622-2480, área de Licencias de la OFAC.

[139] Las licencias específicas exigen una solicitud dirigida a: Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, D.C. 20220.

[140] El informe anual se debe presentar en el formulario TD F 90-22.50.

registros de las propiedades bloqueadas (incluyendo transacciones bloqueadas) durante el período en que permanezcan bloqueadas y durante los cinco años siguientes a la fecha en que cese el bloqueo.

En el sitio web de la OFAC se puede encontrar información adicional sobre los reglamentos de la OFAC, tales como el Programa de Sanciones y folletos que contienen Resúmenes de Países; la lista SDN, tanto de personas como de entidades; acciones recientes de la OFAC; y "Frequently Asked Questions" (Preguntas frecuentes).[141]

Programa de cumplimiento con la OFAC

Aunque no lo exige ningún reglamento específico, por cuestiones de práctica bancaria responsable y para garantizar el cumplimiento, los bancos deben establecer y mantener un programa eficaz de cumplimiento con la OFAC, por escrito que sea adecuado a su perfil de riesgo de la OFAC (dependiendo de los productos, servicios, clientes y ubicaciones geográficas). El programa debe identificar las áreas de mayor riesgo, proporcionar controles internos adecuados para la revisión y presentación de informes, establecer pruebas independientes para evaluar el cumplimiento, designar a un empleado del banco o a varios empleados responsables de que se cumpla con la OFAC, y diseñar programas de capacitación dirigidos al personal adecuado de todas las áreas relevantes del banco. El programa de cumplimiento con la OFAC perteneciente a un banco debe ser adecuado a su respectivo perfil de riesgo de la OFAC.

Análisis de riesgos de la OFAC

Un elemento fundamental de un buen programa de cumplimiento con la OFAC es el análisis del banco de sus líneas de productos, base de clientes, carácter de las transacciones e identificación de áreas de mayor riesgo para las transacciones de la OFAC. La identificación inicial de clientes de mayor riesgo para los fines de la OFAC puede hacerse como parte de los procedimientos del Programa de identificación de clientes (CIP) y debida diligencia de los clientes (CDD) del banco. Puesto que las sanciones de la OFAC pueden alcanzar prácticamente todas las áreas de sus operaciones, los bancos deben considerar todo tipo de transacciones, productos y servicios cuando realicen su análisis de riesgos y establezcan políticas, procedimientos y procesos adecuados. Un análisis de riesgos eficaz debe estar compuesto por múltiples factores (como se describe con más detalle a continuación) y, según las circunstancias, ciertos factores pueden influir más que otros.

Otros elementos a tomar en cuenta en el análisis de riesgos son las partes que intervienen en las cuentas y las transacciones. Las cuentas nuevas deben ser comparadas con las listas de la OFAC antes de su apertura o al poco tiempo de ésta. Sin embargo, la medida en la que un banco incluya a las partes de las cuentas que no sean titulares de las mismas (p. ej., beneficiarios, garantes, mandantes, usufructuarios, accionistas fiduciarios,

[141] La información está disponible en el sitio web de la OFAC, www.treas.gov/offices/enforcement/ofac, o por teléfono si llama a la línea directa de la OFAC al 800-540-6322.

directores, firmantes y apoderados) en el control inicial de la OFAC durante el proceso de apertura y durante los controles posteriores de bases de datos de cuentas existentes dependerá del perfil de riesgo del banco y de la tecnología disponible.

En función del perfil de riesgo del banco según la OFAC en cada área y de la tecnología disponible, éste deberá desarrollar políticas, procedimientos y procesos para controlar las transacciones y las partes que intervienen en ellas (p. ej., banco emisor, beneficiario, endosatario o jurisdicción). Actualmente, la OFAC ofrece orientación sobre las partes que participan en las transacciones de cheques. La guía estipula que si un banco sabe o tiene razones para creer que una de las partes de una transacción con cheques es un objetivo de la OFAC, el hecho de que el banco procese la transacción le acarreará responsabilidad, especialmente respecto a transacciones manejadas personalmente en áreas de mayor riesgo. Por ejemplo, si un banco sabe o tiene razones para creer que en una transacción con cheques participa una parte o un país prohibido por la OFAC, la OFAC esperaría una identificación oportuna y una acción apropiada.

Cuando se evalúa el nivel de riesgo, los bancos deben hacer uso de su buen juicio y tener en cuenta todos los indicadores de riesgo. Aunque la lista no es exhaustiva, algunos de los productos, servicios, clientes y ubicaciones geográficas que pueden implicar un mayor nivel de riesgo para la OFAC son los siguientes:

- Transferencias internacionales de fondos.
- Cuentas de extranjeros no residentes.
- Cuentas de clientes extranjeros.
- Transacciones de compensación automatizada (ACH) transnacionales.
- Cartas de crédito comerciales y otros productos de financiación del comercio.
- Transacciones vía banca electrónica.
- Cuentas de bancos corresponsales extranjeros.
- Cuentas empleadas para pagos.
- Banca privada internacional.
- Subsidiarias o sucursales en el exterior.

El Apéndice M (“Nivel de riesgos – Procedimientos de la OFAC”) proporciona una guía a los inspectores para evaluar los riesgos de la OFAC que enfrentan los bancos. El análisis de riesgos puede utilizarse para ayudar al inspector a establecer el campo de aplicación del control de la OFAC. La información adicional sobre el riesgo de

cumplimiento está publicada por la OFAC en su sitio web bajo el título "Frequently Asked Questions" (Preguntas frecuentes).[142]

Una vez que el banco ha identificado estas áreas de mayor riesgo de la OFAC, debe desarrollar políticas, procedimientos y procesos adecuados para tratar los riesgos asociados. Los bancos pueden adaptar estas políticas, procedimientos y procesos al carácter específico de cada rubro de actividad comercial o producto. Además, se exhorta a los bancos a reexaminar periódicamente sus riesgos de la OFAC.

Controles internos

Un programa de cumplimiento con la OFAC eficaz debe incluir controles internos para identificar cuentas y transacciones sospechosas e informar a la OFAC. Los controles internos deben incluir los siguientes elementos:

Identificación y control de transacciones sospechosas. Las políticas, los procedimientos y los procesos del banco deben centrarse en la manera en que éste habrá de identificar y controlar las transacciones y cuentas para detectar posibles violaciones a la OFAC, ya sea manualmente, a través de un software de interdicción, o mediante una combinación de ambos. A los efectos de la revisión, los bancos deben definir claramente los criterios que emplearán al comparar los nombres de las listas suministradas por la OFAC con los consignados en los archivos del banco o en las transacciones, así como al identificar las transacciones o cuentas que involucren a países sancionados. Las políticas, los procedimientos y los procesos de los bancos también deben considerar cómo se procederá a determinar si un acierto inicial con respecto a las listas de la OFAC es una coincidencia válida o un falso positivo.[143] Un alto volumen de falsos positivos puede indicar la necesidad de revisar el programa de interdicción del banco.

Los criterios de revisión empleados por los bancos para identificar variaciones en los nombres y errores de ortografía deben basarse en el nivel de riesgo de la OFAC asociado al producto o tipo de transacción particular. Por ejemplo, en un área de mayor riesgo con alto volumen de transacciones, el software de interdicción del banco debe ser capaz de identificar las derivaciones cercanas de los nombres para su control. La lista SDN intenta proporcionar derivaciones de nombres; sin embargo, es posible que no incluya todas las derivaciones posibles. Un software de interdicción más sofisticado puede llegar a captar las variaciones de un nombre de SDN que no estén incluidas en la lista SDN. Los bancos o áreas de menor riesgo y aquellos con un volumen bajo de transacciones, pueden optar por el uso de filtros manuales para cumplir con la OFAC. La decisión de usar software de interdicción y el nivel de sensibilidad del mismo deben basarse en la evaluación del banco de su propio riesgo y del volumen de sus transacciones. Para determinar la frecuencia de las verificaciones de la OFAC y los criterios usados para aplicar el filtro

[142] Este documento está disponible en www.treas.gov/offices/enforcement/ofac/faq/index.shtml.

[143] Las medidas de debida diligencia para establecer una coincidencia válida se proporcionan en *Using OFAC's Hotline* (Cómo usar la línea directa de la OFAC), que se encuentra en el sitio web de la OFAC: www.treas.gov/offices/enforcement/ofac.

(p. ej., derivaciones de nombres), los bancos deben tener en cuenta la probabilidad de que se cometa una violación y en la tecnología disponible. Además, los bancos deben reexaminar periódicamente su sistema de filtrado OFAC. Por ejemplo, si un banco identifica una derivación de un nombre que es un objetivo de la OFAC, ésta sugiere que el banco agregue el nombre a su proceso de filtrado.

Las cuentas nuevas deben ser comparadas con las listas de la OFAC antes de su apertura o al poco tiempo de ésta (p. ej., durante el procesamiento diario). Los bancos que realizan las verificaciones de la OFAC después de la apertura de cuenta deben contar con procedimientos dirigidos a evitar transacciones, luego del depósito inicial, hasta que se haya completado la verificación de la OFAC. La realización de transacciones prohibidas antes de que se haga la verificación de la OFAC puede acarrear sanciones. Además, los bancos deben contar con políticas, procedimientos y procesos para controlar a los clientes existentes cuando se realicen adiciones o cambios en la lista de la OFAC. La frecuencia del control debe basarse en el riesgo de la OFAC que enfrenta el banco. Por ejemplo, los bancos con un menor nivel de riesgo de la OFAC deben comparar periódicamente (es decir, mensual o trimestralmente) sus clientes con la lista de OFAC. Las transacciones, tales como transferencias de fondos, cartas de crédito y transacciones de personas físicas que no son clientes, deben compararse con la lista de la OFAC antes de ser ejecutadas. Al desarrollar políticas, procedimientos y procesos de la OFAC, los bancos deben tener en cuenta que la OFAC considera que la operación continua de una cuenta o el procesamiento de transacciones después de una designación, así como la aptitud de sus programas de cumplimiento con la OFAC, son factores determinantes al momento de imponer sanciones.[144] Los bancos deben documentar sus verificaciones OFAC de cuentas nuevas, el tipo de clientela existente, y de transacciones específicas.

Si un banco utiliza a un tercero, como un agente o un prestador de servicios, para realizar verificaciones OFAC en su nombre, al igual que con otras responsabilidades realizadas por un tercero, el banco es el responsable final del cumplimiento con las exigencias de la OFAC por parte del tercero. Como resultado, los bancos deben establecer controles adecuados y controlar los procedimientos de esas relaciones.

Actualización de las listas de la OFAC. El programa de cumplimiento con la OFAC que corresponde a un banco debe incluir políticas, procedimientos y procesos para la actualización oportuna de las listas de países, entidades y personas físicas bloqueadas, y la divulgación de esta información a todas las operaciones nacionales del banco y sus oficinas extraterritoriales, sucursales y, en el caso de Cuba y Corea del Norte, subsidiarias extranjeras. Este programa debería también asegurar que cualquier actualización manual del software de interdicción sea realizada oportunamente.

Revisión de transacciones de compensación automatizada (ACH) Todas las partes involucradas en una transacción ACH están sujetas a las exigencias de la OFAC.

---

[144] Consulte 74 FR 57593 (9 de Noviembre de 2009), *Economic Sanctions Enforcement Guidelines* (Pautas de aplicación de sanciones económicas). www.treas.gov/offices/enforcement/ofac/legal/regs/fr74_57593.pdf. Información adicional disponible en el sitio web de la OFAC: www.treasury.gov/offices/enforcement/ofac.

Consulte la sección del esquema general ampliado, "Transacciones de compensación automatizada", en las páginas 248 a 256, como guía. La OFAC ha aclarado la aplicación de sus normas a las transacciones ACH nacionales y transnacionales, y proporcionó una guía más detallada sobre transacciones ACH internacionales.[145]

Con respecto a las transacciones ACH nacionales, la Institución Financiera de Depósitos Remitente (ODFI, por sus siglas en inglés) es responsable de verificar que el Remitente no sea una parte bloqueada y de esforzarse de buena fe por determinar que el Remitente no esté transmitiendo fondos bloqueados. La Institución Financiera de Depósitos Recibidos (RDFI, por sus siglas en inglés) es igualmente responsable de verificar que el Receptor no sea una parte bloqueada. De este modo, la ODFI y la RDFI dependen mutuamente la una de la otra para cumplir con los reglamentos de la OFAC.

Si una ODFI recibe transacciones ACH nacionales que su cliente ya ha procesado por lotes, la ODFI no es responsable de anular este procesamiento por lotes para asegurarse de que ninguna transacción viole los reglamentos de la OFAC. Si una ODFI anula el procesamiento por lotes de un archivo recibido del Remitente para procesar transacciones *on-us*, tal ODFI es responsable de que las transacciones *on-us* cumplan con la OFAC, debido a que en este caso estará actuando como la ODFI y la RDFI en dichas transacciones. Las ODFI, actuando en esta calidad, deben conocer a sus clientes con anterioridad a los efectos de la OFAC y otras exigencias normativas. En relación con las transacciones residuales del archivo no procesadas por lotes que sean *on-us*, y a otras situaciones en las que los bancos manejen registros de ACH no procesados por lotes por motivos que no sean para desglosar las transacciones *on-us*, los bancos deben determinar el nivel de riesgo OFAC y desarrollar políticas, procedimientos y procesos adecuados para tratar los riesgos asociados. Dichas políticas atenuantes pueden implicar la revisión de cada registro de ACH no procesado por lotes. Del mismo modo, los bancos que entablan relaciones con prestadores de servicios externos deben analizar el carácter de dichas relaciones y sus transacciones ACH relacionadas para confirmar el nivel de riesgo OFAC del banco y para desarrollar políticas, procedimientos y procesos apropiados para mitigar ese riesgo.

Con respecto a la evaluación trasnacional de la OFAC, existen obligaciones similares aunque más estrictas de la OFAC para las transacciones ACH internacionales (IAT). En el caso de las IAT entrantes, e independientemente de si se establece la bandera de la OFAC en la IAT, una RDFI es responsable del cumplimiento con las exigencias de la OFAC Sin embargo, en el caso de las transacciones IAT salientes, la ODFI no puede depender de la evaluación de la OFAC por parte de una RDFI fuera de los Estados Unidos. En tales situaciones, la ODFI debe ejercer diligencia intensificada para garantizar que no se procesen transacciones ilegales.

La debida diligencia para una IAT entrante o saliente puede incluir la evaluación de las partes para una transacción, así como la revisión de los detalles de la información del campo de pago de una indicación de violación a una sanción, la investigación de los

[145] Consulte la Nota Interpretativa 041214-FACRL-GN-02 en www.treas.gov/offices/enforcement/ofac/rulings/. Las normas NACHA especifican aún más este cumplimiento (consulte la página 8 de la sección Búsqueda Rápida de las *Normas Operativas NACHA 2006*).

positivos resultantes, en caso que existan, y, finalmente, el bloqueo o rechazo de la transacción, según corresponda. Consulte la sección del esquema general ampliado, "Transacciones de compensación automatizada", en las páginas 248 a 256, como guía.

Más información sobre los tipos de sistemas de pago al por menor (sistemas de pago ACH) está disponible en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[146]

En una guía emitida el 10 de Marzo de 2009, la OFAC autorizó a instituciones en los Estados Unidos, cuando actúen como una ODFI/operador de puerta de enlace (GO) para débitos de IAT entrantes, a rechazar transacciones que parezcan involucrar intereses de propiedad o propiedad bloqueable.[147] La guía establece además que en la medida que una ODFI/GO evalúe los débitos de IAT entrantes para determinar si existen posibles violaciones a la OFAC antes de la ejecución y en el transcurso de dicha evaluación descubre una potencial violación a la OFAC, la transacción sospechosa se deberá eliminar del lote para realizar una investigación más profunda. Si la ODFI/GO determina que la transacción parece violar los reglamentos de la OFAC, la ODFI/GO debe negarse a procesar la transferencia. El procedimiento se aplica a las transacciones que normalmente serían bloqueadas así como para las transacciones que normalmente serían rechazadas por propósitos de la OFAC en función de la información del pago.

Presentación de informes. El programa de cumplimiento con la OFAC debe incluir también políticas, procedimientos y procesos para gestionar los elementos que han sido válidamente bloqueados o rechazados de acuerdo con los diferentes programas de sanciones. En el caso de las interdicciones relacionadas con el narcotráfico o el terrorismo, los bancos deben notificar a la OFAC lo más pronto posible, por teléfono o línea directa electrónica, sobre posibles aciertos, y enviar el seguimiento que se realice por escrito dentro de los diez días siguientes. La mayoría de los demás elementos se deben informar a través de los conductos normales, dentro de los diez días de haber ocurrido. Las políticas, los procedimientos y los procesos también deben tratar la gestión de cuentas bloqueadas. Los bancos tienen la responsabilidad de rastrear el monto de los fondos bloqueados, la propiedad de esos fondos y los intereses pagados sobre los mismos. El monto total bloqueado, incluyendo intereses, debe informarse a la OFAC al 30 de Septiembre de cada año (cubre información desde el 30 de Junio). Cuando un banco adquiere otro banco o se fusiona con él, ambos deben tener en cuenta la necesidad de controlar y mantener dichos registros e información.

Actualmente, los bancos no tienen la obligación de presentar Informes de actividades sospechosas (SAR) basados únicamente en transacciones bloqueadas relacionadas con el narcotráfico o el terrorismo, siempre que presenten a la OFAC el respectivo informe de bloqueo. Sin embargo, debido a que los informes de bloqueo requieren sólo información limitada, si el banco posee información adicional que no esté incluida en el informe de

---

[146] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

[147] Consulte www.frbservices.org/files/eventseducation/pdf/iat/031809_ofac_update.pdf.

bloqueo presentado a la OFAC, debe presentar un informe SAR por separado ante la FinCEN que incluya esa información. El banco también debe presentar un SAR si la transacción en sí misma se consideraría sospechosa sin necesidad de que existiera una coincidencia válida respecto a la OFAC.[148]

Conservación de información sobre las licencias. La OFAC recomienda que los bancos contemplen la posibilidad de conservar copias de las licencias OFAC de los clientes en sus archivos. Esto permitirá a los bancos verificar si la transacción que inicia un cliente es legal. Los bancos deben también conocer la fecha de expiración de las licencias. Si no es claro si una transacción específica está autorizada por una licencia, el banco debe confirmar esto con la OFAC. Conservar copias de las licencias también es útil si otro banco en la cadena de pagos solicita la verificación de la validez de la licencia. Se deben conservar copias de las licencias durante los cinco años siguientes a la última transacción realizada de conformidad con la licencia.

Pruebas independientes

Todos los bancos deben realizar una prueba independiente de su programa de cumplimiento con la OFAC, que sea llevada a cabo por el departamento de auditoría interna, auditores externos, asesores u otros terceros calificados. Para los bancos grandes, la frecuencia y el área de la prueba independiente se deben basar en el riesgo conocido o percibido de las áreas comerciales específicas. Para los bancos más pequeños, la auditoría debe ser coherente con el perfil de riesgo del banco según la OFAC, o basarse en el riesgo percibido. La persona o personas responsables de la prueba deben realizar una evaluación objetiva e integral de las políticas, los procedimientos y los procesos de la OFAC. El campo de aplicación de la auditoría debe ser lo suficientemente integral como para evaluar los riesgos de cumplimiento con la OFAC y la aptitud del programa de cumplimiento con la OFAC.

Persona responsable

Se recomienda que cada banco designe una persona calificada (o varias) como responsable del cumplimiento diario del programa de cumplimiento con la OFAC, que incluye la presentación de informes sobre transacciones bloqueadas o rechazadas de la OFAC, y la supervisión de los fondos bloqueados. Esta persona debe tener un nivel adecuado de conocimiento de los reglamentos de la OFAC que sean consistentes con el perfil de riesgo del banco según la OFAC.

Capacitación

El banco debe proporcionar capacitación adecuada a todos los empleados apropiados. El campo de aplicación y la frecuencia de la capacitación deben ser consistentes con el perfil de riesgo del banco según la OFAC y adecuados a las responsabilidades del empleado.

---

[148] Consulte el Comunicado de FinCEN Número 2004-02 *Unitary Filing of Suspicious Activity and Blocking Reports* (Presentación unitaria de Informes de actividades sospechosas y bloqueo), 69 RF 76847 (23 de Diciembre de 2004).

Procedimientos de Inspección

Oficina de Control de Activos Extranjeros

Objetivo: *Evaluar el programa de cumplimiento en función del riesgo del banco según la Oficina de Control de Activos Extranjeros (OFAC) para analizar si es adecuado al riesgo del banco según la OFAC, teniendo en cuenta sus productos, servicios, clientes, entidades, transacciones y ubicaciones geográficas.*

1. Determine si la junta directiva y la alta gerencia del banco han desarrollado políticas, procedimientos y procesos en función de su análisis de riesgos para garantizar el cumplimiento con la normativa de la OFAC.

2. Revise el programa de cumplimiento de la OFAC que aplica el banco en el contexto del análisis de riesgos del banco según la OFAC. Tenga en cuenta lo siguiente:

   - El alcance que tendrá y el método que se utilizará para la realización de búsquedas de la OFAC de cada departamento o rubro de la actividad comercial relevante (p. ej., transacciones de compensación automatizada [ACH], ventas de instrumentos monetarios, cobro de cheques, fideicomisos, préstamos, depósitos e inversiones) ya que el proceso puede variar de un departamento o rubro de la actividad comercial a otro.

   - El alcance que tendrá y el método que se utilizará para la realización de búsquedas de la OFAC de personas que sean parte en las cuentas sin ser titulares de éstas; puede incluir beneficiarios, garantes, mandantes, usufructuarios, accionistas fiduciarios, administradores, firmantes y apoderados.

   - Cómo se asigna la responsabilidad para la OFAC.

   - La prontitud de la obtención y actualización de las listas de la OFAC o los criterios de filtrado.

   - La aptitud de los criterios de filtrado utilizados por el banco para identificar razonablemente las coincidencias con la OFAC (p. ej., el grado en que los criterios de búsqueda o filtrado incluyen errores ortográficos y derivaciones de los nombres).

   - El proceso utilizado para investigar las coincidencias potenciales, incluidos los procedimientos de derivación para coincidencias potenciales.

   - El proceso utilizado para bloquear y rechazar transacciones.

   - El proceso utilizado para informar a la gerencia sobre transacciones bloqueadas o rechazadas.

   - La aptitud y prontitud de los informes que se presentan ante la OFAC.

   - El proceso para gestionar las cuentas bloqueadas (dichas cuentas se informan a la OFAC y pagan una tasa de interés comercialmente razonable).

- Las exigencias respecto a la conservación de registros (p. ej., exigencia de conservar los registros relevantes para la OFAC durante cinco años; para las propiedades bloqueadas, se deben conservar los registros mientras permanezcan bloqueadas; una vez desbloqueadas, durante cinco años).

3. Determine la aptitud de las pruebas independientes (auditorías) y procedimientos de seguimiento.

4. Revise la aptitud del programa de capacitación OFAC que aplica el banco en función del análisis de riesgos del banco según la OFAC.

5. Determine si el banco ha tratado de manera adecuada las debilidades o deficiencias identificadas por la OFAC, los auditores o los reguladores.

Pruebas de transacciones

6. En función del análisis de riesgos, informes de inspecciones previas y un control de los resultados de la auditoría del banco, seleccione las siguientes muestras para probar la aptitud del programa de cumplimiento con la OFAC del banco, de la siguiente manera:

   - Tome una muestra de las nuevas cuentas (p. ej., de depósito, de préstamos, fiduciarias, de inversión, de tarjetas de crédito, de oficinas en el extranjero y caja fuerte) y evalúe el proceso de filtrado utilizado para realizar búsquedas en el banco de datos de la OFAC (p. ej., la fecha de la búsqueda) y la documentación conservada para constatar las búsquedas.

   - Tome una muestra de las transacciones adecuadas que pueden no estar relacionadas con una cuenta (p. ej., de transferencias de fondos, de ventas de instrumentos monetarios y de cobro de cheques) y evalúe los criterios de filtrado utilizados para realizar búsquedas en el banco de datos de la OFAC, la hora de la búsqueda, y la documentación conservada para constatar las búsquedas.

   - Si el banco utiliza un sistema automatizado para realizar las búsquedas, analice la fecha en que se realizan las actualizaciones en el sistema y cuándo se realizan los cambios más recientes según la OFAC en el sistema. También, evalúe si todos los bancos de datos del banco se ejecutan mediante el sistema automatizado y la frecuencia con la que se realizan las búsquedas. Si existe alguna duda sobre la eficacia del filtro de la OFAC, ejecute pruebas del sistema ingresando nombres de cuentas de prueba que sean los mismos o similares a aquellos agregados recientemente a la lista de la OFAC para determinar si el sistema identifica un resultado positivo potencial.

   - Si el banco no utiliza un sistema automatizado, evalúe el proceso utilizado para comparar la clientela existente con la lista de la OFAC y la frecuencia de dichas comparaciones.

   - Revise una muestra de las coincidencias potenciales según la OFAC y evalúe la resolución del banco en cuanto a los procesos de bloqueo y rechazo.

- Revise una muestra de informes a la OFAC y evalúe su integridad y prontitud.
- Si se exige que el banco mantenga cuentas bloqueadas, seleccione una muestra y evalúe que el banco mantenga los registros adecuados de las sumas bloqueadas y la información de propiedad de los fondos bloqueados, que el banco esté pagando una tasa de interés comercialmente razonable por todas las cuentas bloqueadas y que esté presentando los informes adecuados con la información exigida anualmente (antes del 30 de Septiembre) a la OFAC. Pruebe los controles de los que se dispone para verificar que la cuenta esté bloqueada.
- Prepare una muestra de falsos positivos (coincidencias potenciales) para comprobar cómo se manejan; la resolución sobre un falso positivo se debe tomar fuera del rubro de la actividad comercial.

7. Identifique cualquier coincidencia potencial que no se haya informado a la OFAC, dialogue con la gerencia del banco y recomiéndele que notifique de inmediato a la OFAC sobre las transacciones no informadas y notifique de inmediato al personal de supervisión de su agencia regulatoria.
8. Determine el origen de las deficiencias (p. ej., capacitación, auditoría, análisis de riesgos, controles internos, supervisión de la gerencia) y formule una conclusión sobre la aptitud del programa de cumplimiento con la OFAC del banco.
9. Dialogue con la gerencia del banco sobre los resultados de la inspección relacionados con la OFAC.
10. Incluya las conclusiones según la OFAC dentro del informe de inspección, según sea pertinente.

ESQUEMA GENERAL AMPLIADO Y PROCEDIMIENTOS DE INSPECCIÓN DE PROGRAMAS CONSOLIDADOS Y OTROS TIPOS DE ESTRUCTURAS DE PROGRAMAS DE CUMPLIMIENTO BSA/AML

Estructuras del Programa de Cumplimiento BSA/AML: Esquema General

Objetivo: *Evaluar la estructura y la gestión del programa de cumplimiento BSA/AML de la organización y, si corresponde, el enfoque consolidado o parcialmente consolidado de la organización respecto del cumplimiento BSA/AML.*

Todos los bancos deben tener un programa de cumplimiento BSA/AML que sea integral y que cumpla con los requisitos de la BSA aplicables a todas las operaciones de la organización.[149] Las organizaciones bancarias deciden a discreción la forma de estructurar y gestionar el programa de cumplimiento BSA/AML. Una organización bancaria puede estructurar y gestionar el programa de cumplimiento BSA/AML o algunas partes del programa dentro de una entidad legal, con cierto grado de consolidación en las entidades de una organización o como parte de un marco integral de gestión de riesgos empresariales.

Muchas organizaciones bancarias grandes y complejas agregan riesgos de todo tipo (por ejemplo, de cumplimiento, operacional, crediticio, de tasa de interés, etc.) en toda la institución para maximizar las eficiencias, e identificar, supervisar y controlar mejor todos los tipos de riesgos dentro de las filiales, las subsidiarias, los rubros de la actividad comercial o las jurisdicciones, o en todos ellos.[150] En estas organizaciones, la gestión del

[149] Ni las reglamentaciones de la FinCEN ni las de las agencias bancarias imponen una obligación a las sociedades de control de bancos, las sociedades de control de asociaciones de ahorro y préstamo y las compañías matrices de las asociaciones de ahorro industrial con respecto a un programa de cumplimiento BSA/AML específico. No obstante, como resultado de su función comercial principal (por ejemplo, compañía de seguro, o agente de valores o de bolsa), estas entidades pueden estar sujetas a dicha obligación según las reglamentaciones del Tesoro o las de otras agencias.

[150] Para obtener información detallada, consulte *Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles* (Programas de gestión del riesgo de cumplimiento y supervisión en las grandes organizaciones bancarias con perfiles de cumplimiento complejos), Carta de SR 08-8 de la Junta de la Reserva Federal (FRB), 16 de Octubre de 2008 (Guía de FRB). Generalmente, la Guía de FRB abarca todas las funciones de cumplimiento generales dentro de las instituciones grandes y complejas, y avala para todas las empresas los principios establecidos en la guía

riesgo BSA generalmente es responsabilidad de una función de cumplimiento corporativo que respalda y supervisa el programa de cumplimiento BSA/AML.

Otras organizaciones bancarias pueden adoptar una estructura menos centralizada pero que de todas formas consolide algunos o todos los aspectos del cumplimiento BSA/AML. Por ejemplo, el análisis de riesgos, los controles internos (como la supervisión de actividades sospechosas), las pruebas independientes o la capacitación pueden administrarse centralmente. Esta centralización permite maximizar las eficiencias y optimizar de manera eficaz el análisis de riesgos y la implementación de controles en los rubros de la actividad comercial, las entidades legales y las jurisdicciones donde se realizan operaciones. Por ejemplo, una función de análisis de riesgos BSA/AML centralizada puede habilitar a una organización bancaria para que determine su exposición al riesgo general con relación a un cliente que hace negocios con la organización en diversos rubros de la actividad comercial o jurisdicciones.[151] Independientemente de cómo esté organizado un programa de cumplimiento BSA/AML consolidado, debe reflejar la estructura comercial, el tamaño y la complejidad de la organización, y debe diseñarse para contemplar con eficacia los riesgos, las exposiciones y las exigencias legales pertinentes en toda la organización.

Además, un enfoque consolidado debe incluir el establecimiento de normas corporativas para el cumplimiento BSA/AML que reflejen las expectativas de la junta directiva de la organización, con una labor por parte de la alta gerencia para asegurar que el programa de cumplimiento BSA/AML implemente estas normas corporativas. Las políticas individuales sobre los rubros de la actividad comercial complementarían las normas corporativas y contemplarían riesgos específicos dentro del departamento o rubro de la actividad comercial.

Por lo general, un programa de cumplimiento BSA/AML consolidado incluye un punto central donde se agregan riesgos BSA/AML en toda la organización. Consulte “Análisis de riesgos de cumplimiento BSA/AML consolidado”, en la página 30. En un enfoque consolidado, el riesgo debe analizarse dentro de los rubros de la actividad comercial, las entidades legales y las jurisdicciones donde se realizan operaciones, y en todos ellos. Los programas de las organizaciones globales deben incorporar los requisitos y las leyes AML de las distintas jurisdicciones en las que operan. La auditoría interna debe analizar el nivel de acatamiento al programa de cumplimiento BSA/AML consolidado.

Los inspectores deben tener en cuenta que algunas organizaciones bancarias diversificadas y complejas pueden tener varias subsidiarias que cuenten con diferentes tipos de licencias o autorizaciones bancarias para funcionar o que pueden organizar

---

del Comité de Supervisión Bancaria de Basilea, *Compliance and the compliance function in banks* (Cumplimiento y la función del cumplimiento en los bancos), de Abril de 2005, en www.bis.org/publ/bcbs113.htm.

[151] Como guía, consulte la sección del esquema general ampliado, “Sucursales y oficinas en el extranjero de bancos estadounidenses”, en las páginas 189 a 193, y la Guía del Comité de Supervisión Bancaria de Basilea: *Consolidated Know Your Customer (KYC) Risk Management* (Gestión de riesgos Conozca a su cliente [KYC] consolidada) en www.bis.org/press/p041006.htm.

actividades comerciales y componentes del programa de cumplimiento BSA/AML para todas sus personas jurídicas. Por ejemplo, una organización bancaria altamente diversificada puede establecer o mantener las cuentas mediante varias entidades legales examinadas por varios reguladores. Esta medida se puede tomar para maximizar las eficiencias, mejorar los beneficios impositivos, cumplir con los reglamentos jurisdiccionales, etc. Esta metodología puede presentar un desafío para un inspector que revise el cumplimiento BSA/AML en una entidad legal dentro de una organización. Según sea pertinente, los inspectores deben coordinar los esfuerzos con las otras agencias regulatorias para abordar estos desafíos o asegurar que el campo de aplicación de la inspección cubra adecuadamente la entidad legal bajo inspección.

Estructura de la función de cumplimiento BSA/AML

Según se mencionó anteriormente, una organización bancaria decide a discreción la forma de estructurar y gestionar su programa de cumplimiento BSA/AML. Por ejemplo, una institución pequeña puede optar por combinar el cumplimiento BSA/AML con otras funciones y utilizar el mismo personal para desempeñar diversas funciones. En estas circunstancias, sigue siendo conveniente que la alta gerencia se dedique al cumplimiento BSA/AML y que se implementen suficientes recursos dedicados. Como en el caso de todas las estructuras, la función de auditoría debe permanecer independiente.

Una institución más grande y compleja puede establecer una función BSA/AML corporativa para coordinar algunas o todas las responsabilidades BSA/AML. Por ejemplo, cuando las responsabilidades de cumplimiento BSA/AML han sido delegadas y el personal de cumplimiento BSA/AML está ubicado en los rubros de la actividad comercial, deben establecerse claramente las expectativas a fin de asegurar la implementación eficaz del programa de cumplimiento BSA/AML. En especial, la asignación de la responsabilidad debe ser clara con respecto al contenido y el alcance de los informes de los sistemas para la información de gestión, la exhaustividad y la frecuencia de las actividades de supervisión, y el papel de las diferentes partes dentro de una organización bancaria (por ejemplo, riesgo, rubros de la actividad comercial, operaciones) en los procesos de toma de decisiones con respecto al cumplimiento BSA/AML. La comunicación clara de cuáles han sido las funciones delegadas y cuáles permanecen centralizadas permite asegurar una implementación coherente del programa de cumplimiento BSA/AML entre los rubros de la actividad comercial, las filiales y las jurisdicciones. Además, una línea de responsabilidad clara puede evitar los conflictos de interés y garantizar que se mantenga la objetividad.

Independientemente de la estructura de gestión o el tamaño de la institución, el personal de cumplimiento BSA/AML ubicado en los rubros de la actividad comercial puede tener una interacción estrecha con la gerencia y el personal de los diversos rubros de la actividad comercial. Con frecuencia, las funciones de cumplimiento BSA/AML son más eficaces cuando existen relaciones de trabajo sólidas entre el personal de cumplimiento y el del rubro de la actividad comercial.

En algunas estructuras de cumplimiento, el personal de cumplimiento debe rendirle cuentas a la gerencia del rubro de actividad comercial. Esto puede ocurrir en instituciones

más pequeñas donde el personal de cumplimiento BSA/AML depende de un directivo de la alta gerencia del banco, en las instituciones más grandes donde el personal de cumplimiento depende de un gerente del rubro de la actividad comercial o en una organización bancaria extranjera que realiza operaciones en los Estados Unidos donde el personal depende de un solo directivo o ejecutivo. Estas situaciones pueden plantear el riesgo de posibles conflictos de interés que pueden dificultar el cumplimiento BSA/AML eficaz. Para garantizar la solidez de los controles de cumplimiento, debe mantenerse un nivel adecuado de independencia del cumplimiento BSA/AML, por ejemplo:

- al proporcionar al personal de BSA/AML una línea de comunicación para la función de cumplimiento corporativo u otra función independiente;
- al asegurar que el personal de cumplimiento BSA/AML participe activamente en todas las cuestiones relacionadas con el riesgo AML (por ejemplo, productos nuevos, revisión o finalización de las relaciones con los clientes, determinaciones sobre la presentación de informes);
- al establecer un proceso de derivación y resolución objetiva de los conflictos entre el personal de cumplimiento BSA/AML y la gerencia del rubro de la actividad comercial; y
- al establecer controles internos para asegurar que se mantenga la objetividad del cumplimiento cuando se asignen responsabilidades bancarias adicionales al personal de cumplimiento BSA/AML.

Gestión y supervisión del programa de cumplimiento BSA/AML

La junta directiva y la alta gerencia de un banco tienen funciones y responsabilidades diferentes en la gestión y la supervisión del riesgo de cumplimiento BSA/AML. La junta directiva tiene la responsabilidad principal de asegurar que el banco cuente con un programa de cumplimiento BSA/AML integral y eficaz, y de supervisar que el marco de gestión se diseñe de manera razonable para garantizar el cumplimiento del reglamento BSA/AML. La alta gerencia es responsable de implementar el programa de cumplimiento BSA/AML aprobado por la junta directiva.

Junta directiva.[152] La junta directiva es responsable de aprobar el programa de cumplimiento BSA/AML, y de supervisar la estructura y la gestión de la función de cumplimiento BSA/AML del banco. La junta directiva tiene la responsabilidad de establecer una cultura de cumplimiento BSA/AML adecuada, desarrollar políticas claras con respecto a la gestión de los riesgos BSA/AML clave y asegurar que estas políticas se cumplan en la práctica.

[152] Con respecto a las operaciones en los Estados Unidos, las organizaciones bancarias extranjeras deben cerciorarse de cumplir adecuadamente las responsabilidades de la junta descritas en esta sección mediante su estructura de supervisión y el marco de gestión de riesgos BSA/AML.

La junta debe asegurar que la alta gerencia esté completamente capacitada, calificada y adecuadamente motivada para gestionar los riesgos de cumplimiento BSA/AML que surjan de las actividades comerciales de la organización de manera coherente con las expectativas de la junta. Debe garantizar que la función de cumplimiento BSA/AML tenga una condición de preeminencia adecuada dentro de la organización. La alta gerencia dentro de la función de cumplimiento BSA/AML y el personal de cumplimiento de nivel superior dentro de los rubros individuales de la actividad comercial deben tener la autoridad, la independencia y el acceso al personal y la información correctos dentro de la organización, y los recursos adecuados para llevar a cabo las actividades con eficacia. La junta debe asegurarse de que se entiendan sus puntos de vista acerca de la importancia del cumplimiento BSA/AML y que se comuniquen en todos los niveles de la organización bancaria. Además, debe corroborar que la alta gerencia establezca incentivos adecuados para integrar los objetivos de cumplimiento BSA/AML en las metas de gestión y la estructura de compensación de la organización, y que se tomen medidas correctivas, incluidas las sanciones disciplinarias, de corresponder, cuando se identifican faltas graves de cumplimiento BSA/AML.

Alta gerencia. La alta gerencia es responsable de comunicar y consolidar la cultura de cumplimiento BSA/AML establecida por la junta, y de implementar y hacer respetar el programa de cumplimiento BSA/AML aprobado por la junta. Si la organización bancaria tiene una función de cumplimiento BSA/AML independiente, la alta gerencia de la función debe establecer, respaldar y supervisar el programa de cumplimiento BSA/AML de la organización. El personal de cumplimiento BSA/AML debe informar a la junta, o a un comité pertinente, sobre la eficacia del programa de cumplimiento BSA/AML y los problemas de cumplimiento BSA/AML significativos.

La alta gerencia de una organización bancaria extranjera que realiza operaciones en los Estados Unidos debe proporcionar información suficiente relacionada con el cumplimiento BSA/AML en cuanto a las operaciones en los Estados Unidos a las funciones de control o de gobierno en su país de origen, y debe garantizar que la alta gerencia responsable en el país de origen tenga el nivel de comprensión adecuado del riesgo BSA/AML y el entorno de control que rige a las operaciones en los Estados Unidos. La gerencia estadounidense debe evaluar constantemente la eficacia de los mecanismos de control de BSA/AML establecidos para las operaciones en los Estados Unidos y derivar los temas de inquietud según sea necesario. Cuando corresponda, deberá desarrollarse e implementarse una medida correctiva.

Programas de cumplimiento BSA/AML consolidados

Las organizaciones bancarias que gestionan centralmente las operaciones y funciones de los bancos subsidiarios, otras subsidiarias y los rubros de la actividad comercial, deben garantizar que se disponga de políticas, procedimientos y procesos de gestión de riesgos exhaustivos para ocuparse del espectro de riesgos de toda la organización. Un programa adecuado de cumplimiento BSA/AML consolidado proporciona el marco para todas las subsidiarias, los rubros de la actividad comercial y las sucursales en el extranjero a fin de que cumplan con sus exigencias normativas específicas (por ejemplo, exigencias del país o la industria). Consecuentemente, las organizaciones que gestionan centralmente un

programa de cumplimiento BSA/AML consolidado deben, entre otras cosas, proporcionar la estructura adecuada, y notificar a los rubros de la actividad comercial, las subsidiarias y las sucursales en el extranjero sobre el desarrollo de pautas adecuadas. Como guía, consulte la sección del esquema general ampliado, "Sucursales y oficinas en el extranjero de bancos estadounidenses", en las páginas 189 a 193.

Una organización que ejecuta un programa de cumplimiento BSA/AML consolidado puede optar por administrar solamente controles de cumplimiento específicos (por ejemplo, sistemas de supervisión de actividades sospechosas o auditorías) de manera consolidada, junto con otros controles de cumplimiento administrados exclusivamente en las filiales, las subsidiarias y los rubros de la actividad comercial. Cuando se implementa este enfoque, los inspectores deben identificar cuáles son las secciones del programa de cumplimiento BSA/AML que forman parte del programa de cumplimiento BSA/AML consolidado. Esta información es esencial cuando se establezca el campo de aplicación y la planificación de la inspección BSA/AML.

Al evaluar la aptitud del programa de cumplimiento BSA/AML consolidado, el inspector debe determinar las líneas de comunicación y cómo cada filial, subsidiaria, rubro de la actividad comercial o jurisdicción se adecua a la estructura general de cumplimiento. Esto debe incluir un análisis de cuán claramente se comunican los papeles y responsabilidades en el banco o la organización bancaria. El inspector debe analizar cuán eficazmente el banco o la organización bancaria supervisan el cumplimiento BSA/AML en toda la institución, incluido el grado de eficacia del programa de cumplimiento BSA/AML consolidado y no consolidado para captar los datos relevantes de las subsidiarias.

En la evaluación del programa de cumplimiento BSA/AML consolidado se debe tener en cuenta la información disponible acerca de la aptitud del programa de cumplimiento BSA/AML de las subsidiarias individuales. Independientemente de la decisión de implementar un programa de cumplimiento BSA/AML consolidado por completo, o en parte, dicho programa debe garantizar que todas las filiales, incluidas aquellas que realicen operaciones en jurisdicciones extranjeras, cumplan con sus exigencias normativas aplicables. Por ejemplo, un programa de auditoría implementado únicamente de manera consolidada que no lleva a cabo las pruebas de transacciones pertinentes en todas las subsidiarias sujetas a la BSA, no será suficiente para cumplir con las exigencias normativas de las pruebas independientes para esas subsidiarias.

Presentación de informes de actividades sospechosas

Las sociedades de control de bancos (BHC) o cualquier subsidiaria no bancaria de estas, o un banco extranjero que esté sujeto a la Ley de BHC o cualquier subsidiaria no bancaria de dicho banco extranjero que opere en los Estados Unidos, tienen la obligación de presentar informes de actividades sospechosas (12 CFR 225.4(f)). Las subsidiarias no bancarias de una BHC que operan sólo fuera de los Estados Unidos no tienen la obligación de presentar informes de actividades sospechosas. Ciertas sociedades de control de asociaciones de ahorro y préstamo, y sus subsidiarias que no se dediquen al depósito, tienen la obligación de presentar los informes de actividades sospechosas de

conformidad con los reglamentos del Tesoro (por ejemplo, compañías de seguro (31 CFR 103.16) y agentes bursatiles (31 CFR 103.19)). Además, a las sociedades de control de asociaciones de ahorro y préstamo, en los casos en que no se les exija, se las exhorta a que presenten informes de actividades sospechosas en las circunstancias adecuadas. El 20 de Enero de 2006, la Red de Lucha contra Delitos Financieros, la Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro expidieron una guía autorizando a las organizaciones bancarias a compartir los informes de actividades sospechosas con oficinas centrales y compañías controlantes, ya sea ubicadas en los Estados Unidos o en el extranjero. Si desea más información, consulte la sección del esquema general, “Informes de actividades sospechosas”, en las páginas 73 a 89.

Procedimientos de Inspección

Estructuras del programa de cumplimiento BSA/AML

Objetivo: *Evaluar la estructura y la gestión del programa de cumplimiento BSA/AML de la organización y, si corresponde, el enfoque consolidado o parcialmente consolidado de la organización bancaria respecto del cumplimiento BSA/AML. Un programa de cumplimiento BSA/AML puede estructurarse de diversas formas, y un inspector debe realizar los procedimientos en función de la estructura de la organización. La implementación de estos procedimientos puede requerir la comunicación con otros reguladores.*

1. Revise la estructura y la gestión del programa de cumplimiento BSA/AML. Comuníquese con sus compañeros en otras agencias bancarias federales y estatales, según sea necesario, para confirmar que comprenden el programa de cumplimiento BSA/AML de la organización. Este enfoque fomenta la supervisión coherente y disminuye las cargas legales de la organización bancaria. Determine el grado en el que la estructura del programa de cumplimiento BSA/AML afecta la organización que se está inspeccionando, teniendo en cuenta:

   - La existencia de operaciones o funciones consolidadas o parcialmente consolidadas responsables de las operaciones BSA/AML diarias, incluidas, entre otros, la centralización de la supervisión y presentación de informes de actividades sospechosas, la presentación de informes de transacciones en efectivo, el control y presentación de informes de exención monetaria o las actividades de gestión de registros.

   - La consolidación de unidades operativas, como las unidades de inteligencia financiera, que se dedican a la supervisión de transacciones en todas las actividades, los rubros de la actividad comercial o personas jurídicas y son responsables de ello. (Analice la variedad y el alcance de la información que las fuentes de datos o transacciones (por ejemplo, los bancos, agentes bursatiles, compañías fiduciarias, corporaciones que se rigen por la Ley de Organizaciones Bancarias Extranjeras (*Edge Act*) y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal, compañías de seguro o sucursales en el extranjero) ingresan en los sistemas de supervisión e informe).

   - El grado en que la organización bancaria (u otra unidad de nivel corporativo, como de auditoría o cumplimiento) lleva a cabo pruebas independientes habituales de las actividades BSA/AML.

   - Si una unidad de nivel corporativo auspicia la capacitación BSA/AML y en qué medida lo hace.

2. Revise las pruebas para verificar el cumplimiento BSA/AML en toda la organización bancaria, según corresponda, e identifique las deficiencias del programa.

3. Revise el acta de la junta para determinar la aptitud de los sistemas para la información de gestión y de los informes proporcionados a la junta directiva. Asegúrese de que la junta directiva haya recibido la notificación adecuada de los informes de actividades sospechosas.

4. Revise las políticas, los procedimientos, los procesos y los análisis de riesgos formulados e implementados por la junta directiva, un comité de la misma, o la alta gerencia de la organización. Como parte de este control, evalúe la eficacia de la capacidad de la organización para cumplir con las siguientes responsabilidades:

   - Gestionar el programa de cumplimiento BSA/AML y proporcionar la supervisión adecuada.
   - Establecer y comunicar las normas corporativas que reflejen las expectativas de la junta directiva de la organización y proporcionar una asignación clara de las responsabilidades de cumplimiento BSA/AML.
   - Identificar prontamente y medir, supervisar y controlar de manera eficaz los riesgos clave en toda la organización.
   - Desarrollar un análisis de riesgos adecuado, y las políticas, los procedimientos y los procesos para gestionar esos riesgos exhaustivamente.
   - Desarrollar procedimientos para la evaluación, aprobación y supervisión de límites de riesgo, nuevas iniciativas comerciales y cambios estratégicos.
   - Supervisar el cumplimiento de las subsidiarias con las exigencias normativas aplicables (por ejemplo, exigencias del país o la industria).
   - Supervisar el cumplimiento de las exigencias del programa de cumplimiento BSA/AML por parte de las subsidiarias.
   - Identificar las debilidades del programa de cumplimiento BSA/AML e implementar las medidas correctivas necesarias y oportunas, a nivel de la organización y las subsidiarias.

5. Para garantizar el cumplimiento de las exigencias normativas, revise los procedimientos de la organización para supervisar y presentar los informes de actividades sospechosas.[153] Como guía, consulte el esquema general principal

[153] Las sociedades de control de bancos (BHC) o cualquier subsidiaria no bancaria de estas, o un banco extranjero que esté sujeto a la Ley de BHC o cualquier subsidiaria no bancaria de dicho banco extranjero que opere en los Estados Unidos, tienen la obligación de presentar informes de actividades sospechosas (12 CFR 225.4(f)). Las subsidiarias no bancarias de una BHC que operan sólo fuera de los Estados Unidos no tienen la obligación de presentar informes de actividades sospechosas. Ciertas sociedades de control de asociaciones de ahorro y préstamo, y sus subsidiarias que no se dediquen al depósito, tienen la obligación de presentar los informes de actividades sospechosas de conformidad con los reglamentos del Tesoro (por ejemplo, compañías de seguro (31 CFR 103.16) y agentes bursatiles (31 CFR 103.19)). Además, a las sociedades de control de asociaciones de ahorro y préstamo, en los casos en que no se les exija, se las exhorta a que presenten informes de actividades sospechosas en las circunstancias adecuadas. El 20 de

y procedimientos de inspección, “Informes de actividades sospechosas”, en las páginas 73 a 89 y 90 a 95, respectivamente.

6. Una vez que el inspector haya finalizado los procedimientos anteriores, éste debe dialogar sobre los resultados con los siguientes, según sea pertinente:

   - El inspector a cargo.
   - La o las personas responsables de la supervisión continua de la organización y los bancos subsidiarios, según sea pertinente.
   - La gerencia corporativa.

7. En función de los procedimientos de inspección implementados, formule una conclusión sobre la aptitud de las estructuras y la gestión del programa de cumplimiento BSA/AML, incluida, si corresponde, la eficacia del enfoque consolidado o parcialmente consolidado respecto del cumplimiento.

Enero de 2006, la Red de Lucha contra Delitos Financieros, la Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro expidieron una guía autorizando a las organizaciones bancarias a compartir los informes de actividades sospechosas con oficinas centrales y compañías controlantes, ya sea ubicadas en los Estados Unidos o en el extranjero. Si desea más información, consulte la sección del esquema general principal, “Informes de actividades sospechosas”, en las páginas 73 a 89.

Sucursales y Oficinas en el Extranjero de Bancos Estadounidenses: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con sus oficinas y sucursales en el extranjero, y de la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Los bancos estadounidenses abren oficinas y sucursales en el extranjero[154] para cumplir con las demandas de los clientes, para ayudar a que el banco crezca o para ampliar el alcance de los productos y servicios ofrecidos. Las oficinas y sucursales en el extranjero varían significativamente en tamaño, complejidad de operaciones y campo de aplicación de los productos y servicios ofrecidos. Los inspectores deben tener en cuenta estos factores al controlar el programa de cumplimiento AML de las oficinas y sucursales en el extranjero. Las definiciones de "institución financiera" y "banco" de la BSA y sus reglamentos de ejecución no incluyen las oficinas o inversiones en el extranjero de bancos estadounidenses o corporaciones que se rigen por la Ley de Organizaciones Bancarias Extranjeras (*Edge Act*) y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal.[155] No obstante, se espera que los bancos dispongan de políticas, procedimientos y procesos en todas sus sucursales y oficinas para protegerse contra los riesgos de lavado de dinero y financiamiento del terrorismo.[156] Las políticas, los procedimientos y los procesos AML de la sucursal u oficina en el extranjero deben cumplir con las exigencias locales y ser consistentes con las normas de los bancos estadounidenses; sin embargo, es posible que deban adaptarse a las prácticas comerciales o locales.[157]

Factores de riesgo

Los inspectores deben comprender los tipos de productos y servicios que se ofrecen en las oficinas y sucursales en el extranjero, como también a los clientes y ubicaciones geográficas a los que se prestan servicios en las oficinas y sucursales en el extranjero. Las oficinas y sucursales en el extranjero pueden ofrecer cualquier servicio que ofrece el banco estadounidense si no lo prohíbe el país anfitrión. Dichos productos y servicios ofrecidos en las oficinas y sucursales en el extranjero pueden tener un perfil de riesgo diferente al del mismo producto o servicio ofrecido en el banco estadounidense (por ejemplo, los negocios de servicios monetarios se regulan en los Estados Unidos; sin

[154] Las oficinas en el extranjero incluyen las filiales y subsidiarias.

[155] Las corporaciones que se rigen por la Ley de organizaciones bancarias extranjeras (*Edge Act*) y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal pueden utilizarse para retener inversiones extranjeras (por ejemplo, inversiones en cartera extranjeras, sociedades conjuntas o subsidiarias).

[156] 71 FR 13935.

[157] Para obtener más información, consulte *Consolidated Know Your Customer (KYC) Risk Management* (Gestión de riesgos Conozca a su cliente [KYC] consolidada), Comité de Supervisión Bancaria de Basilea, 2004, en www.bis.org/forum/research.htm.

embargo, entidades similares en otro país pueden no estar reguladas). Por lo tanto, el inspector debe saber que los riesgos asociados a las oficinas y sucursales en el extranjero pueden diferir (por ejemplo, operaciones de venta al por mayor frente a operaciones de venta al por menor).

El inspector debe comprender las diversas exigencias AML de la jurisdicción extranjera. Las leyes de secreto o sus equivalentes pueden afectar la capacidad de una oficina o sucursal en el extranjero de compartir información con la casa matriz estadounidense, o la capacidad del inspector de inspeccionar la entidad. Aunque a las organizaciones bancarias con sucursales o subsidiarias en el exterior les resulte necesario adaptar los enfoques de supervisión como consecuencia de las leyes de privacidad locales, el mecanismo de supervisión del cumplimiento debe garantizar el análisis y la supervisión eficaz de los riesgos dentro de dichas sucursales y subsidiarias. A pesar de las exigencias de la BSA específicas no se aplican a las oficinas y sucursales en el extranjero, se espera que los bancos dispongan de políticas, procedimientos y procesos en todas sus sucursales y oficinas para protegerse contra los riesgos de lavado de dinero y financiamiento del terrorismo. En este sentido, las oficinas y sucursales en el extranjero deben guiarse por las políticas, los procedimientos y los procesos BSA/AML del banco estadounidense. Las oficinas y sucursales en el extranjero deben cumplir con las exigencias de la OFAC aplicables y todas las leyes, normas y reglamentos AML locales.

Mitigación del riesgo

Las oficinas y sucursales de los bancos estadounidenses que se encuentren en ubicaciones geográficas de riesgo más alto pueden ser vulnerables al abuso por parte de los responsables del lavado de dinero. Para abordar este peligro, las políticas, los procedimientos y los procesos del banco estadounidense para las operaciones en el extranjero deben ser consistentes con las siguientes recomendaciones:

- La oficina central y la gerencia del banco estadounidense en la operación extranjera deben comprender la eficacia y calidad de la supervisión bancaria en el país anfitrión y comprender las exigencias legales y normativas de éste. La oficina central del banco estadounidense debe conocer y comprender cualquier preocupación que los supervisores del país anfitrión puedan tener con respecto a la oficina o sucursal en el extranjero.

- La oficina central del banco estadounidense debe comprender el perfil de riesgo de las oficinas y sucursales en el extranjero (por ejemplo, productos, servicios, clientes y ubicaciones geográficas).

- La oficina central y la gerencia del banco estadounidense deben tener acceso a información suficiente para supervisar periódicamente la actividad de sus oficinas y sucursales en el extranjero, incluidos su nivel de cumplimiento con las políticas, los procedimientos y los procesos de la oficina central. Parte de esto se puede lograr mediante los informes de los sistemas para la información de gestión.

- La oficina central del banco estadounidense debe desarrollar un sistema para probar y verificar la integridad y eficacia de los controles internos en las oficinas o sucursales en el extranjero llevando a cabo auditorías dentro del país. La alta gerencia de la

oficina central debe obtener y controlar las copias, escritas en inglés, de los informes de auditoría y cualquier otro informe relacionado con las evaluaciones AML y de control interno.

- La oficina central del banco estadounidense debe establecer prácticas firmes de intercambio de información entre las oficinas y sucursales, particularmente con respecto a las relaciones asociadas a cuentas de riesgo más alto. El banco debe utilizar la información para evaluar y comprender las relaciones de cuenta en toda la estructura corporativa (por ejemplo, fuera de las fronteras o las estructuras legales).

- La oficina central del banco estadounidense debe ser capaz de proporcionar a los inspectores cualquier información considerada necesaria para analizar el cumplimiento con las leyes bancarias estadounidenses.

Las estructuras de cumplimiento y de auditoría de la oficina y sucursal en el extranjero pueden variar sustancialmente en función del campo de aplicación de las operaciones (por ejemplo, ubicaciones geográficas) y el tipo de productos, servicios y clientes. Las oficinas y sucursales en el extranjero con múltiples ubicaciones dentro de una región geográfica (por ejemplo, Europa, Asia y Sudamérica) están supervisadas frecuentemente por personal de auditoría y de cumplimiento regional. Independientemente del tamaño o el campo de aplicación de las operaciones, el personal de auditoría y de cumplimiento y los programas de auditoría deben ser suficientes para supervisar los riesgos AML.

Establecimiento del campo de aplicación de las inspecciones AML

Las inspecciones se pueden realizar en el país anfitrión o en los Estados Unidos. Los factores que se tendrán en cuenta al decidir si la labor de inspección debe llevarse a cabo en la jurisdicción anfitriona o en los Estados Unidos incluyen:

- El perfil de riesgo de la oficina o sucursal en el extranjero y si el perfil es estable o cambiante como resultado de una reorganización, la incorporación de nuevos productos o servicios, u otros factores, incluido el perfil de riesgo de jurisdicción misma.

- La eficacia y calidad de la supervisión bancaria en el país anfitrión.

- La existencia de un acuerdo de intercambio de información entre el país anfitrión y el supervisor estadounidense.

- Los antecedentes de inspección o las preocupaciones relacionadas con las auditorías de la oficina o sucursal en el extranjero.

- El tamaño y complejidad de las operaciones de la oficina o sucursal en el extranjero.

- La eficacia de los controles internos, incluidos los sistemas para gestionar los riesgos AML de manera concreta y auditorías internas.

- La capacidad de gestión de la oficina o sucursal en el extranjero para proteger la entidad del lavado de dinero o el financiamiento del terrorismo.

- La disponibilidad en los Estados Unidos de los registros de la oficina o sucursal en el extranjero.

En algunas jurisdicciones, el secreto financiero y otras leyes pueden evitar o limitar rigurosamente la evaluación directa de los registros o las actividades del cliente por parte de los inspectores estadounidenses o el personal de la oficina central estadounidense. En algunos casos en los que una inspección en la entidad no se puede llevar a cabo de manera eficaz, los inspectores deben consultar con el personal de la agencia correspondiente. En tales casos, el personal de la agencia puede comunicarse con los supervisores extranjeros para llegar a un acuerdo adecuado para la inspección o intercambio de información. En situaciones de riesgo más bajo cuando la información está restringida, los inspectores pueden realizar inspecciones en los Estados Unidos (consulte el tema a continuación). En las situaciones de riesgo más alto en las que las inspecciones adecuadas (en la entidad o de otra manera) no puedan efectuarse, la agencia puede exigir a la oficina central que tome medidas para abordar la situación, que pueden incluir el cierre de la oficina en el extranjero.

Inspecciones en los Estados Unidos

Las inspecciones en los Estados Unidos, o fuera de la entidad, generalmente exigen una mayor confianza en el programa AML de la oficina o sucursal en el extranjero, como también la capacidad de acceder a registros suficientes. Dichas inspecciones fuera de la entidad deben incluir el diálogo con la alta gerencia del banco de la oficina central y en el extranjero. Dichos diálogos son esenciales para comprender las operaciones, riesgos AML y programas AML de las oficinas o sucursales en el extranjero. Además, la inspección de la oficina o sucursal en el extranjero debe incluir un control de la participación del banco estadounidense en la gestión o supervisión de las operaciones, sistemas de controles internos (por ejemplo, políticas, procedimientos e informes de supervisión) de la sucursal en el extranjero, y, donde estén disponibles, los resultados de la inspección, de la auditoría y los documentos de los supervisores del país anfitrión. Como sucede con todas las inspecciones BSA/AML, el grado de las pruebas de transacciones y actividades con transacciones que se realicen está basado en varios factores que incluyen la estimación de los riesgos hecha por el inspector, los controles y la aptitud de las pruebas independientes.

Inspecciones en la jurisdicción anfitriona

La inspección en la jurisdicción anfitriona permite a los inspectores no sólo comprender mejor el papel del banco estadounidense en relación con su oficina o sucursal en el extranjero, sino también, y quizás más importante, determinar el grado en que se cumple a nivel local con las políticas, los procedimientos y los procesos globales del banco estadounidense.

El proceso de establecimiento del campo de aplicación y planificación estándar determinará el objetivo de la inspección y las necesidades con respecto a los recursos. Puede haber

algunas diferencias en el proceso de inspección que se lleva a cabo en el extranjero. La autoridad de supervisión anfitriona puede enviar un inspector para que se una al equipo estadounidense o solicitar su asistencia a las reuniones al inicio y finalización de la inspección. Las exigencias de presentación de informes AML probablemente también sean diferentes, ya que se ajustarán a las exigencias normativas locales.

Para las inspecciones en los Estados Unidos y en el país anfitrión de las oficinas y sucursales en el extranjero, los procedimientos utilizados respecto a productos, servicios, clientes y entidades específicos se encuentran en este manual. Por ejemplo, si un inspector observa actividades de depósitos vía maletines/bolsos en oficinas y sucursales en el extranjero, éste debe hacer uso de los procedimientos de inspección de la sección ampliada aplicables.

Procedimientos de Inspección

Sucursales y oficinas en el extranjero de bancos estadounidenses

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con sus oficinas y sucursales en el extranjero, y de la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, procedimientos y procesos relacionados con las sucursales y oficinas en el extranjero[158] para evaluar su aptitud dada la actividad en relación con el riesgo del banco y analizar si los controles son idóneos para proteger de manera razonable al banco del lavado de dinero y el financiamiento del terrorismo.

2. En función de un control de los sistemas de información de gestión y los factores de valoración de riesgos internos, determine si la oficina central del banco estadounidense identifica y supervisa de manera eficaz las sucursales y oficinas en el extranjero, particularmente aquellas que realizan transacciones de riesgo más alto o que están ubicadas en jurisdicciones de riesgo más alto.

3. Determine si el sistema de la oficina central del banco estadounidense de supervisión de sucursales y oficinas en el extranjero y detección de actividades sospechosas o poco habituales en esas sucursales y oficinas, es idóneo dado el tamaño, complejidad, ubicación y tipos de relaciones con los clientes. Determine si el país anfitrión exige la presentación de informes de actividades sospechosas y, si está permitido y puede disponer de los documentos, revise dichos informes. Determine si esta información es proporcionada a la oficina central del banco estadounidense y filtrada a todo el banco o, si corresponde, a un análisis aplicable a toda la institución en busca de actividades sospechosas.

4. Revise el informe de la estructura organizativa o la estratificación del banco, que debe incluir una lista de todas las personas jurídicas y los países en los que están registradas. Determine las ubicaciones de las sucursales y oficinas extranjeras, que incluyen el entorno normativo extranjero y el nivel de acceso que tienen los reguladores estadounidenses para inspecciones y registros de los clientes dentro del sitio.

5. Revise cualquier relación de asociación o tercerización de sucursales y oficinas extranjeras. Determine si la relación es coherente con el programa AML del banco.

6. Determine el tipo de productos, servicios, clientes, entidades y ubicaciones geográficas a los que las sucursales y oficinas en el extranjero les prestan servicios. Revise los análisis de riesgos de las sucursales y oficinas en el extranjero.

[158] Las oficinas en el extranjero incluyen las filiales y subsidiarias.

7. Revise la gerencia, el cumplimiento y la estructura de auditoría de las sucursales y oficinas en el extranjero. Identifique las decisiones que se toman en la oficina central del banco estadounidense frente a aquellas que se toman en la sucursal u oficina en el extranjero.

8. Determine la participación de la oficina central del banco estadounidense en la gestión y supervisión de las sucursales y oficinas en el extranjero. Realice una evaluación preliminar de las sucursales u oficinas en el extranjero por medio de conversaciones con la alta gerencia en la oficina central del banco estadounidense (por ejemplo, operaciones, clientes, entidades, jurisdicciones, productos, servicios, estrategias de la gerencia, programas de auditoría, líneas de productos previstas, cambios en la gerencia, ampliaciones de la sucursal, riesgos AML y programas AML). Se deben realizar conversaciones similares con la gerencia de las sucursales y oficinas en el extranjero, particularmente aquellas que pueden ser consideradas de mayor riesgo.

9. Coordine con el supervisor del país anfitrión y, si es pertinente, con las agencias regulatorias federales y estatales estadounidenses. Hable sobre sus análisis del cumplimiento con las leyes locales de las sucursales y oficinas en el extranjero. Determine si existe alguna restricción respecto a los materiales que pueden ser revisados, copiados o llevados fuera del país.

10. Si está disponible, revise lo siguiente:

    - Informes de inspecciones normativas previas.
    - Informe de inspecciones normativas del país anfitrión.
    - Informes de auditoría y documentación respaldatoria.
    - Controles de cumplimiento y documentación respaldatoria.

11. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

12. Determine si las pruebas de transacciones son viables. Si lo son, seleccione una muestra de las actividades de riesgo más alto de la sucursal y oficina en el extranjero, en función del análisis de riesgos del banco de esta actividad, inspecciones previas e informes de auditoría. Realice una prueba de transacción de las secciones de procedimientos de inspección ampliados adecuadas (por ejemplo, depósitos vía maletines/bolsos).

13. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados a las sucursales y oficinas en el extranjero del banco estadounidense.

Banca Paralela: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones de banca paralela, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, debida diligencia e informe.*

Una organización de banca paralela existe cuando por lo menos un banco estadounidense y una institución financiera extranjera son controlados directa o indirectamente por una misma persona o grupo de personas con estrecha relación comercial entre sí o que actúan en forma conjunta, sin estar sujetos a la supervisión consolidada de un único supervisor del país de origen. La institución financiera extranjera estará sujeta a distintas normas y controles de lavado de dinero y a una estructura de vigilancia y de supervisión diferentes, las que pueden ser menos rigurosas que las aplicables en los Estados Unidos. Las diferencias normativas y de supervisión incrementan los riesgos BSA/AML asociados a las organizaciones de banca paralela.

Factores de riesgo

Las organizaciones de banca paralela pueden tener una gestión común, compartir políticas y procedimientos, venderse productos mutuamente, o en general estar vinculadas a una institución financiera extranjera paralela en muchos sentidos. La principal preocupación relativa al lavado de dinero respecto a las organizaciones de banca paralela es que el banco estadounidense puede estar expuesto a mayor riesgo por las transacciones realizadas con la institución financiera extranjera paralela. Se pueden facilitar las transacciones y los riesgos pueden aumentar debido a la ausencia de mecanismos de distanciamiento en los negocios o los controles reducidos que se aplican a las transacciones entre bancos vinculados o estrechamente asociados. Por ejemplo, es posible que compartan sus funcionarios o directores o que éstos trabajen conjuntamente aun si son diferentes.[159]

Mitigación del riesgo

Las políticas, los procedimientos y los procesos del banco estadounidense establecidos para las relaciones de banca paralela deben ser consistentes con los aplicables a las demás relaciones de banco corresponsal extranjero. Además, las bancas paralelas deben:

- Proporcionar líneas independientes de autoridad en la toma de decisiones.
- Protegerse contra conflictos de intereses.
- Garantizar que los negocios sean realizados en condiciones de mercado y con independencia entre las instituciones relacionadas.

[159] Para obtener información sobre riesgos adicionales asociados con banca paralela, consulte *Joint Agency Statement on Parallel-Owned Banking Organizations* (Declaración de agencias conjuntas sobre organizaciones bancarias que son propiedad paralela) publicada por la Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro, el 23 de Abril de 2002.

Procedimientos de Inspección

Banca paralela

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones de banca paralela, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, debida diligencia e informe.*

1. Determine si las relaciones de banca paralela existen mediante diálogos con la gerencia o el análisis de actividades desarrolladas entre varias partes que involucren al banco y a otra institución financiera extranjera. Revise las políticas, los procedimientos y los procesos con respecto a las relaciones de banca paralela. Evalúe la aptitud de las políticas, los procedimientos y los procesos con relación a las actividades de banca paralela del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Determine si existen conflictos de interés o diferencias en las políticas, los procedimientos y los procesos entre las relaciones de banca paralela y otras relaciones bancarias corresponsales extranjeras. Se debe considerar especialmente las actividades de transferencia de fondos, depósitos vía maletines/bolsos y cuentas empleadas para pagos porque estas actividades son más vulnerables al lavado de dinero. Si el banco participa en alguna de estas actividades, los inspectores deben analizar si corresponde realizar procedimientos de inspección de la sección ampliada aplicables que se ocupen de cada uno de estos temas.

3. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones de banca paralela, particularmente aquellas que presenten un riesgo más alto de lavado de dinero.

4. Determine si el sistema del banco para supervisar las relaciones de banca paralela en busca de actividades sospechosas e informar de actividades sospechosas, es adecuado a su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con los clientes.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de sus actividades de banca paralela, así como inspecciones previas e informes de auditoría, seleccione una muestra de actividades de riesgo más alto que puedan presentar las relaciones de banca paralela (por ejemplo, bancos corresponsales extranjeros, transferencia de fondos, cuentas empleadas para pagos y depósitos vía maletines/bolsos).

7. Considere la ubicación de la institución financiera paralela extranjera. Si la jurisdicción es de riesgo más alto, los inspectores deben controlar una muestra mayor de transacciones entre las dos instituciones. Los bancos que realizan negocios con organizaciones bancarias extranjeras paralelas en países que no han sido designados como de riesgo más alto pueden exigir de todos modos debida diligencia especial, pero esa determinación estará basada en el tamaño, carácter y tipo de las transacciones entre las instituciones.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las organizaciones de banca paralela. Concéntrese en determinar si existen controles para garantizar que los negocios se desarrollen en condiciones de mercado y con independencia entre las dos entidades. Si surgen inquietudes importantes acerca de la relación entre las dos entidades, recomiende que esta información sea enviada a las autoridades de supervisión adecuadas.

ESQUEMA GENERAL AMPLIADO Y PROCEDIMIENTOS DE INSPECCIÓN DE PRODUCTOS Y SERVICIOS

Cuentas Corresponsales (Nacionales): Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con el ofrecimiento de relaciones de cuentas corresponsales nacionales, y de la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Los bancos mantienen relaciones corresponsales en otros bancos nacionales para proporcionar algunos servicios que pueden realizarse de manera más económica o eficaz debido al tamaño, la pericia técnica en un rubro de la actividad comercial específico o la ubicación geográfica del otro banco. Dichos servicios pueden incluir:

- **Cuentas de depósito.** Los activos conocidos como "efectivo en depósitos bancarios" o "saldos en bancos corresponsales" pueden representar la cuenta principal de operaciones del banco.
- **Transferencias de fondos.** Una transferencia de fondos entre bancos puede ser el resultado del cobro de cheques u otros instrumentos en efectivo, transferencia y liquidación de transacciones de valores, transferencia de fondos de préstamos participables, compra o venta de fondos federales o procesamiento de transacciones de los clientes.
- **Otros servicios.** Los servicios incluyen el procesamiento de participaciones de préstamos, la facilitación de ventas de préstamos de mercado secundarios, el procesamiento de datos y servicios de nómina y el cambio de moneda extranjera.

Bancos de los banqueros

Un banco de los banqueros, que está organizado y constituido para negociar con otros bancos, por lo general es propiedad de los bancos a los que le ofrece servicios. Los bancos de banqueros, que no negocian directamente con el público, ofrecen servicios bancarios corresponsales a bancos comunitarios independientes, instituciones de ahorro y crédito, cooperativas de crédito y préstamo y fideicomisos de inversión de bienes inmuebles. Los bancos de los banqueros prestan servicios directamente, mediante contratación tercerizada o a través del patrocinio o aval otorgado a terceros. Los productos que ofrecen los bancos de los banqueros por lo general consisten en servicios tradicionales de bancos corresponsales. Los bancos de los banqueros deben tener políticas, procedimientos y procesos en función del riesgo para gestionar los riesgos BSA/AML planteados en estas relaciones corresponsales, detectar e informar actividades sospechosas.

Por lo general, un banco de los banqueros firma un acuerdo de servicio con el banco respondiente[160] describiendo las responsabilidades de cada parte. El acuerdo de servicios puede incluir lo siguiente:

- Productos y servicios que se ofrecen.
- Responsabilidad de la gestión de registros (por ejemplo, informes de transacciones en efectivo presentados).
- Responsabilidad de las tareas realizadas (por ejemplo, filtrados según la OFAC).
- Control de la documentación supervisada (por ejemplo, informes de consultores y de auditoría).

Factores de riesgo

Debido a que los bancos nacionales deben seguir las mismas exigencias normativas, los riesgos BSA/AML en los bancos corresponsales nacionales, incluidos los bancos de los banqueros, son mínimos en comparación a otros tipos de servicios financieros, especialmente para las cuentas de propiedad privada (es decir, el banco nacional utiliza la cuenta corresponsal para sus propias transacciones). Cada banco, sin embargo, tiene su propio enfoque para realizar su programa de cumplimiento BSA/AML, que incluye debida diligencia de los clientes, los sistemas para la información de gestión, la supervisión de cuentas y los informes de actividades sospechosas. Además, si bien es posible que las cuentas corresponsales nacionales no se consideren de riesgo más alto, las transacciones realizadas a través de esas cuentas, que pueden ser realizadas en nombre del cliente de banco representado, pueden implicar riesgo más alto. Los riesgos de lavado de dinero pueden aumentar cuando un banco respondiente le permite a sus clientes efectuar o ejecutar transacciones mediante la cuenta corresponsal, especialmente cuando dichas transacciones son efectuadas o ejecutadas mediante una cuenta de propiedad privada aparente.

El banco corresponsal también enfrenta un aumento en los riesgos cuando proporciona envíos de moneda directos a clientes de bancos respondientes. Esto no significa que esas actividades impliquen necesariamente lavado de dinero, sino que esos envíos de moneda directos deben ser supervisados de manera apropiada en busca de actividades sospechosas y poco habituales. Sin dicho sistema de supervisión, el banco corresponsal está esencialmente proporcionando estos servicios directos a un cliente desconocido.

Mitigación del riesgo

Los bancos que ofrecen servicios bancarios corresponsales a otros bancos respondientes deben disponer de políticas, procedimientos y procesos para gestionar los riesgos BSA/AML que surgen en estas relaciones corresponsales y para detectar e informar actividades sospechosas. Los bancos deben cerciorarse de que las cuentas corresponsales

[160] A respondent bank is any bank for which another bank establishes, maintains, administers, or manages a correspondent account relationship.

nacionales sean de propiedad privada o permitan transacciones de terceros. Cuando el banco respondiente permite a clientes de terceros hacer negocios a través de cuentas corresponsales, el banco corresponsal debe garantizar que comprende los procedimientos de supervisión y debida diligencia aplicados por el banco respondiente a sus clientes que utilizarán la cuenta.

El nivel de riesgo varía dependiendo de los servicios proporcionados y los tipos de transacciones realizadas a través de la cuenta; así como del programa de cumplimiento BSA/AML, productos, servicios, clientes, entidades y ubicaciones geográficas del banco respondiente. Cada banco debe supervisar de manera adecuada las transacciones de cuentas corresponsales nacionales con relación al nivel del riesgo analizado. Además, los bancos nacionales son responsables de manera independiente del cumplimiento de la OFAC de cualquier transacción que fluya a través de sus bancos. Se debe disponer de un filtrado adecuado. Consulte la sección del esquema general principal y los procedimientos de inspección, “Oficina de control de activos extranjeros”, en las páginas 165 a 175 y 176 a 178, respectivamente.

Procedimientos de Inspección

Cuentas corresponsales (nacionales)

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con el ofrecimiento de relaciones de cuentas corresponsales nacionales, y de la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos y cualquier acuerdo de servicio bancario relativo a las relaciones de bancos corresponsales nacionales. Evalúe la aptitud de las políticas, procedimientos y procesos en relación con las cuentas corresponsales nacionales del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y de los factores de valoración de riesgos internos, determine si el banco ha identificado alguna actividad de los bancos corresponsales nacionales como de riesgo más alto.

3. Determine si el sistema del banco para supervisar las cuentas corresponsales nacionales en busca de actividades sospechosas, y para informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del control del banco de las cuentas de bancos respondientes[161] para detectar actividad poco habitual o de riesgo más alto, su análisis de riesgos y los informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de bancos respondientes. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise los estados de cuenta del banco de las cuentas corresponsales nacionales.
   - Revise las transacciones de grandes volúmenes o poco habituales para determinar su carácter. Según sea necesario, obtenga y revise las copias de notas de crédito o débito, los tiquetes de libro mayor y otra documentación respaldatoria.

[161] Un banco respondiente es todo banco para el cual otro banco establece, mantiene, administra o gestiona una relación de cuenta corresponsal.

- Tenga en cuenta cualquier envío de moneda o depósitos realizados en nombre del cliente del banco respondiente. En función de esta información determine si:
  - Los envíos de moneda están documentados de manera adecuada.
  - El banco respondiente ha implementado debida diligencia en los clientes que realizan importantes transacciones en efectivo.
  - Los informes de transacciones en efectivo están presentados de manera adecuada y la actividad es acorde a la actividad prevista.

6. Revise los estados de cuenta del banco para los registros de cuentas corresponsales nacionales o registros de télex de cuentas controladas por la misma persona para depósitos importantes de cheques de caja, giros postales o instrumentos similares librados por otros bancos en sumas inferiores a USD 10.000. Estos fondos serán transferidos probablemente a otra parte en grandes cantidades. Tenga en cuenta si los instrumentos por debajo de USD 10.000 están numerados secuencialmente.
7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las relaciones de los bancos corresponsales nacionales.

Cuentas Corresponsales (Extranjeras): Esquema General

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con los bancos corresponsales extranjeros, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, debida diligencia e informe. Esta sección amplía la revisión principal anterior de las exigencias normativas y legales de las relaciones asociadas con cuentas de bancos corresponsales para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

Las instituciones financieras extranjeras mantienen cuentas en los bancos estadounidenses para acceder al sistema financiero de ese país y aprovechar servicios y productos que pueden no estar disponibles en la jurisdicción de la institución financiera extranjera. Estos servicios pueden ser realizados de manera más económica o eficiente por el banco estadounidense o pueden ser necesarios por otros motivos, como para facilitar el comercio internacional. Los servicios pueden incluir:

- Servicios de administración de efectivo, que incluyen cuentas de depósito.
- Transferencias internacionales de fondos.
- Compensación *(Clearing)* de cheques.
- Cuentas empleadas para pagos.
- Depósitos vía maletines/bolsos.
- Servicios de cambio de moneda extranjera.
- Cuentas de inversión automática (cuentas con servicio de barrido).
- Préstamos y cartas de crédito.

Acuerdos contractuales

Cada relación que un banco estadounidense mantenga con instituciones financieras corresponsales extranjeras debe regirse por un acuerdo o contrato que especifique las obligaciones de cada una de las partes y otros detalles de la relación (por ejemplo, productos y servicios que se ofrecerán, aceptación de depósitos, compensación de elementos, formas de pago y tipos de endoso que se aceptarán). El acuerdo o contrato debe también considerar las exigencias normativas AML de la institución financiera extranjera, el tipo de clientela, los procedimientos de debida diligencia y el uso autorizado de la cuenta corresponsal por terceros.

Factores de riesgo

Algunas instituciones financieras extranjeras no están sujetas a las mismas pautas normativas que se aplican a los bancos estadounidenses; por lo tanto, esas instituciones pueden representar un riesgo de lavado de dinero mayor para su respectivo banco corresponsal estadounidense o sus respectivos bancos estadounidenses. Se han realizado investigaciones que demuestran que, en el pasado, las cuentas corresponsales extranjeras han sido utilizadas por narcotraficantes y otros delincuentes para lavar fondos. A veces se usan compañías fantasmas en el proceso de transformación para ocultar la verdadera propiedad de las cuentas en las instituciones financieras corresponsales extranjeras. Debido al gran volumen de fondos, las múltiples transacciones y la posible falta de familiaridad de los bancos estadounidenses con los clientes de las instituciones financieras corresponsales extranjeras, los delincuentes y terroristas pueden ocultar con mayor facilidad el origen y la utilización de los fondos ilícitos. Por lo tanto, cada banco estadounidense, incluso todas las sucursales, oficinas y subsidiarias en el exterior, debe supervisar cuidadosamente las transacciones relacionadas con las cuentas corresponsales extranjeras.

Sin los controles adecuados, puede ocurrir que los bancos estadounidenses abran cuentas corresponsales tradicionales en una institución financiera extranjera sin saber que ésta les permite a algunos clientes realizar transacciones en forma anónima a través de la cuenta del banco estadounidense (por ejemplo, cuentas para realizar pagos[162] y cuentas anidadas).

Cuentas anidadas

Las cuentas anidadas se producen cuando una institución financiera extranjera logra acceder al sistema financiero de los Estados Unidos operando a través de una cuenta corresponsal estadounidense que pertenece a otra institución financiera extranjera. Si el banco estadounidense desconoce que la institución financiera corresponsal extranjera que es cliente suyo permite dicho acceso a instituciones financieras extranjeras ajenas a esa relación (terceros), éstas pueden efectivamente acceder en forma anónima al sistema financiero estadounidense. El comportamiento que indica la existencia de cuentas anidadas y otras cuentas que despiertan alarma incluye transacciones dirigidas a jurisdicciones en las cuales la institución financiera extranjera no tiene actividades comerciales conocidas ni intereses, y transacciones cuyo volumen total y frecuencia supera significativamente la actividad prevista de la institución financiera extranjera, teniendo en cuenta su base de clientes y el tamaño de sus activos.

Mitigación del riesgo

Los bancos estadounidenses que ofrecen los servicios de instituciones financieras extranjeras corresponsales deben disponer de políticas, procedimientos y procesos para gestionar los riesgos BSA/AML inherentes a estas relaciones, y deben supervisar cuidadosamente las transacciones relacionadas con estas cuentas para detectar e informar

[162] Consulte la sección del esquema general ampliado, “Cuentas empleadas para pagos”, en las páginas 221 a 223, como guía.

actividades sospechosas. El nivel de riesgo varía según los productos, servicios, clientes y ubicación geográfica de la institución financiera extranjera. The Clearing House Payments Co., LLC. y el Grupo Wolfsberg han publicado las normas de la industria y las pautas sugeridas para bancos que prestan servicios bancarios corresponsales extranjeros.[163] Además, la sección del esquema general principal "Debida diligencia y gestión de registros de cuentas corresponsales extranjeras" de las páginas 130 a 138 contiene información adicional. Las políticas, los procedimientos y los procesos de los bancos estadounidenses deben:

- Especificar los procedimientos adecuados de apertura de cuentas, que pueden incluir niveles mínimos de documentación a obtenerse de los clientes probables, un proceso de aprobación de cuenta independiente del rubro de la actividad comercial de la cuenta corresponsal para posibles clientes de riesgo más alto, y una descripción de las circunstancias en las que el banco no abrirá una cuenta.

- Evaluar los riesgos que plantean las relaciones de clientes de cuentas corresponsales extranjeras probables empleando metodologías de análisis de riesgos bien documentadas y coherentes, e incorporar esa determinación del riesgo en el sistema de supervisón de actividades sospechosas del banco.

- Comprender el uso deseado de las cuentas y la actividad de la cuenta prevista (por ejemplo, determinar si la relación ofrecerá servicios de cuenta empleada para pagos).

- Comprender las otras relaciones corresponsales de la institución financiera corresponsal extranjera (por ejemplo, determinar si se podrán utilizar cuentas anidadas).

- Realizar debida diligencia adecuada y continua en las relaciones de la institución financiera corresponsal extranjera, que puede incluir visitas periódicas.

- Establecer un proceso formal para derivar información sospechosa sobre clientes existentes y potenciales a un nivel de gestión apropiado para su control.

- Garantizar que las relaciones de instituciones financieras corresponsales extranjeras estén incluidas de manera apropiada dentro de los sistemas de informe y supervisión de actividades sospechosas del banco estadounidense.

- Garantizar que se apliquen las normas de debida diligencia apropiadas a aquellas cuentas determinadas como de riesgo más alto.

- Establecer criterios para cerrar cuentas de instituciones financieras corresponsales extranjeras.

---

[163] Consulte *Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking* (Pautas para las políticas y procedimientos contra el lavado de dinero en los bancos corresponsales), de Marzo de 2002, en www.theclearinghouse.org/docs/000592.pdf y *Wolfsberg AML Principles for Correspondent Banking* (Principios AML de Wolfsberg para los bancos corresponsales), de Noviembre de 2002, en www.wolfsberg-principles.com/standards.html.

Como práctica responsable, se exhorta a los bancos estadounidenses a comunicar sus expectativas relacionadas con AML a sus clientes de instituciones financieras corresponsales extranjeras. Por otra parte, el banco estadounidense debe comprender en general los controles AML en la institución financiera corresponsal extranjera, que incluyen prácticas de debida diligencia de los clientes y gestión de registros documentales.

Procedimientos de Inspección

Cuentas corresponsales (extranjeras)

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con los bancos corresponsales extranjeros, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, debida diligencia e informe. Esta sección amplía la revisión principal anterior de las exigencias normativas y legales de las relaciones asociadas con cuentas de bancos corresponsales para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras. Evalúe la aptitud de las políticas, los procedimientos y los procesos. Analice si los controles son adecuados para proteger razonablemente al banco estadounidense del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco estadounidense identifica y supervisa de manera eficaz las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras, particularmente aquellas que planteen un riesgo más alto de lavado de dinero.

3. Si el banco estadounidense tiene un acuerdo con bancos corresponsales extranjeros estándar, revise un acuerdo de muestra para determinar si las responsabilidades, los productos y los servicios prestados por cada parte, y el uso permitido de terceros de la cuenta corresponsal, están cubiertos por el acuerdo contractual. Si el banco estadounidense no tiene un acuerdo estándar, consulte los procedimientos de inspección de las pruebas de transacciones.

4. Determine si el sistema del banco estadounidense para supervisar las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras, detectar e informar de actividades sospechosas, es adecuado a su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con los clientes.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de sus actividades con bancos corresponsales extranjeros, así como de informes de inspecciones previas y de auditoría, seleccione una muestra de las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras de riesgo más alto. La muestra de riesgo más alto debe incluir las relaciones con instituciones financieras extranjeras ubicadas en jurisdicciones que no cooperan con las iniciativas AML internacionales y en otras jurisdicciones que el banco estadounidense haya considerado que presentan

un riesgo mayor. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

- Revise un acuerdo con bancos corresponsales extranjeros o un contrato que delimite las responsabilidades y los productos y servicios proporcionados por cada parte.
- Revise los estados de cuenta del banco estadounidense para verificar las cuentas corresponsales extranjeras y, según sea necesario, detalles específicos de las transacciones. Compare las transacciones previstas con la actividad real.
- Determine si la actividad real es coherente con el tipo de negocio del cliente. Identifique cualquier actividad sospechosa o poco habitual.
- Revise las transacciones de grandes volúmenes o poco habituales para determinar su carácter. Según sea necesario, obtenga y revise las copias de notas de crédito o débito, los tiquetes de libro mayor y otra documentación respaldatoria.
- Analice transacciones para identificar un comportamiento que indique la existencia de cuentas anidadas, servicios de agente de compensación o intermediario, u otros servicios para instituciones financieras extranjeras externas que no se hayan identificado claramente.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con relaciones con instituciones financieras corresponsales extranjeras.

Envíos de Efectivo en Grandes Cantidades: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con la recepción de envíos de efectivo en grandes cantidades y la implementación por parte de la gerencia de sistemas eficaces de supervisión e informe.*

Los envíos de efectivo en grandes cantidades implican la utilización de empresas de transporte aéreo, terrestre o marítimo, comunes, independientes o pertenecientes al Servicio Postal, para transportar grandes volúmenes de papel moneda (estadounidense o extranjero) desde fuentes ubicadas dentro o fuera de los Estados Unidos a un banco en los Estados Unidos. A menudo, pero no siempre, los envíos se realizan en contenedores.

Los expedidores pueden ser "remitentes de moneda", es decir, personas o empresas que generan efectivo a partir de la venta al contado de materias primas, u otros productos o servicios (incluidos los instrumentos monetarios o los cambios de moneda). También pueden ser "intermediarios" que envían el efectivo que recolectan de sus clientes remitentes de moneda. Además, los intermediarios pueden enviar el efectivo que recolectan de otros intermediarios. Los intermediarios pueden ser otros bancos, los bancos centrales, las instituciones financieras que no están destinadas al depósito o agentes de estas entidades.

Los bancos reciben los envíos de efectivo en grandes cantidades de manera directa cuando toman posesión de un envío real, y los reciben de manera indirecta cuando toman posesión del equivalente económico de un envío de efectivo, por ejemplo, mediante una notificación de carta de remesa. En el caso de un envío recibido de manera indirecta, generalmente el envío real se traslada al Banco de la Reserva Federal o una sucursal, donde se registra como acreditado a nombre del banco.

Los bancos tienen la obligación de declarar los envíos de efectivo por un importe acumulado superior a USD 10.000 recibidos desde o enviados a ubicaciones que están fuera de los Estados Unidos mediante el Formulario 105 de la FinCEN (Informe sobre el transporte internacional de moneda o instrumentos monetarios), y están exentos de cumplir con esta exigencia de declaración cuando el efectivo se envía por vía terrestre mediante una empresa de transporte común o el Servicio Postal (consulte 31 CFR 103.23). Los bancos no están exentos de cumplir con esta exigencia de declaración cuando el efectivo se envía mediante otros métodos, como las aerolíneas o una empresa de transporte aéreo. Independientemente de que se aplique o no la exención de presentar el Formulario 105 de la FinCEN, los bancos deben supervisar e informar cualquier actividad sospechosa. Además, sin considerar la exigencia de declaración mediante este formulario, los bancos deben informar toda recepción o desembolso de moneda superior a USD 10.000 mediante el Formulario 104 de la FinCEN (Informe de transacciones en efectivo), sujeto a las exenciones de 31 CFR 103.122(d). Esta exigencia de declaración se aplica incluso si las transacciones internacionales están sujetas a la exención de presentar el Formulario 105.

Factores de riesgo

Los envíos de efectivo en grandes cantidades a los bancos por parte de expedidores que se suponen honrados pueden, de todas maneras, originarse a partir de una actividad ilícita. Por ejemplo, frecuentemente los ingresos monetarios resultantes de actividades delictivas reaparecen en el sistema financiero como fondos aparentemente legítimos que han sido colocados y finalmente integrados mediante su circulación a través de numerosos intermediarios y transacciones transformadas que ocultan el origen de los fondos. Las fases de transformación pueden incluir envíos desde y hacia otras jurisdicciones. Consecuentemente, los bancos que reciben envíos de efectivo en grandes cantidades de manera directa o indirecta corren el riesgo de ser coautores en las estratagemas de lavado de dinero y financiamiento del terrorismo.

En los últimos años, el contrabando de efectivo en grandes cantidades se ha convertido en el método preferido para trasladar fondos ilícitos a través de las fronteras.[164] Debido a que las grandes cantidades de efectivo que se contrabandean fuera de los Estados Unidos generalmente son en dólares estadounidenses, quienes reciben dichas cantidades deben encontrar la forma de reintegrar la moneda en un banco estadounidense. A menudo, esto ocurre mediante el uso de una institución financiera extranjera que deliberada o involuntariamente recibe los ingresos ilícitos en dólares estadounidenses y luego emite un instrumento de carta de remesa (o realiza una transferencia de fondos) para su procesamiento (o depósito) en un banco estadounidense. Posteriormente, la institución financiera extranjera inicia el proceso de repatriar físicamente (enviar) el efectivo de regreso a los Estados Unidos.[165] La experiencia a demostrado una correlación directa entre el contrabando de efectivo en grandes cantidades, el aumento del uso de los instrumentos de carta de remesa o las transferencias electrónicas de ciertas instituciones financieras extranjeras, y los envíos de grandes cantidades de efectivo a los Estados Unidos por parte de las mismas instituciones.[166]

---

[164] El lavado de dinero y la evaluación de amenazas en los Estados Unidos, Diciembre de 2005, página 33. El Congreso penalizó el contrabando de grandes cantidades de efectivo como parte de la Ley PATRIOTA de EE. UU. Específicamente, la sección 5332 del Título 31 del U.S.C. sobre el contrabando de efectivo en grandes cantidades establece que es un delito contrabandear o intentar contrabandear un importe superior a USD 10.000 en moneda u otros instrumentos monetarios hacia o desde los Estados Unidos, con el propósito específico de evadir las exigencias de declaración de moneda estadounidense estipuladas en 31 U.S.C. 5316.

[165] En algunos casos, la institución financiera extranjera enviará el efectivo a su banco central o un banco ubicado en uno de los centros financieros del país extranjero en el que se originó el instrumento de carta de remesa. En ocasiones, se realizan varias transacciones trasformadas para ocultar el origen del efectivo, después de las cuales la moneda puede devolverse directamente a los Estados Unidos o puede ser enviada hacia o a través de otras jurisdicciones. El efectivo será enviado a los Estados Unidos a nombre del banco estadounidense donde se procesó el instrumento de carta de remesa o donde se realizó el depósito de la transferencia de fondos.

[166] Si desea ver un ejemplo de estos tipos de transacciones, consulte la Evaluación nacional de amenaza de las drogas 2008 acerca del financiamiento ilícito del Centro Nacional de Inteligencia sobre Droga, Diciembre de 2007.

El envío de efectivo en grandes cantidades no es necesariamente indicativo de una actividad delictiva o terrorista. Muchas personas y empresas, nacionales y extranjeras, generan efectivo a partir de ventas legítimas al contado de materias primas, u otros productos o servicios. Además, los intermediarios recolectan y envían el efectivo de uno o más remitentes de moneda cuyas actividades son legítimas. Los bancos pueden ofrecer servicios en forma legítima para recibir tales envíos. Sin embargo, los bancos deben tener presente el posible uso indebido de sus servicios por parte de los expedidores de efectivo en grandes cantidades. Además, deben protegerse contra la incorporación de los ingresos monetarios resultantes de actividades delictivas o terroristas en el sistema financiero. Con el objeto de informar a los bancos sobre el tema de los envíos de efectivo en grandes cantidades, en 2006 la FinCEN emitió un comunicado que incluye algunas actividades que pueden estar asociadas con el contrabando de efectivo.[167] Según la FinCEN, las autoridades de aplicación de las leyes estadounidenses han observado un aumento significativo en el contrabando de grandes cantidades de efectivo producto de la venta de narcóticos y otras actividades delictivas desde los Estados Unidos hacia México. Si bien el comunicado de la FinCEN menciona específicamente el envío de efectivo en grandes cantidades desde y hacia los Estados Unidos y México, los temas tratados pueden aplicarse también al envío de grandes cantidades de efectivo desde y hacia otras jurisdicciones.

Las autoridades de aplicación de la ley han identificado las siguientes actividades que, en diversas combinaciones, pueden estar asociadas con el contrabando de efectivo:[168]

- Un incremento en la venta de papel moneda estadounidense de alta denominación a instituciones financieras extranjeras por parte de bancos estadounidenses.

- El canje de papel moneda estadounidense de baja denominación que ha sido contrabandeado a un país extranjero por papel moneda estadounidense de alta denominación en posesión de instituciones financieras extranjeras.

- El envío de grandes volúmenes de papel moneda estadounidense de baja denominación desde instituciones financieras no bancarias a sus cuentas estadounidenses vía transporte blindado o su venta directa a bancos estadounidenses.

- Transferencias electrónicas múltiples iniciadas por instituciones financieras extranjeras no bancarias que dan instrucciones a bancos estadounidenses para que remitan fondos a otras jurisdicciones que no parecen tener ninguna relación comercial aparente con esa institución financiera no bancaria extranjera (los receptores de transferencias de fondos incluyen individuos, empresas y otras entidades en áreas de libre comercio y otras ubicaciones).

- El canje de papel moneda estadounidense de baja denominación por papel moneda estadounidense de alta denominación que podría enviarse a países extranjeros.

---

[167] *Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States* (Guía para las instituciones financieras sobre la repatriación de moneda introducida de contrabando a México desde los Estados Unidos) de la FinCEN, FIN-2006-A003, 28 de Abril de 2006.

[168] *Id.*

- Depósitos efectuados por instituciones financieras extranjeras no bancarias en sus cuentas en bancos estadounidenses que incluyen elementos de terceros (entre ellos, instrumentos monetarios numerados en secuencia).

- Depósitos de moneda y elementos de terceros por parte de instituciones financieras extranjeras no bancarias en sus cuentas en instituciones financieras extranjeras y posteriores transferencias bancarias electrónicas directas a las cuentas de la institución financiera extranjera no bancaria en bancos estadounidenses.

Mitigación del riesgo

Los bancos estadounidenses que ofrecen servicios para recibir envíos de efectivo en grandes cantidades deben tener políticas, procedimientos y procesos que permitan mitigar y gestionar los riesgos BSA/AML asociados con la recepción de envíos de efectivo en grandes cantidades. Además, los bancos deben supervisar de cerca las transacciones de envío de efectivo en grandes cantidades con el objeto de detectar e informar cualquier actividad sospechosa, poniendo especial atención en el origen de los fondos y en la adecuación de los volúmenes de transacción por parte de los remitentes de moneda y los intermediarios.

La mitigación del riesgo comienza con un proceso de análisis de riesgos eficaz que permita distinguir las relaciones y las transacciones que presenten un mayor riesgo de lavado de dinero o financiamiento del terrorismo. Los procesos de análisis de riesgos deben considerar la propiedad de los remitentes de moneda y los intermediarios, las geografías, y la naturaleza, el origen, la ubicación y el control de las grandes cantidades de efectivo. Para obtener información adicional relacionada con el análisis de riesgos y la debida diligencia, consulte las secciones del esquema general principal “Análisis de riesgos BSA/AML” en las páginas 23 a 33, y “Debida diligencia de los clientes” en las páginas 69 a 71.

Las políticas, los procedimientos y los procesos de un banco estadounidense deben:

- Especificar los procedimientos adecuados de establecimiento de relaciones en función del riesgo, que pueden incluir niveles mínimos de documentación que deberán proporcionar los posibles remitentes de moneda e intermediarios; un proceso de aprobación de las relaciones que, en el caso de las relaciones con un posible riesgo más alto, sea independiente del rubro de la actividad comercial y pueda incluir una visita al probable expedidor o a los sitios de preparación de los envíos; y una descripción de las circunstancias en las que el banco no establecerá una relación.

- Determinar el fin deseado de la relación , los volúmenes previstos, la frecuencia de la actividad derivada de las transacciones, los orígenes de los fondos, la adecuación de los volúmenes en función de los remitentes y los expedidores, y las obligaciones de presentación de informes según la BSA (CTR, CMIR, etc.).

- Identificar las características de las transacciones aceptables y no aceptables, incluidas las circunstancias en las que el banco aceptará o no los envíos de efectivo en grandes cantidades.

- Evaluar los riesgos que plantea una probable relación de envío mediante metodologías de análisis de riesgos bien documentadas y coherentes.
- Incorporar los análisis de riesgos, según corresponda, en la debida diligencia de los clientes del banco, la EDD y los sistemas de supervisión de actividades sospechosas.
- Una vez establecida la relación, exigir una debida diligencia adecuada y continua que, según corresponda, puede incluir visitas periódicas al expedidor y a los sitios de preparación de los envíos. Según sea necesario, realizar el escrutinio de la legitimidad del origen de los envíos de efectivo mediante procesos basados en el riesgo.
- Garantizar que se apliquen las normas de debida diligencia apropiadas a las relaciones determinadas como de riesgo más alto.
- Incluir los procedimientos para el procesamiento de los envíos, que incluyen las responsabilidades de los empleados, los controles, las exigencias de conciliación y documentación, y las autorizaciones de la gerencia para los empleados.
- Establecer un proceso formal para derivar la información sospechosa sobre las relaciones y las transacciones que involucran a remitentes de moneda e intermediarios existentes y potenciales a un nivel de gestión apropiado para su control.
- Rechazar los envíos cuyos orígenes son sospechosos o cuestionables.
- Asegurar la inclusión de las relaciones de envío y las comparaciones de los volúmenes de envío previstos y reales, según corresponda, en los sistemas de los bancos estadounidenses con el objeto de supervisar e informar las actividades sospechosas.
- Establecer los criterios para finalizar una relación de envío.

Como práctica responsable, los bancos estadounidenses deben informar a los remitentes de moneda y a los intermediarios acerca de las expectativas y las exigencias relacionadas con BSA/AML que se aplican a los bancos estadounidenses. Los bancos estadounidenses también deben comprender los controles de BSA/AML que se aplican a, o que de lo contrario son adoptados por, el remitente de moneda o el intermediario, que incluyen la debida diligencia de los clientes, y las prácticas o las obligaciones relacionadas con la gestión de registros.

También puede haber otros controles que sean útiles para proteger a los bancos contra los envíos ilícitos de grandes cantidades de efectivo, entre los que se pueden incluir los controles de los bancos corresponsales extranjeros, los depósitos vía maletines/bolsos, las transferencias de fondos, las transacciones internacionales de compensación automatizada y la captura de depósitos remotos.

Acuerdos contractuales

Los bancos estadounidenses deben establecer acuerdos o contratos con los remitentes de moneda o los intermediarios. El acuerdo o contrato debe describir las responsabilidades de cada parte y demás detalles relevantes de la relación. Además, debe reflejar y ser coherente con las consideraciones de BSA/AML que se aplican al banco, el remitente de moneda o el intermediario, y los clientes del intermediario o el remitente de moneda. Asimismo, debe cubrir las expectativas acerca de la debida diligencia y el permiso de uso de los servicios del expedidor por parte de terceros. Si bien los acuerdos y los contratos también deben proporcionar las consideraciones, obligaciones y controles de BSA/AML respectivos, los bancos estadounidenses no pueden ceder sus responsabilidades según BSA/AML a otros.

Procedimientos de Inspección

Envíos de efectivo en grandes cantidades

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con los envíos de efectivo en grandes cantidades, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, debida diligencia e informe.*

1. Determine si el banco recibe envíos de efectivo en grandes cantidades.

2. Revise la aptitud de las políticas, los procedimientos y los procesos relacionados con la recepción de envíos de efectivo en grandes cantidades, dados la actividad y los riesgos presentes.

3. Revise la lista de remitentes de moneda e intermediarios que envían efectivo en grandes cantidades al banco.

4. Determine si la gerencia ha analizado los riesgos asociados con la recepción de envíos de efectivo en grandes cantidades de remitentes de moneda e intermediarios. Tenga en cuenta el origen del dinero del remitente de moneda o el intermediario y la adecuación de los volúmenes de transacción. Evalúe la aptitud de la metodología de análisis de riesgos.

5. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones con los remitentes de moneda y los intermediarios, particularmente aquellas que presenten un riesgo más alto de lavado de dinero o financiamiento del terrorismo.

6. Si el banco tiene un acuerdo o un contrato con remitentes de moneda o intermediarios, revise un acuerdo o un contrato de muestra para determinar si las responsabilidades, los productos y los servicios provistos de cada parte, y el uso permitido de terceros de la relación, incluidas las responsabilidades de BSA/AML de las partes, están cubiertos. Si el banco estadounidense no tiene un acuerdo o un contrato estándar, consulte los procedimientos de inspección de las pruebas de transacciones a continuación.

7. Determine si el sistema del banco para supervisar e informar las actividades sospechosas relacionadas con las relaciones y las transacciones de envío es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

8. Determine si el banco está supervisando los volúmenes de envío reales en comparación con los previstos y si está tomando medidas ante los aumentos excesivos o poco habituales en los volúmenes.

Pruebas de transacciones

9. En función del análisis de riesgos del banco de sus relaciones con los remitentes de moneda y los intermediarios, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de los remitentes de moneda o los intermediarios, y de los últimos envíos de efectivo en grandes cantidades. La muestra debe incluir relaciones con remitentes de moneda e intermediarios que estén ubicados en jurisdicciones que puedan plantear un riesgo más alto de lavado de dinero y financiamiento del terrorismo o que realicen envíos desde dichas jurisdicciones, o que participen en actividades comerciales que puedan plantear un riesgo más alto de lavado de dinero y financiamiento del terrorismo.

10. Preferentemente sin previo aviso y durante un período de varios días, no necesariamente consecutivos, observe el proceso de aceptación de envíos de efectivo en grandes cantidades. Revise los registros y los envíos en busca de irregularidades. A partir de las muestras seleccionadas, lleve a cabo los siguientes procedimientos de inspección:

    - Revise la integridad de un acuerdo o un contrato de relación que delimite las responsabilidades, los productos y los servicios provistos de cada parte.

    - Revise los estados de cuenta del banco estadounidense y, según sea necesario, los detalles específicos de las transacciones.

    - Revise los registros de control de la bóveda con relación a las transacciones de envío de efectivo en grandes cantidades (depósitos y extracciones) para identificar la actividad de alta denominación como resultado de los cambios de billetes de baja denominación.

    - Evalúe la adecuación de la información de debida diligencia de los clientes y EDD concerniente a los remitentes de moneda y los intermediarios de la muestra.

    - Determine si la naturaleza, el volumen y la frecuencia de la actividad con coherentes con las expectativas asociadas al remitente de moneda y al intermediario. Hable con la gerencia del banco sobre cualquier incoherencia identificada. Según sea necesario, obtenga y revise las copias de notas de crédito o débito, los tiquetes de libro mayor y otra documentación respaldatoria.

    - Revise las transacciones poco habituales y la información de debida diligencia de los clientes para determinar si las transacciones son potencialmente sospechosas.

    - Hable con la gerencia sobre las conclusiones y los resultados preliminares.

11. Si el remitente de moneda o el intermediario, o el agente referente que trabaja para el remitente de moneda o el intermediario, tienen una cuenta en el banco, revise una muestra de la actividad de la cuenta.

12. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con el envío de efectivo en grandes cantidades.

Giros en Dólares Estadounidenses: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los giros en dólares estadounidenses, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Un giro en dólares estadounidenses es un giro o cheque bancario en dólares estadounidenses disponible en instituciones financieras extranjeras. Estos giros se libran de una cuenta corresponsal estadounidense por una institución financiera extranjera. Los giros se adquieren con frecuencia para pagar transacciones personales o comerciales, y para conciliar obligaciones en el exterior.

Factores de riesgo

La mayoría de los giros en dólares estadounidenses son legítimos; sin embargo, se ha comprobado que éstos son vulnerables al abuso del lavado de dinero. Dichas estratagemas relacionadas con los giros en dólares estadounidenses pueden involucrar el contrabando de moneda estadounidense a instituciones financieras extranjeras para la compra de un cheque o giro en dólares estadounidenses. La institución financiera extranjera acepta la moneda estadounidense y expide un giro en dólares estadounidenses librado de su cuenta de banco corresponsal estadounidense. Una vez que el dinero se encuentra en la forma de giro bancario, la persona implicada en el lavado de dinero puede ocultar más fácilmente el origen de los fondos. La capacidad de convertir ingresos ilícitos a un giro bancario en una institución financiera extranjera permite que el lavador de dinero transporte el instrumento nuevamente a los Estados Unidos o lo endose a un tercero en una jurisdicción donde las leyes contra el lavado de dinero o de cumplimiento son laxas. En cualquier caso, el individuo habrá blanqueado los ingresos ilícitos; finalmente, el giro o cheque se devolverá para su procesamiento en el banco corresponsal estadounidense.

Mitigación del riesgo

Las políticas, los procedimientos y los procesos de un banco estadounidense deben incluir lo siguiente:

- Descripción de los criterios para iniciar una relación asociada con giros en dólares estadounidenses con una institución o entidad financiera extranjera (por ejemplo: jurisdicción; productos, servicios, mercado objetivo; propósito de la cuenta y actividad prevista; o antecedentes del cliente).
- Especificación de las transacciones aceptables y no aceptables (por ejemplo, el fraccionamiento de las transacciones o la compra de múltiples giros numerados en secuencia para el mismo beneficiario).
- Especificación de la supervisión y elaboración de informes de actividades sospechosas asociadas con giros en dólares estadounidenses.
- Planteamiento de los criterios para cesar relaciones asociadas con giros en dólares estadounidenses.

Procedimientos de Inspección

Giros en dólares estadounidenses

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los giros en dólares estadounidenses, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a los giros en dólares estadounidenses. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de giros en dólares estadounidenses del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo. Determine si las políticas abordan lo siguiente:

   - Criterios para permitir que una institución o entidad financiera extranjera expida giros en dólares estadounidenses (por ejemplo: jurisdicción; productos, servicios y mercados objetivo; propósito de la cuenta y actividad prevista; antecedentes del cliente; y otra información disponible).
   - Identificación de transacciones poco habituales (por ejemplo, fraccionamiento de las transacciones o la compra de múltiples giros en dólares estadounidenses numerados en secuencia para el mismo beneficiario).
   - Criterios para cesar la expedición de giros en dólares estadounidenses a través de una institución o entidad financiera extranjera.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de giros en dólares estadounidenses de riesgo más alto.

3. Determine si el sistema del banco para supervisar las cuentas de giros en dólares estadounidenses, detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Obtenga una lista de las cuentas de bancos corresponsales extranjeros en los que se ofrezcan giros en dólares estadounidenses. Revise el volumen, por número y suma en dólares, de las transacciones mensuales de cada cuenta. Determine si la gerencia ha analizado los riesgos de manera adecuada.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades con giros en dólares estadounidenses, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de bancos corresponsales extranjeros en los que se procesen giros en dólares estadounidenses. En la muestra seleccionada, incluya las cuentas con gran volumen de actividad con giros en dólares estadounidenses. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

- Revise las transacciones para verificar los giros en dólares estadounidenses numerados en secuencia para el mismo beneficiario o del mismo emisor. Investigue cualquier transacción con giros en dólares estadounidenses sospechosa o poco habitual.
- Revise los contratos y acuerdos del banco con bancos corresponsales extranjeros. Determine si los contratos describen los procedimientos para procesar y compensar giros en dólares estadounidenses.
- Verifique que el banco haya obtenido y controlado la información acerca de las exigencias normativas AML del país de origen de la institución financiera extranjera (por ejemplo, identificación de clientes y presentación de informes de actividades sospechosas).

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con giros en dólares estadounidenses.

Cuentas Empleadas para Pagos: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las cuentas empleadas para pagos (PTA), y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Las instituciones financieras extranjeras utilizan PTA, también conocidas como cuentas "directas" o "de transferencias", para proporcionar a sus clientes el acceso al sistema bancario estadounidense. Algunos bancos estadounidenses, corporaciones que se rigen por la Ley de Organizaciones Bancarias Extranjeras (*Edge Act*) y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal, sucursales estadounidenses y agencias de instituciones financieras extranjeras (colectivamente denominados bancos estadounidenses) ofrecen estas cuentas como un servicio a las instituciones financieras extranjeras. Las autoridades de aplicación de la ley han declarado que el riesgo de lavado de dinero y otras actividades ilícitas es más alto en las PTA que no se controlan de manera adecuada.

Generalmente, una institución financiera extranjera solicita una PTA para sus clientes que desean efectuar transacciones bancarias en los Estados Unidos a través de la cuenta en un banco estadounidense de la institución financiera extranjera. La institución financiera extranjera proporciona a sus clientes, comúnmente denominados "cotitulares de cuentas", cheques que les permiten retirar fondos de la cuenta en el banco estadounidense de la institución financiera extranjera.[169] Los cotitulares de PTA, que pueden ser cientos o miles para una sola cuenta, se convierten todos en firmantes de la cuenta en el banco estadounidense de la institución financiera extranjera. Aunque los clientes de cuentas empleadas para pagos pueden librar cheques y efectuar depósitos en un banco en los Estados Unidos como cualquier otro titular de cuenta, es posible que no estén sujetos de manera directa a las exigencias de apertura de cuentas del banco en los Estados Unidos.

Las actividades de PTA no deben confundirse con las relaciones tradicionales con bancos corresponsales internacionales, en las que una institución financiera extranjera celebra un acuerdo con un banco estadounidense para procesar y efectuar transacciones en nombre de la institución financiera extranjera y sus clientes. Bajo el mencionado acuerdo corresponsal, los clientes de la institución financiera extranjera no tienen acceso directo a la cuenta corresponsal en el banco estadounidense, pero sí realizan negocios a través del banco estadounidense. Este acuerdo difiere significativamente de una PTA con cotitulares de cuentas que tienen acceso directo al banco estadounidense en virtud de su capacidad de efectuar transacciones de manera independiente con el banco estadounidense a través de la PTA.

[169] En este tipo de relación, la institución financiera extranjera se denomina comúnmente "titular principal de cuenta".

Factores de riesgo

Las PTA pueden ser propensas a un riesgo mayor porque los bancos estadounidenses generalmente no implementan las mismas exigencias de debida diligencia para PTA que para los clientes nacionales que desean abrir una cuenta corriente u otro tipo de cuenta. Por ejemplo, algunos bancos estadounidenses simplemente solicitan una copia de las tarjetas de registro de firmas completadas por los clientes de cuentas empleadas para pagos (el cliente de la institución financiera extranjera). Luego, estos bancos estadounidenses procesan miles de cheques de cotitulares de cuentas y otras transacciones, incluidos los depósitos de dinero en efectivo, a través de la PTA de la institución financiera extranjera. En la mayoría de los casos, se hace poco o ningún esfuerzo para obtener o confirmar la información acerca de los cotitulares de cuenta comerciales e individuales que utilizan las PTA.

El uso de las PTA por parte de las instituciones financieras extranjeras, junto a una supervisión inadecuada por parte de los bancos estadounidenses, pueden facilitar las prácticas bancarias cuestionables, incluidos el lavado de dinero y las actividades delictivas relacionadas. La probabilidad de facilitar el lavado de dinero o el financiamiento del terrorismo, las violaciones de la normativa de la OFAC y otros delitos graves aumenta cuando un banco estadounidense no puede identificar y comprender de manera adecuada las transacciones de los usuarios finales (todos o la mayoría de los cuales se encuentran afuera de los Estados Unidos) de su cuenta con un banco corresponsal extranjero. Las PTA que se utilizan para fines ilegales pueden ocasionar a los bancos graves pérdidas financieras en multas y sanciones civiles y penales, embargo o confiscación de bienes dados en garantía, y daños a la reputación.

Mitigación del riesgo

Los bancos estadounidenses que ofrecen servicios de PTA deben desarrollar y mantener políticas, procedimientos y procesos adecuados para protegerse contra el posible uso ilícito de estas cuentas. Como mínimo, las políticas, los procedimientos y los procesos deben permitir a cada banco estadounidense identificar los usuarios finales de su PTA de la institución financiera extranjera y permitirle obtener (o tener la capacidad de obtener a través de un acuerdo con un tercero fiable) sustancialmente la misma información sobre los usuarios finales de la PTA como la que obtiene de sus clientes directos.

Las políticas, los procedimientos y los procesos deben incluir un control de los procesos de la institución financiera extranjera para identificar y supervisar las transacciones de los cotitulares de cuenta y para cumplir con cualquier exigencia normativa y estatutaria AML existente en el país anfitrión y el acuerdo marco de la institución financiera extranjera con el banco estadounidense. Además, los bancos estadounidenses deben contar con procedimientos para supervisar las transacciones efectuadas en las PTA de las instituciones financieras extranjeras.

En un intento de considerar el riesgo inherente a las PTA, los bancos estadounidenses deben contar con un contrato firmado (es decir, un acuerdo marco) que incluya:

- Papeles y responsabilidades de cada parte.
- Límites o restricciones en cuanto a los tipos y las cantidades de transacciones (por ejemplo, depósitos de dinero en efectivo, transferencias de fondos, cobro de cheques).
- Restricciones en cuanto a los tipos de cotitulares de cuentas (por ejemplo, casas de cambio, compañías de financiamiento, emisores de fondos u otras instituciones financieras no bancarias).
- Prohibiciones o restricciones en cuanto a los cotitulares de cuentas con varios niveles.[170]
- Acceso a los documentos internos y auditorías de la institución financiera extranjera concernientes a su actividad de PTA.

Los bancos estadounidenses deben contemplar la posibilidad de cerrar la PTA bajo las siguientes circunstancias:

- Información insuficiente sobre los usuarios finales de la PTA.
- Evidencia de actividad sospechosa sustantiva o continua.
- Incapacidad de garantizar que las PTA no se estén utilizando para el lavado de dinero u otros fines ilícitos.

[170] Una subcuenta se puede subdividir en más subcuentas para diferentes personas.

Procedimientos de Inspección

Cuentas empleadas para pagos

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las cuentas empleadas para pagos (PTA), y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las PTA. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de PTA del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo. Determine si:

   - Los criterios para iniciar relaciones asociadas con PTA con una institución financiera extranjera son adecuados. Los ejemplos de los factores que pueden utilizarse incluyen: jurisdicción; refugios en cuanto al lavado de dinero o secreto bancario; productos, servicios y mercados; propósito; actividad prevista; antecedentes del cliente; propiedad; alta gerencia; acta constitutiva; licencia bancaria; certificado de solvencia y existencia; y demostración de la capacidad operativa de la institución financiera extranjera de supervisar la actividad de cuenta.

   - Se ha obtenido y validado la información adecuada de la institución financiera extranjera sobre la identidad de cualquier persona que tenga autoridad para efectuar transacciones a través de la PTA.

   - Se ha obtenido información y debida diligencia especial de la institución financiera extranjera en cuanto a la fuente y el usufructo de los fondos de personas que tienen autoridad para efectuar transacciones a través de la PTA (por ejemplo, nombre, domicilio, nivel de actividad prevista, lugar de empleo, descripción de la empresa, cuentas relacionadas, identificación de personalidades sujetas a exposición política extranjeras, fuente de los fondos y actas constitutivas).

   - No se han abierto subcuentas antes de que el banco estadounidense haya controlado y aprobado la información del cliente.

   - Las cuentas principales o las subcuentas se pueden cerrar si la información proporcionada al banco es materialmente errónea o está incompleta.

   - El banco puede identificar a todos los firmantes de cada subcuenta.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las PTA.

3. Determine si el sistema de supervisión de las PTA del banco para detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Para analizar el volumen de riesgo y determinar si se han asignado recursos adecuados a la actividad de supervisión, procúrese una lista de cuentas de bancos corresponsales extranjeros en los que se ofrezcan PTA y solicite informes de los sistemas para la información de gestión que muestren:

   - La cantidad de subcuentas en cada PTA.
   - El volumen y suma en dólares de las transacciones mensuales de cada subcuenta.

5. Verifique que el banco haya obtenido y controlado la información acerca de las exigencias normativas AML del país de origen de la institución financiera extranjera (por ejemplo, exigencias de identificación de clientes y presentación de informes de actividades sospechosas) y tenga en cuenta estas exigencias al controlar las PTA. Determine si el banco ha garantizado que los acuerdos de subcuentas cumplan con cualquier exigencia normativa y estatutaria AML existente en el país de origen de la institución financiera extranjera.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de control de activos extranjeros", en las páginas 176 a 178, como guía.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus actividades de PTA, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las PTA. De la muestra, revise los contratos o acuerdos con la institución financiera extranjera. Determine si los contratos o acuerdos:

   - Describen claramente las responsabilidades contractuales tanto del banco estadounidense como de la institución financiera extranjera.
   - Definen los procesos de apertura de PTA y subcuentas, y exigen un control y un proceso de aprobación independientes al abrir la cuenta.
   - Exigen a la institución financiera extranjera que cumpla con sus exigencias AML locales.
   - Restringen la apertura de subcuentas por parte de casas de cambio, compañías de financiamiento, emisores de fondos u otras instituciones financieras no bancarias.
   - Prohíben la existencia de cotitulares de cuentas con varios niveles.
   - Proporcionan controles adecuados sobre los depósitos y las extracciones de dinero en efectivo por parte de los cotitulares de cuentas y garantizan que los informes de transacciones en efectivo se hayan presentado de manera adecuada.
   - Proporcionan límites de dólares para las transacciones de cada cotitular de cuenta que sean coherentes con la actividad prevista de la cuenta.
   - Cuentan con exigencias de documentación que sean coherentes con aquellas utilizadas para la apertura de cuentas nacionales del banco estadounidense.

- Proporcionan al banco estadounidense la capacidad de controlar la información acerca de la identidad de los cotitulares de cuentas (por ejemplo, de manera directa o través de un tercero fiable).
- Exigen a la institución financiera extranjera que supervise las actividades de las subcuentas para detectar actividades sospechosas o poco habituales e informe de los resultados al banco estadounidense.
- Permiten al banco estadounidense, según lo autoricen las leyes locales, llevar a cabo una auditoría de las operaciones de PTA de la institución financiera extranjera y tener acceso a los documentos de PTA.

8. Revise los estados de cuenta principal de PTA. (El inspector debe determinar el plazo en base al tamaño y la complejidad del banco). Los estados de cuenta elegidos deben incluir las transacciones frecuentes y de grandes volúmenes en dólares. Verifique los estados de cuenta según el libro mayor y las conciliaciones bancarias. Tenga en cuenta cualquier envío o depósito de moneda efectuado en el banco estadounidense en nombre de un cotitular de cuenta en particular para verificar el crédito a la subcuenta del cliente.
9. De la muestra seleccionada, revise la información de identificación y transacciones relacionadas de cada cotitular de cuenta durante el período que determine el inspector. Evalúe las transacciones de los cotitulares de PTA. Determine si las transacciones son coherentes con las transacciones previstas o si requieren más investigación. (La muestra debe incluir cotitulares de cuenta con actividad en dólares significativa).
10. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las PTA.

Actividades de Depósitos vía Maletines/Bolsos: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de depósitos vía maletines/bolsos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Las actividades de depósitos vía maletines/bolsos implican la utilización de empresas de transporte, de servicios de correo especial (independiente o público) o de agentes referentes empleados por los servicios de correo especial,[171] para transportar moneda, instrumentos monetarios y otros documentos desde afuera de los Estados Unidos a bancos estadounidenses.[172] Otros bancos o personas físicas pueden remitir depósitos vía maletines/bolsos. Los servicios de depósitos vía maletines/bolsos normalmente se ofrecen conjuntamente con servicios de bancos corresponsales extranjeros. Los depósitos vía maletines/bolsos pueden contener pagos de préstamos, transacciones de cuentas corrientes y otros tipos de transacciones. Cada vez más, algunos bancos están utilizando la captura de depósitos remotos (RDC, por sus siglas en inglés), que es un sistema de ejecución de transacciones de depósito que permite reemplazar las actividades de depósitos vía maletines/bolsos. Si desea más información sobre la RDC, consulte la sección del esquema general ampliado sobre Transacciones bancarias electrónicas en las páginas 231 a 235.

Factores de riesgo

Los bancos deben tener en cuenta que con frecuencia se han encontrado en los depósitos vía maletines/bolsos o remesas de cheques recibidos de instituciones financieras extranjeras grandes cantidades de instrumentos monetarios comprados en los Estados Unidos que parecen haber sido estructurados para evitar las exigencias de informe de la BSA. Esto es especialmente válido en el caso de depósitos vía maletines/bolsos y remesas de cheques recibidas de jurisdicciones cuyas estructuras AML son laxas o deficientes. Los instrumentos monetarios involucrados son con frecuencia giros postales, cheques de viajeros y cheques bancarios que usualmente comparten una o más de las siguientes características:

- Los instrumentos se compraron el mismo día o en días consecutivos en diferentes localidades.

---

[171] Los agentes referentes son personas físicas o corporaciones extranjeras, que están obligadas por contrato con el banco estadounidense. Prestan servicios de representación a los clientes del banco en el extranjero a cambio de honorarios. Los servicios pueden ir desde derivar clientes nuevos al banco hasta la administración especial de correo, la obtención y el transporte de documentos, la distribución de folletos y solicitudes o formularios del banco, la escrituración o autenticación de documentos para los clientes y el envío por correo de los fondos de los clientes al banco en los Estados Unidos para su depósito.

[172] Como guía, consulte la sección del esquema general principal, "Informe sobre el transporte internacional de moneda o instrumentos monetarios", en las páginas 162 y 163.

- Están numerados consecutivamente y sus montos son ligeramente inferiores a USD 3.000 o USD 10.000.
- Los espacios donde se deben completar los datos de los beneficiarios se dejan en blanco o se hacen a la misma persona (o solamente a unas pocas personas).
- Contienen poca o ninguna información sobre el comprador.
- Tienen la misma estampilla, símbolo o iniciales.
- Se compran por valores expresados en cifras redondas o por montos repetidos.
- Al depósito de los instrumentos le sigue al poco tiempo una extracción de fondos en forma de transferencia por el mismo valor en dólares.

Mitigación del riesgo

Los bancos deben disponer de políticas, procedimientos y procesos relativos a las actividades de depósitos vía maletines/bolsos que deben:

- Describir los criterios de apertura de una relación de depósitos vía maletines/bolsos con una persona o institución financiera extranjera (por ejemplo, exigencias de debida diligencia de los clientes, tipo de institución o persona, propósito aceptable de la relación).
- Detallar las transacciones aceptables e inaceptables (por ejemplo, instrumentos monetarios cuyos beneficiarios aparecen en blanco, instrumentos monetarios sin firmar, y gran cantidad de instrumentos monetarios con numeración consecutiva).
- Detallar los procedimientos para el procesamiento de los depósitos vía maletines/bolsos, incluidos la responsabilidad de los empleados, controles dobles, exigencias de conciliación y documentación y comprobación de empleados.
- Detallar los procedimientos para el control de actividades poco habituales o sospechosas, incluida la derivación de cualquier inquietud a la gerencia. (Los contenidos de los depósitos vía maletines/bolsos pueden estar sujetos a la exigencia de presentar informes de transacciones en efectivo [CTR], informes sobre el transporte internacional de moneda o instrumentos monetarios [CMIR] e informes de actividades sospechosas [SAR]).
- Dialogar sobre los criterios a emplear para el cierre de las relaciones de depósitos vía maletines/bolsos.

Los factores anteriores deben incluirse en un acuerdo o contrato entre el banco y el correo especial que detalle los servicios que se prestarán y las responsabilidades de las dos partes.

Procedimientos de Inspección

Actividades de depósitos vía maletines/bolsos

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de depósitos vía maletines/bolsos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Determine si el banco tiene actividad saliente o entrante de depósitos vía maletines/bolsos y si la actividad se realiza por medio de empresas de transporte o servicios de correo especial.

2. Revise las políticas, los procedimientos, los procesos y cualquier acuerdo contractual relativos a las actividades de depósitos vía maletines/bolsos. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de depósitos vía maletines/bolsos y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

3. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las actividades de depósitos vía maletines/bolsos.

4. Determine si el sistema de supervisión de las actividades de depósitos vía maletines/bolsos del banco para detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Revise la lista de los clientes del banco a los que se les permite utilizar servicios de depósitos vía maletines/bolsos (entrante y saliente). Determine si la gerencia ha analizado el riesgo de los clientes a los que se les permite utilizar este servicio.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus actividades de depósitos vía maletines/bolsos, así como de informes de inspecciones previas y de auditoría, seleccione una muestra de los depósitos vía maletines/bolsos diarios para realizar un control. Preferentemente sin previo aviso y durante un período de varios días, no necesariamente consecutivos, observe la apertura de depósitos vía maletines/bolsos y el proceso de obtención de datos sobre los elementos incluidos en la muestra de depósitos vía maletines/bolsos entrantes, y observe la preparación de los depósitos vía maletines/bolsos salientes. Revise los registros y los contenidos de los depósitos vía

maletines/bolsos en busca de moneda, instrumentos monetarios,[173] valores al portador, tarjetas prepagadas, piedras preciosas, trabajos artísticos, sustancias ilegales, artículos de contrabando u otros elementos que no deberían aparecer normalmente en un depósito vía maletines/bolsos del banco.

8. Si el correo especial o el agente referente que trabaja para este, tiene una cuenta en el banco, revise una muestra adecuada de la actividad de su cuenta.

9. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con los depósitos vía maletines/bolsos.

---

[173] Consulte los procedimientos de inspección de la sección principal, “Informes sobre el transporte internacional de moneda o instrumentos monetarios”, en las páginas 162 y 163, como guía.

Banca Electrónica: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los clientes de banca electrónica (transacciones bancarias electrónicas), incluida la actividad de captura de depósitos remotos (RDC), y la capacidad de la gerencia para implementar sistemas de supervisión e informe eficaces.*

Los sistemas de transacciones bancarias electrónicas, que proporcionan la entrega electrónica de productos bancarios a los clientes, incluyen las transacciones por cajero automático (ATM); la apertura de cuentas por Internet; las transacciones bancarias por Internet; y las transacciones bancarias telefónicas. Por ejemplo, las tarjetas de crédito, las cuentas de depósito, los préstamos hipotecarios y las transferencias de fondos pueden iniciarse a través de Internet, sin contacto directo. La gerencia debe reconocer ésta como un área de un posible riesgo más alto y elaborar políticas, procedimientos y procesos para identificar a clientes y supervisar áreas específicas de las operaciones bancarias. Consulte la sección del esquema general principal, "Programa de identificación de clientes" (CIP), en las páginas 65 a 68, como guía. Más información sobre las transacciones bancarias electrónicas está disponible en *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[174]

Factores de riesgo

Los bancos deben asegurar que sus sistemas de supervisión detecten de manera adecuada las transacciones que se realicen electrónicamente. Como en cualquier cuenta, deben estar alerta a toda anomalía que presente la cuenta. Las señales de advertencia pueden incluir la velocidad con que ingresan fondos a la cuenta o, en el caso de los cajeros automáticos, el número de tarjetas de débito asociadas a la cuenta.

Las cuentas abiertas sin contacto directo pueden implicar mayor riesgo de lavado de dinero y financiamiento del terrorismo, por las siguientes razones:

- Es más difícil verificar positivamente la identidad de la persona.
- El cliente puede estar fuera del área geográfica o país que es el objetivo del banco.
- El cliente puede percibir las transacciones como menos transparentes.
- Las transacciones son instantáneas.
- Pueden ser utilizadas por una empresa "pantalla" o terceros desconocidos.

[174] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

Mitigación del riesgo

Los bancos deben establecer supervisión, identificación e informe BSA/AML de actividades sospechosas y poco habituales que ocurran a través de sistemas de transacciones bancarias electrónicas. Los sistemas para la información de gestión útiles para detectar las actividades poco habituales en cuentas de mayor riesgo incluyen los informes de actividad de cajeros automáticos, informes de transferencias de fondos, informes de actividad de cuentas nuevas, informes de cambio de dirección de Internet, informes de direcciones de Protocolo de Internet (IP) e informes para identificar cuentas relacionadas o vinculadas (por ejemplo, direcciones, números telefónicos, direcciones de correo electrónico y números de identificación tributaria comunes). Para determinar el nivel de supervisión que requiere una cuenta, uno de los factores que los bancos deberían considerar es la forma en que fue abierta la cuenta. Los bancos que se dedican a realizar transacciones bancarias a través de Internet deben contar con métodos confiables y eficaces para legitimar la identidad de los clientes cuando se abren cuentas en línea y deben establecer políticas que determinen cuándo los clientes deberán abrir cuentas mediante contacto directo.[175] Los bancos pueden también imponer otros controles, como establecer límites a las transacciones en dólares de montos elevados, de manera que se requiera una intervención manual para superar el límite preestablecido.

Captura de depósitos remotos

La captura de depósitos remotos (RDC) es un sistema de ejecución de transacciones de depósito que ha aumentado la eficacia del procesamiento de cheques e instrumentos monetarios (por ejemplo, cheques de viajero o giros postales). En términos más amplios, la RDC les permite a los clientes de un banco escanear un cheque o un instrumento monetario, y transmitir posteriormente la imagen escaneada o digitalizada a la institución. Las actividades de escaneado y transmisión ocurren en ubicaciones remotas que incluyen las sucursales del banco, los ATM, los bancos corresponsales nacionales y extranjeros, y las ubicaciones permitidas o controladas por los clientes minoristas o comerciales. Al eliminar las transacciones en persona, la RDC permite disminuir el costo y el volumen de papel asociados con el envío por correo o el depósito físico de elementos. Además, la RDC es compatible con los productos bancarios nuevos y existentes, y posibilita un mejor acceso de los clientes a sus depósitos.

El 14 de Enero de 2009, el FFIEC publicó una guía denominada *Risk Management of Remote Deposit Capture* (Gestión del riesgo de la captura de depósitos remotos) que cubre los componentes fundamentales de la gestión del riesgo de la RDC: la identificación, el análisis y la mitigación del riesgo. Incluye un desarrollo exhaustivo de los factores de riesgo de la RDC y los elementos de mitigación. Consulte www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf.

---

[175] Para obtener más información, consulte *Authentication in an Internet Banking Environment* (Autenticación en un entorno bancario en Internet), publicado por el FFIEC el 13 de OctubreOctubre de 2005.

Factores de riesgo

La RDC puede exponer a los bancos a diferentes riesgos, entre ellos, de lavado de dinero, fraude y seguridad de la información. Los documentos fraudulentos, numerados en secuencia o físicamente modificados, en especial los cheques de viajero y los giros postales, son más difíciles de detectar cuando se envían mediante la RDC y no son revisados por una persona calificada. Los bancos pueden enfrentar desafíos al tratar de controlar o conocer la ubicación del equipo de RDC, debido a que el equipo se puede trasportar rápidamente de una jurisdicción a otra. Este desafío aumenta en la medida en que cada vez más compañías de servicios en moneda extranjera y bancos corresponsales extranjeros usan los servicios de RDC para reemplazar las actividades de depósitos vía maletines/bolsos y ciertas actividades de procesamiento y compensación de instrumentos. Los controles inadecuados pueden derivar en alteraciones intencionales o accidentales de los datos del elemento de depósito, el reenvío de un archivo de datos o la presentación duplicada de cheques e imágenes en una o más instituciones financieras. Además, los elementos de depósito originales generalmente no son enviados a los bancos, sino que, por el contrario, quedan en poder del cliente o del prestador de servicios del cliente. En consecuencia, pueden aumentar los problemas de integridad, seguridad de los datos y gestión de registros.

Los clientes de riesgo más alto se pueden definir según la industria, la incidencia de fraude u otros criterios. Algunos ejemplos de partes de riesgo más alto incluyen los procesadores de pago en línea, ciertos servicios de reparación de crédito, ciertas compañías de solicitud de pedidos por vía telefónica o por correo, las operaciones de apuestas en línea, las empresas instaladas en el exterior y las empresas de entretenimiento para adultos.

Mitigación del riesgo

La gerencia debe desarrollar políticas, procedimientos y procesos adecuados para mitigar los riesgos asociados con los servicios de RDC y para supervisar actividades sospechosas o poco habituales de manera eficaz. Los ejemplos de medidas apropiadas para mitigar el riesgo incluyen:

- Identificar y analizar exhaustivamente el riesgo de RDC antes de su implementación. La alta gerencia debe identificar los riesgos de BSA/AML, operativos, de seguridad de la información, de cumplimiento, legales y aquellos que comprometen la reputación. Según el tamaño y la complejidad del banco, este proceso de análisis de riesgos integral debe incluir a miembros del personal de las áreas de BSA/AML, tecnología de la información y seguridad, operaciones de depósito, tesoro o administración del dinero resultante de las ventas al contado, continuidad empresarial, auditoría, cumplimiento, contabilidad y asuntos legales.

- Implementar adecuadamente la EDD y la CDD de los clientes.

- Crear parámetros basados en el riesgo que se puedan usar para realizar controles de la aptitud de la RDC para los clientes. Los parámetros pueden incluir una lista de industrias aceptables, criterios de colocación estandarizados (por ejemplo,

antecedentes de crédito, estados financieros, y estructura de propiedad comercial) y otros factores de riesgo (procesos de gestión de riesgos del cliente, ubicación geográfica y base de clientes). Cuando el nivel de riesgo lo justifique, el personal debe considerar realizar una visita a la ubicación física del cliente como parte del control de aptitud. Durantes estas visitas, deben evaluarse los controles operativos y los procesos de gestión de riesgos del cliente.

- Llevar a cabo la debida diligencia del proveedor cuando los bancos utilicen un prestador de servicios para las actividades de RDC. La gerencia debe garantizar la implementación de procesos de gestión de proveedores sólidos.

- Obtener la actividad de cuenta prevista del cliente de RDC, como el volumen de transacciones de RDC previsto, el volumen en dólares y el tipo (por ejemplo, cheques de nómina, cheques de terceros o cheques de viajero), compararla con la actividad real y corregir las desviaciones significativas. Comparar la actividad prevista con el tipo de actividad comercial a fin de asegurar que sea razonable y coherente.

- Establecer o modificar los límites de las transacciones mediante RDC para los clientes.

- Desarrollar contratos correctamente estructurados que identifiquen claramente el papel, las responsabilidades y las obligaciones de cada parte, y que detallen los procedimientos de conservación de registros para los datos de RDC. Estos procedimientos deben incluir las expectativas de seguridad física y lógica para el acceso, la transmisión, el almacenamiento y la eliminación definitiva de los documentos originales. El contrato también debe estipular la responsabilidad del cliente de asegurar adecuadamente el equipo de RDC y evitar su uso indebido, incluido el establecimiento de controles eficaces de seguridad del equipo (por ejemplo, contraseñas, acceso de doble control). Asimismo, los contratos deben incluir la obligación de los clientes de RDC de proporcionar los documentos originales al banco para facilitar las investigaciones relacionadas con las transacciones poco habituales o las transmisiones de mala calidad, o para resolver conflictos. Los contratos deben detallar claramente la autoridad del banco para implementar controles internos específicos, realizar auditorías o finalizar la relación de RDC.

- Implementar una supervisión o un control adicional cuando haya cambios significativos en el tipo o el volumen de las transacciones, o en los criterios de colocación, tipo de clientela, los procesos de gestión de riesgos de los clientes o la ubicación geográfica de los que el banco se haya valido cuando estableció los servicios de RDC.

- Asegurar que los clientes de RDC reciban la capacitación adecuada. Dicha capacitación debe incluir la documentación que cubra cuestiones como los procedimientos y las operaciones de rutina, la presentación duplicada y la resolución de problemas.

- Utilizar capacidad optima de supervisión y acumulación facilitadas por los datos digitalizados.

- Según corresponda, utilizar la tecnología para minimizar los errores (por ejemplo, el uso del franqueo para imprimir o identificar un depósito que está siendo procesado).[176]

[176] El franqueo involucra la impresión o el estampado de frases como "Procesado" o "Procesado electrónicamente" en el frente del cheque original. Este proceso se utiliza como un indicador de que el cheque impreso ya ha sido procesado electrónicamente y, en consecuencia, ya no debe depositarse físicamente.

Procedimientos de Inspección

Banca electrónica

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los clientes de banca electrónica (transacciones bancarias electrónicas), incluida la actividad de captura de depósitos remotos (RDC), y la capacidad de la gerencia para implementar sistemas de supervisión e informe eficaces.*

1. Revise las políticas, los procedimientos y los procesos relacionados con transacciones bancarias electrónicas, incluida la actividad de RDC según sea pertinente. Evalúe la aptitud de las políticas, los procedimientos y los procesos con relación con las actividades de transacciones bancarias electrónicas del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las actividades de transacciones bancarias electrónicas de riesgo más alto.

3. Determine si el sistema del banco para supervisar las transacciones bancarias electrónicas, incluyendo las actividades de RDC según sea pertinente, para detectar e informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de transacciones bancarias electrónicas, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de transacciones bancarias electrónicas. De la muestra seleccionada, lleve a cabo los siguientes procedimientos:

   - Revise la documentación de apertura de la cuenta, incluida la del CIP, la debida diligencia continua de los clientes y los antecedentes de transacciones.
   - Compare la actividad prevista con la actividad real.
   - Determine si la actividad es coherente con el tipo de negocio del cliente. Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos con respecto a la relacion asociada con transacciones bancarias electrónicas.

Transferencias de Fondos: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transferencias de fondos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe. Esta sección amplía la revisión principal de las exigencias normativas y legales de las transferencias de fondos para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

En los Estados Unidos, los sistemas de pago consisten en numerosos intermediarios financieros, empresas de servicios financieros y empresas no bancarias que generan, procesan y distribuyen pagos. La expansión nacional e internacional de la industria de operaciones bancarias y los servicios financieros no bancarios ha intensificado la importancia de las transferencias electrónicas de fondos, como las transferencias de fondos a través de sistemas de pago al por mayor. Más información sobre los tipos de sistemas de pago al por mayor está disponible en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[177]

Servicios de transferencia de fondos

La gran mayoría del valor de las transferencias o los pagos efectuados en dólares estadounidenses en los Estados Unidos se procesa en última instancia a través de sistemas de pago al por mayor, que por lo general manejan transacciones de mucho valor entre bancos. Los bancos realizan estas transferencias tanto a nombre propio como en beneficio de otros prestadores de servicios financieros y clientes del banco, ya sean corporaciones o particulares.

Los sistemas de transferencia al por menor relacionados facilitan las transacciones dado que incluyen cámaras de compensación automática (ACH); cajeros automáticos (ATM); sistemas de puntos de venta (POS); pago telefónico de cuentas; sistemas *home banking;* y tarjetas de crédito, de débito, y prepagadas. Los que inician la mayoría de estas transacciones al por menor son los clientes, en lugar de los bancos y las corporaciones. Estas transacciones individuales pueden entonces procesarse por lotes para formar transferencias al por mayor más grandes, que son el centro de interés en esta sección.

Los dos principales sistemas nacionales de pago al por mayor de transferencias de fondos interbancarias son los Servicios de fondos Fedwire (Fedwire®)[178] y el Sistema de pagos interbancarios por cámara de compensación (CHIPS).[179] La mayor parte del valor en dólares de estos pagos se origina electrónicamente para hacer pagos de alto valor en los

[177] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

[178] Fedwire® es una marca registrada de servicio de los Bancos de la Reserva Federal. Consulte www.frbservices.org/fedwire/index.html para obtener más información.

[179] CHIPS es un sistema privado de liquidación multilateral que pertenece y es operado por The Clearing House Payments Co., LLC.

que el tiempo es un factor clave, como liquidar compras interbancarias y vender fondos federales, liquidar transacciones de cambio de moneda extranjera, desembolsar o pagar préstamos, liquidar transacciones de bienes inmuebles u otras transacciones del mercado financiero; y la compra, venta o financiación de transacciones de valores. Las personas que utilizan Fedwire y CHIPS facilitan estas transacciones en su nombre y en nombre de sus clientes, incluyendo instituciones financieras no bancarias, empresas comerciales, y bancos corresponsales que no tienen acceso directo. Estructuralmente, hay dos componentes de las transferencias de fondos.

La estructura de las transferencias de fondos posee dos componentes: las instrucciones, que contienen información del remitente y el receptor de los fondos, y el movimiento o transferencia real de los fondos. Las instrucciones pueden enviarse por diferentes vías, por ejemplo accediendo electrónicamente a las redes operadas por los sistemas de pago Fedwire o CHIPS; accediendo a los sistemas de telecomunicaciones financieras, como la Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT); o por correo electrónico, fax, teléfono o télex. Se utilizan Fedwire y CHIPS para facilitar las transferencias en dólares estadounidenses entre dos extremos nacionales o de la porción en dólares estadounidenses de las transacciones internacionales. SWIFT es un servicio de mensajería internacional que se utiliza para transmitir las instrucciones de pago de la gran mayoría de transacciones internacionales interbancarias, que pueden estar denominadas en muchos tipos de moneda.

Fedwire

El sistema Fedwire es operado por los Bancos de la Reserva Federal y le permite a todo participante transferir fondos desde su cuenta principal en el Banco de la Reserva Federal a cualquier otra cuenta principal de cualquier otro banco.[180] El pago a través de Fedwire es definitivo e irrevocable cuando el Banco de la Reserva Federal acredita el monto de la orden de pago en la cuenta principal que el banco receptor tiene en el Banco de la Reserva Federal, o envía una notificación al banco receptor, según lo que ocurra primero. Aunque los participantes del sistema Fedwire no corren el riesgo de liquidación, pueden estar expuestos a otros riesgos, como errores, omisiones y fraude.

---

[180] Una entidad que cumple con los requisitos para mantener una cuenta principal en la Reserva Federal generalmente cumple con los requisitos para participar en el Servicio de Fondos Fedwire. Estos participantes incluyen:

- Instituciones de depósito.
- Agencias y sucursales estadounidenses de bancos extranjeros.
- Bancos miembros del Sistema de la Reserva Federal.
- El Tesoro de los EE. UU y cualquier entidad específicamente autorizada por ley federal para utilizar los Bancos de la Reserva Federal como agentes fiscales o de depósito.
- Entidades designadas por el Secretario del Tesoro.
- Los bancos centrales extranjeros, autoridades monetarias extranjeras, gobiernos extranjeros, y ciertas organizaciones internacionales.
- Cualquier otra entidad autorizada por el Banco de la Reserva Federal para utilizar el Servicio de Fondos Fedwire.

Los participantes pueden acceder al sistema Fedwire a través de los siguientes tres métodos:

- Interfaz directa de computador (sistema FedLine directo).
- Acceso a Internet a través de una red privada virtual a aplicaciones basadas en la Web (*FedLine Advantage*).
- Acceso autónomo o a través de una línea telefónica a un sitio de operaciones de un Banco de la Reserva Federal.

CHIPS

CHIPS es un sistema de pagos multilateral administrado por particulares que opera en tiempo real y que se utiliza generalmente para el pago de grandes montos en dólares. El sistema CHIPS es de propiedad de los bancos, y toda organización bancaria con presencia estadounidense regulada puede participar del sistema. Los bancos utilizan CHIPS para la liquidación tanto de transacciones interbancarias como de clientes, incluidos, por ejemplo, los pagos asociados con transacciones comerciales, los préstamos bancarios y las transacciones de valores. CHIPS también desempeña un papel importante en la liquidación de pagos en dólares relacionados con las transacciones internacionales, como el cambio de moneda extranjera, las transacciones comerciales internacionales y las inversiones en el extranjero.

Banco de liquidación vinculada continua (CLS)

El Banco de CLS es un banco con un propósito especial de sector privado que liquida de manera simultánea ambas obligaciones de pago que surgen de una sola transacción de cambio de moneda extranjera. El pago de CLS frente al modelo de la liquidación de pago garantiza que una parte del pago de una transacción de cambio de moneda extranjera se liquide si y sólo si la parte de pago correspondiente también se liquida, eliminando el riesgo de la liquidación de cambio de moneda extranjera que surge cuando cada parte de la transacción de moneda extranjera se liquida por separado. La CLS es propiedad de instituciones financieras mundiales a través de la posesión de acciones en CLS Group Holdings AG, una compañía suiza que es la sociedad de control final para el Banco de CLS. Actualmente, el Banco de CLS liquida instrucciones de pago para transacciones de cambio de moneda extranjera en 17 divisas y se espera que con el tiempo incluya más divisas.

SWIFT

La red SWIFT no es un sistema de pagos sino una infraestructura de mensajería, que proporciona a los usuarios un vínculo privado de comunicaciones internacionales entre ellos mismos. Los movimientos de fondos reales (pagos) se realizan a través de las relaciones bancarias corresponsales, Fedwire o CHIPS. El movimiento de los pagos denominados en monedas diferentes se produce mediante las relaciones bancarias corresponsales o los sistemas de transferencias de fondos existentes en el país pertinente. Además de las transferencias de fondos del banco y del cliente, se utiliza la SWIFT para transmitir confirmaciones de cambio de moneda extranjera, confirmaciones de ingresos de débitos y créditos, estados de cuenta, cobros y créditos documentados.

Pagos de cobertura

Una transferencia de fondos típica involucra a un remitente que le indica a su banco (el banco del remitente) que efectúe un pago en la cuenta de un beneficiario en el banco del beneficiario. Un pago de cobertura ocurre cuando el banco del remitente y el banco del beneficiario no tienen una relación que les permita realizar el pago directamente. En dicho caso, el banco del remitente le indica al banco del beneficiario que efectúe el pago y notifica que la transmisión de fondos para "cubrir" la obligación creada por la orden de pago se ha dispuesto a través de cuentas corresponsales a uno o más bancos intermediarios.

Los pagos de cobertura transnacionales generalmente involucran varios bancos en diversas jurisdicciones. Por lo general, para las transacciones en dólares estadounidenses, los bancos intermediarios son bancos estadounidenses que mantienen relaciones de banca corresponsal con los bancos no estadounidenses de los remitentes y los beneficiarios. En el pasado, los protocolos de mensaje de SWIFT permitían que los pagos de cobertura transnacionales se realizaran mediante el uso de formatos de mensaje simultáneos e independientes:

- el MT 103: orden de pago del banco del remitente al banco del beneficiario con información identificativa del remitente y el beneficiario; y
- el MT 202: órdenes de pago de banco a banco mediante las que se indica a los bancos intermediarios que "cubran" la obligación de pago del banco del remitente al banco del beneficiario.

A fin de evitar la falta de transparencia, SWIFT adoptó un nuevo formato de mensaje para los pagos de cobertura (el MT 202 COV) que contiene campos obligatorios para rellenar con información del remitente y el beneficiario. Vigente desde el 21 de Noviembre de 2009, el MT 202 COV es obligatorio para todo pago de banco a banco que tenga asociado un MT 103. El MT 202 COV proporciona a los bancos intermediarios información adicional sobre el remitente y el beneficiario para ejecutar la revisión de sanciones y la supervisión de las actividades sospechosas.[181] La incorporación del MT 202 COV no altera las obligaciones de OFAC o BSA/AML de un banco estadounidense.

El formato MT 202 sigue estando disponible para las transferencias de fondos de banco a banco que no tengan un mensaje MT 103 asociado. Si desea obtener información adicional sobre la transparencia en los pagos de cobertura, consulte *Transparency and Compliance for U.S. Banking Organizations Conducting Cross-Border Funds Transfers* (Transparencia y cumplimiento de las organizaciones bancarias estadounidenses que realizan transferencias de fondos transnacionales), del 18 de Diciembre de 2009, disponible en el sitio web de las agencias bancarias federales.

---

[181] En el sitio web de SWIFT, www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2009/Newstandardsforcoverpayments.page, se puede encontrar información adicional sobre los detalles del formato MT 202 COV

Sistemas informales de transferencia de valor

Por sistema informal de transferencia de valor (IVTS, por sus siglas en inglés) (por ejemplo, los hawalas) se entiende el sistema de transferencia de moneda o valor que opera informalmente para transferir dinero como negocio.[182] En los países que carecen de un sector financiero estable o que tienen grandes áreas no atendidas por bancos formales, el sistema IVTS puede ser el único método para realizar transacciones financieras. Las personas que viven en los Estados Unidos también pueden utilizar IVTS para transferir fondos hacia sus países de origen.

Transacciones pagaderas mediante presentación de identificación apropiada

Un tipo de transacción de transferencia de fondos que implica un riesgo particular es el servicio de transacciones pagaderas mediante presentación de identificación apropiada (PUPID). Las transacciones PUPID son transferencias de fondos en las que no existe una cuenta específica para depositar los fondos y el beneficiario de los fondos no es cliente del banco. Por ejemplo, una persona física puede transferir fondos a un familiar o a una persona que no tenga una relación de cuenta con el banco que recibe la transferencia de fondos. En este caso, el banco beneficiario puede colocar los fondos que ingresan en una cuenta puente o de tránsito y, en última instancia, liberar los fondos cuando la persona presente pruebas respecto a su identidad. En algunos casos, los bancos autorizan a entidades que no son clientes a iniciar transacciones PUPID. Estas transacciones se consideran de un riesgo extremadamente alto y requieren controles estrictos.

Factores de riesgo

Las transferencias de fondos pueden presentar un aumento en el grado de riesgo, que depende de factores como la cantidad y volumen en dólares de las transacciones, la ubicación geográfica de remitentes y beneficiarios, y de si el remitente o el beneficiario es cliente del banco. El tamaño y la complejidad de la operación de un banco, y el origen y el destino de los fondos que están siendo transferidos determinarán qué tipo de sistema de transferencia de fondos utilizará el banco. La gran mayoría de las instrucciones de

[182] Las fuentes de información sobre IVTS incluyen:

- Asesoría 33 de la FinCEN, *Informal Value Transfer Systems* (Sistemas Informales de Transferencia de Valor), de Marzo de 2003.
- *Informal Value Transfer Systems Report to the Congress in Accordance with Section 359 of the Patriot Act* (Informe al Congreso de los sistemas informales de transferencia de valores del Tesoro de los Estados Unidos según la Sección 359 de la Ley *Patriot*), de Noviembre 2002.
- Grupo de Acción Financiera en Contra del Lavado de Dinero (FATF), *Interpretative Note to Special Recommendation VI: Alternative Remittance* (Nota interpretativa a la Recomendación Especial VI: Remesas alternativas), de Junio de 2003.
- FATF, *Combating the Abuse of Alternative Remittance Systems, International Best Practices* (Lucha contra el abuso de los sistemas de remesas alternativas, Mejores prácticas internacionales), de Octubre de 2002.

transferencia de fondos se envía electrónicamente; sin embargo, los inspectores deben ser conscientes de que las instrucciones físicas se pueden transmitir por otras vías informales, como las descritas anteriormente.

Los pagos de cobertura realizados a través de SWIFT plantean un riesgo adicional para cualquier banco intermediario que no reciba un MT 103 o un MT 202 COV correctamente completo, en el que se identifique el remitente y el beneficiario de la transferencia de fondos. Sin estos datos, el banco intermediario no puede supervisar o filtrar la información de pago. Esta falta de transparencia limita la capacidad del banco intermediario estadounidense para analizar y gestionar adecuadamente el riesgo asociado con las operaciones de compensación y cuentas corresponsales, supervisar las actividades sospechosas y corroborar el cumplimiento con la OFAC.

Los IVTS plantean un problema serio porque pueden burlar el sistema formal. La ausencia de exigencias de gestión de registros junto a la falta de identificación de quienes participan en el sistema IVTS puede atraer a lavadores de dinero y terroristas. Los IVTS también pueden implicar mayor riesgo BSA/AML porque permiten evadir los controles internos y la supervisión establecidos en el entorno bancario formal. Los mandantes que operan sistemas IVTS con frecuencia utilizan los bancos para liquidar cuentas.

Los riesgos que implican las transacciones PUPID para los bancos beneficiarios son similares a los de otras actividades en las que los bancos hacen negocios con quienes no son clientes. Sin embargo, los riesgos son mayores en las transacciones PUPID si el banco permite que una persona que no es cliente acceda al sistema de transferencias de fondos proporcionando mínima o ninguna información de identidad. Los bancos que permiten a quienes no son clientes transferir fondos utilizando el servicio PUPID ponen en riesgo significativo tanto al banco beneficiario como al banco en donde se originó la transferencia. En estas situaciones, los dos bancos tienen mínima información sobre la identidad tanto del remitente como del beneficiario o carecen de ella por completo.

Mitigación del riesgo

Las transferencias de fondos se pueden utilizar en las fases de colocación, transformación e integración del lavado de dinero. Las transferencias de fondos compradas con moneda son un ejemplo de la etapa de colocación. Es más difícil para los bancos detectar actividad poco habitual en las etapas de transformación e integración porque las transacciones pueden parecer legítimas. En muchos casos, los bancos no participan en la colocación de los fondos o en la integración final, sino únicamente en la transformación de las transacciones. Los bancos deben tener en cuenta las tres fases del lavado de dinero cuando evalúan o analizan los riesgos de la transferencia de fondos.

Los bancos necesitan establecer políticas, procedimientos y procesos responsables para gestionar los riesgos BSA/AML que presentan sus actividades de transferencia de fondos. Dichas políticas pueden incluir más que exigencias normativas mínimas en cuanto a la gestión de registros y expandirse para cubrir la OFAC. Las políticas, los procedimientos y los procesos de las transferencias de fondos deben ocuparse de todas las actividades de bancos corresponsales extranjeros, incluidas las transacciones en las que las sucursales y agencias estadounidenses de bancos extranjeros sean intermediarias para sus oficinas centrales.

La obtención de información de CDD es importante para mitigar el riesgo en la prestación de servicios de transferencia de fondos. Debido al carácter de las transferencias de fondos, es fundamental contar con políticas, procedimientos y procesos CDD eficaces y adecuados para detectar actividades sospechosas y poco habituales. Es igualmente importante disponer de un sistema de informe y supervisión de actividades sospechosas eficaz en función del riesgo. Tanto si este sistema de informe y supervisión es automatizado como si es manual, debe ser suficiente para detectar patrones y tendencias sospechosos que por lo general se asocian con el lavado de dinero.

Las instituciones deben tener procesos para gestionar las relaciones de banca corresponsal de acuerdo con la sección 312 de la Ley PATRIOTA de EE. UU. y los reglamentos pertinentes (31 CFR 103.176). La debida diligencia de la banca corresponsal debe tener en cuenta las prácticas del banco corresponsal con relación a la transferencia de fondos a través del banco estadounidense.

Los bancos estadounidenses pueden mitigar el riesgo asociado con los pagos de cobertura al gestionar relaciones de banca corresponsal, al cumplir con las mejores prácticas de The Clearing House Payments Co., LLC y el Grupo Wolfsberg (tema desarrollado a continuación) y las normas de SWIFT para el envío de mensajes, y al realizar la correcta revisión y supervisión de las transacciones.

En Mayo de 2009, el Comité de Supervisión Bancaria de Basilea publicó un documento sobre los mensajes de pagos cobertura de transnacionales (Documento sobre los pagos de cobertura del BIS).[183] El Documento sobre los pagos de cobertura del BIS admitía el aumento de la transparencia y recomendaba a todos los bancos involucrados en las transacciones de pagos internacionales que cumplieran con las normas de mensajes desarrolladas por The Clearing House Payments Co., LLC y el Grupo Wolfsberg en 2007. Estas son:

- Las instituciones bancarias no deben omitir, eliminar o alterar la información en las órdenes o los mensajes de pago con el fin de evitar la detección de dicha información por parte de cualquier otra institución financiera en el proceso de pago.
- Las instituciones financieras no deben utilizar los mensajes de pago particulares con el fin de evitar la detección de información por parte de cualquier otra institución en el proceso de pago.
- Sujeto a todas las leyes pertinentes, las instituciones financieras deben cooperar tanto como sea viable con otras instituciones financieras en el proceso de pago cuando se les solicite que proporcionen información acerca de las partes involucradas.

[183] Comité de Supervisión Bancaria de Basilea, *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers* (Debida diligencia y transparencia relacionadas con los mensajes de pagos de cobertura correspondientes a las transferencias electrónicas transnacionales, disponibles en www.bis.org/publ/bcbs154.htm. Además, durante el mes de Agosto de 2009, el comité, junto con The Clearing House Payments Co., LLC, publicó preguntas y respuestas con el objeto de aumentar la comprensión de MT 202 COV.

- Las instituciones financieras deben recomendar enfáticamente a sus bancos corresponsales que respeten estos principios.

Asimismo, los procesos eficaces de supervisión de los pagos de cobertura incluyen:

- La supervisión de las transferencias de fondos procesadas mediante sistemas automatizados con el fin de identificar actividades sospechosas. Esta supervisión puede realizarse después del procesamiento de las transferencias, en forma automatizada, y se puede utilizar un enfoque basado en el riesgo. El MT 202 COV proporciona a los bancos intermediarios información útil, que se puede filtrar usando los factores de riesgo desarrollados por el banco intermediario. El proceso de supervisión puede ser similar al de los pagos mediante MT 103.

- Dado el volumen de los mensajes y la información de los grandes bancos intermediarios estadounidenses, es posible que el control manual de cada orden de pago no sea factible o eficaz. Sin embargo, los bancos intermediarios deben tener, como parte de sus procesos de supervisión, un método basado en el riesgo para identificar los campos incompletos o los campos con información sin sentido. Los bancos estadounidenses que participan en el procesamiento de pagos de cobertura deben tener políticas para abordar tales circunstancias, incluidas aquellas que involucran sistemas distintos de SWIFT.

Los bancos remitentes y beneficiarios deben establecer políticas, procedimientos y procesos adecuados para las actividades PUPID que incluyan:

- Especificación del tipo de identificación que se considera aceptable.

- Mantener documentación de personas físicas que sea consistente con las políticas de conservación de registros del banco.

- Delimitación de los empleados del banco que pueden realizar transacciones PUPID.

- Fijación de límites en la cantidad de fondos que pueden ser transferidos desde y hacia los bancos para quienes no son clientes (incluyendo el tipo de fondos que se acepta (es decir, moneda o cheque oficial) de parte del banco remitente.

- Supervisión e informe de actividades sospechosas.

- Escrutinio especial para transferencias realizadas desde y hacia ciertas jurisdicciones.

- Identificación de los métodos de desembolso (es decir, en moneda o cheque oficial) de los fondos provenientes de un banco beneficiario.

Procedimientos de Inspección

Transferencias de fondos

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transferencias de fondos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe. Esta sección amplía la revisión principal de las exigencias normativas y legales de las transferencias de fondos para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las transferencias de fondos. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de transferencias de fondos del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las actividades de transferencias de fondos.

3. Evalúe los riesgos del banco relacionados con las actividades de transferencias de fondos al analizar la frecuencia y el volumen en dólares de las transferencias de fondos, las jurisdicciones y el papel del banco en el proceso de transferencia de fondos (por ejemplo, si es el banco del remitente, del intermediario o del beneficiario). Estos factores deben evaluarse con relación al tamaño del banco, su ubicación y la naturaleza de las relaciones de las cuentas corresponsales y los clientes.

4. Determine si existe un rastro de auditoría respecto a las actividades de transferencias de fondos. Determine si se dispone de una división de responsabilidades u otros controles compensatorios adecuados para garantizar la autorización adecuada para enviar y recibir transferencias de fondos, y corregir las imputaciones a cuentas.

5. Determine si el sistema del banco para supervisar las transferencias de fondos e informar sobre las actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco. Determine si los sistemas de supervisión e informe de actividades sospechosas incluyen:

   - Transferencias de fondos adquiridas con dinero en efectivo.
   - Transacciones en las que el banco actúe como intermediario.
   - Todos los formatos de mensaje de SWIFT, incluidos MT 103, MT 202 y MT 202 COV.
   - Transacciones en las que el banco remite o recibe transferencias de fondos de instituciones financieras extranjeras, particularmente desde o hacia jurisdicciones con leyes de secreto y privacidad estrictas, o aquellas identificadas como de riesgo más alto.

- Depósitos de dinero en efectivo frecuentes o transferencias de fondos y las transferencias posteriores, particularmente a una institución más grande o fuera del país.

6. Revise los procedimientos del banco para realizar las transferencias de fondos transnacionales:

   - Determine si los procesos del banco para la debida diligencia de bancos corresponsales extranjeros, según se estipula en la sección 312 de la Ley PATRIOTA de EE. UU. y los reglamentos pertinentes, incluyen la revisión y la evaluación de las prácticas de transparencia de los corresponsales del banco involucrados en las transferencias de fondos transnacionales a través del banco (por ejemplo, si los corresponsales están utilizando correctamente el formato de mensaje MT 202 COV).

   - Según corresponda y en tanto no se haya hecho hasta el momento, revise los procedimientos del banco para garantizar el cumplimiento de la *Travel Rule*, incluido el uso adecuado del formato MT 202 COV.

   - Evalúe las políticas del banco para cooperar con sus corresponsales cuando estos le soliciten al banco que proporcione información acerca de las partes involucradas en las transferencias de fondos.

   - Evalúe la aptitud de los procedimientos del banco para abordar las instancias aisladas y reiteradas donde la información de pago proporcionada por un corresponsal falta, claramente carece de sentido, está incompleta o es sospechosa.

7. Determine los procedimientos del banco para transacciones pagaderas mediante presentación de identificación apropiada (PUPID).

   - Banco beneficiario: determine cómo desembolsa el banco los ingresos (es decir, mediante dinero en efectivo o cheque oficial).

   - Banco remitente: determine si el banco admite las transferencias de fondos PUPID a quienes no son clientes. De ser así, determine el tipo de fondos aceptados (es decir, en dinero en efectivo o cheque oficial).

8. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

9. En función del análisis de riesgos del banco de sus actividades de transferencias de fondos, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de actividades de transferencias de fondos de riesgo más alto, que pueden incluir lo siguiente:

   - Transferencias de fondos adquiridas con dinero en efectivo.

- Transacciones en las que el banco actúe como intermediario, como los pagos de cobertura.
- Transacciones en las que el banco remite o recibe transferencias de fondos de instituciones financieras extranjeras, particularmente desde o hacia jurisdicciones con leyes de secreto y privacidad estrictas, o aquellas identificadas como de riesgo más alto.
- Transacciones PUPID.

10. De la muestra seleccionada, analice las transferencias de fondos para determinar si las cantidades, la frecuencia y las jurisdicciones de origen o destino son coherentes con el tipo de negocio u ocupación del cliente.
11. Además, para las transferencias de fondos procesadas con los formatos de mensaje MT 202 y MT 202 COV, revise la muestra de mensajes para determinar si el banco ha utilizado los formatos de mensaje correctos y ha incluido toda la información del remitente y el beneficiario (por ejemplo, no falta información ni se incluyó información sin sentido).
12. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las actividades de transferencias de fondos.

Transacciones de Compensación Automatizada: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con la compensación automatizada (ACH) y las transacciones ACH internacionales (IAT), y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

El uso de ACH ha aumentado notablemente en los últimos años debido al gran volumen de conversiones electrónicas de cheques[184] y débitos únicos en ACH, lo que refleja el bajo costo del procesamiento en ACH respecto al procesamiento de cheques.[185] Las transacciones de conversión de cheques, como los débitos únicos en ACH, generalmente involucran transacciones de particulares de poco valor en dólares para la adquisición de bienes y servicios o el pago de facturas de consumidores. ACH se utiliza principalmente para los pagos nacionales, pero el sistema FedGlobal[186] de los Bancos de la Reserva Federal actualmente admite los pagos transnacionales a muchos países del mundo.

En Septiembre de 2006, la Oficina del Interventor Monetario expidió una guía con el título *Automated Clearinghouse Activities — Risk Management Guidance* (Actividades de compensación automatizada: guía sobre gestión de riesgos). El documento proporciona una guía para gestionar los riesgos de la actividad de ACH. Los bancos pueden estar expuestos a una variedad de riesgos cuando originan, reciben o procesan transacciones de ACH o subcontratan un servicio externo para que realice estas actividades.[187]

Sistema de pagos ACH

Tradicionalmente, el sistema ACH se ha utilizado para el depósito directo de nómina y pagos de beneficios gubernamentales, y para el pago directo de hipotecas y préstamos. Como se indicó anteriormente, ACH se está expandiendo hasta incluir los débitos únicos

[184] En el proceso de conversión electrónica de cheques, los intermediarios que reciben un cheque para pago no cobran el cheque a través del sistema de cobro de cheques, ya sea electrónicamente o en papel. En cambio, los intermediarios utilizan la información del cheque para iniciar un tipo transferencia de fondos electrónica conocida como débito ACH de la cuenta del individuo que libra el cheque. El cheque se utiliza para obtener el número ABA del banco, número de cuenta, número de serie del cheque y suma en dólares de la transacción, pero el cheque en sí mismo no se envía a través del sistema de cobro de cheques en ninguna forma como instrumento de pago. Los intermediarios utilizan la conversión electrónica de cheques porque puede resultar una forma más eficaz de obtener los pagos que cobrando el cheque.

[185] Consulte www.nacha.org.

[186] Los Bancos de la Reserva Federal operan el FedACH, una institución de compensación central para transmitir y recibir pagos ACH, y FedGlobal, que envía pagos de créditos ACH transnacionales a más de 35 países del mundo y pagos de débito solamente a Canadá.

[187] Consulte el boletín de la OCC 2006-39 del 1.º de Septiembre de 2006) en www.occ.gov/ftp/bulletin/2006-39.pdf.

y la conversión de cheques. Las transacciones de ACH constituyen instrucciones de pago para acreditar o debitar de una cuenta de depósito. Los ejemplos de transacciones de pago con crédito incluyen los depósitos directos de nómina, Seguro Social, dividendos y pagos de intereses. Los ejemplos de transacciones con débito incluyen los pagos de hipoteca, préstamos, primas de seguro y una variedad de pagos de particulares iniciados a través de intermediarios (en inglés, *merchants*) o comercios.

Generalmente, una transacción de ACH es una transferencia de fondos electrónica procesada por lotes y con fecha efectiva entre un banco remitente y uno receptor. A una transacción de crédito ACH la origina el titular de cuenta que envía los fondos (pagador); en cambio, a una transacción de débito ACH la origina el titular de cuenta que recibe los fondos (beneficiario). Dentro del sistema ACH, estos participantes y usuarios se conocen con los siguientes términos:

- **Remitente.** Una organización o persona que inicia una transacción de ACH en una cuenta como un débito o un crédito.

- **Institución Financiera de Depósito de Origen (ODFI).** La institución financiera de depósito del remitente que envía la transacción de ACH a la red ACH nacional a través de un operador ACH.

- **Operador ACH.** Un operador ACH procesa todas las transacciones de ACH que fluyen entre las diferentes instituciones financieras de depósito. Un operador ACH sirve de institución de compensación central que recibe entradas de las ODFI y las distribuye a la Institución Financiera de Depósito Receptora correspondiente. Actualmente existen dos operadores ACH: Red de pago electrónico (EPN) y FedACH.

- **Institución Financiera de Depósito Receptora (RDFI).** La institución de depósito del Receptor que recibe la transacción de ACH de los operadores ACH y fondos de crédito o débito de las cuentas de los receptores.

- **Receptor.** Una organización o persona que autoriza al remitente a iniciar una transacción de ACH, ya sea como débito o crédito a una cuenta.

- **Operador de puerta de enlace (GO).** Una institución financiera, un operador ACH o una ODFI que actúa como un punto de entrada o de salida hacia o desde los Estados Unidos. Como operador de puerta de enlace, no se requiere una declaración formal de estado. Los operadores ACH y las ODFI que actúan como operadores de puerta de enlace tienen garantías y obligaciones específicas relacionadas con determinadas entradas internacionales. Una institución financiera que actúa como un operador de puerta de enlace generalmente puede procesar transacciones de débito y crédito de entrada y de salida. Los operadores ACH que actúan como operadores de puerta de enlace pueden procesar asientos de crédito y débito de salida, pero pueden limitar los asientos de entrada a asientos de crédito solamente y contraasientos.

Pagos ACH internacionales

NACHA: La Asociación de Pagos Electrónicos estableció formatos y normas operativas sobre las transacciones ACH internacionales (IAT) que entraron en vigencia el 18 de Septiembre de 2009.[188] IAT es un nuevo código de clase de entrada estándar para los pagos ACH que habilita a las instituciones financieras a identificar y supervisar los pagos ACH internacionales, y a realizar una revisión conforme a la OFAC. Las normas requieren que los operadores de puerta de enlace clasifiquen los pagos que son transmitidos a una agencia financiera[189] fuera de la jurisdicción territorial de los Estados Unidos, o bien que son recibidos desde la agencia, como IAT. La clasificación dependerá de la ubicación de la agencia financiera que administra la transacción de pago (movimiento de fondos) y no de la ubicación de cualquier otra parte de la transacción (por ejemplo, el remitente o el receptor).

De conformidad con las normas operativas de la NACHA, todas las instituciones financieras estadounidenses que participan en la red ACH deben poder utilizar el formato IAT.

Definición de IAT

Una IAT es una entrada ACH que es parte de una transacción de pago que involucra una oficina de una agencia financiera que no está ubicada en la jurisdicción territorial de los Estados Unidos. Una oficina de una agencia financiera está involucrada en una transacción de pago si se cumplen una o más de las siguientes condiciones:

- Tiene una cuenta que se acredita o debita como parte de la transacción de pago.
- Recibe fondos directamente de una persona o realiza pagos directamente a una persona como parte de una transacción de pago.
- Sirve de intermediaria en la liquidación de cualquier parte de una transacción de pago.

Términos relacionados con IAT

Un “asiento de entrada” se origina en otro país y se transmite a los Estados Unidos. Por ejemplo, un asiento de entrada puede ser la obtención de fondos para la nómina de una empresa. Cada IAT subsiguiente que se utilice para el depósito directo sería un asiento de IAT de entrada.

Un “asiento de salida” se origina en los Estados Unidos y se transmite a otro país. Por ejemplo, los pagos de jubilación de IAT de una ODFI estadounidense a una RDFI

[188] Si desea información adicional sobre las IAT, consulte www.nacha.org/c/IATIndustryInformation.cfm.

[189] “Agencia financiera” es una entidad que, según la ley aplicable, tiene autorización para aceptar depósitos o está en el negocio de realizar giros postales o transferencias de fondos.

estadounidense en la que los fondos luego se transfieren a una cuenta en otro país serían asientos de IAT de salida.

Guía de transacción de pago

Una transacción de pago es:

- la instrucción de un remitente a un banco de pagar, o de obtener el pago de, o de que otro banco pague u obtenga el pago de, una suma de dinero fija o determinada que se pagará a un receptor, o que se obtendrá de este; y
- todos y cada una de las liquidaciones, asientos contables o desembolsos que sean necesarios o adecuados para llevar a cabo la instrucción.

Identificación de las partes de IAT

Las normas operativas de la NACHA definen nuevas partes como parte de un asiento de IAT:

- Banco corresponsal extranjero: Una institución financiera de depósito participante (DFI) que retiene depósitos que son propiedad de otras instituciones financieras, y que proporciona pagos y otros servicios a dichas instituciones.
- Operador de puerta de enlace extranjera (FGO): Un operador de puerta de enlace que actúa como un punto de entrada o de salida desde un país extranjero.

Información adicional

El nuevo formato de IAT aumenta la cantidad de información del remitente y el beneficiario a la que los bancos tendrán acceso. Dicha información puede ser de utilidad en sus esfuerzos de supervisión, de prevención de lavado de dinero y OFAC.[190] Algunos ejemplos de la información que actualmente está a disposición de los bancos con el nuevo formato de IAT incluyen:

- Nombre y dirección del remitente.
- Nombre y dirección del receptor.
- Números de cuenta del remitente y el receptor.
- Nombre de la ODFI (IAT de entrada, DFI extranjera), número de identificación y código de país de la sucursal.

---

[190] Por conveniencia, esta información a menudo se denomina información "*Travel Rule*", pero por cuestiones técnicas las reglas de transmisión y gestión de registros de transferencias de fondos de 31 CFR 103.33(g) no se aplican a las transacciones ACH, y las reglas operativas de NACHA no han cambiado.

- Nombre de la RDFI (IAT de salida, DFI extranjera), número de identificación y código de país de la sucursal.
- Código de país.
- Código de divisa.
- Indicador de cambio de moneda extranjera.

Consulte www.nacha.org para obtener más información sobre los datos adicionales a disposición de los bancos con el nuevo formato de IAT.

Prestadores de servicios externos

Un prestador de servicios externo (TPSP) es una entidad distinta a un remitente, ODFI o RDFI que lleva a cabo cualquier función en nombre del remitente, la ODFI o la RDFI con respecto al procesamiento de entradas ACH.[191] Las normas operativas de la NACHA definen los TPSP y los subconjuntos relevantes de TPSP que incluyen "remitentes externos" y "puntos de envío".[192] Las funciones de estos TPSP pueden incluir, entre otras, la creación de archivos ACH en nombre del remitente o la ODFI, o actuando como punto de envío de una ODFI (o punto de recepción en nombre de una RDFI).

Factores de riesgo

El sistema ACH fue diseñado para transferir un gran volumen de transacciones de poco valor en dólares, que plantean riesgos BSA/AML menores. No obstante, la capacidad de enviar transacciones internacionales y de mayor valor en dólares a través de ACH puede exponer a los bancos a mayores riesgos BSA/AML. Los bancos sin un sistema de supervisión BSA/AML sólido pueden estar expuestos a riesgos adicionales particularmente cuando las cuentas se abren en Internet sin contacto directo.

Las transacciones ACH que se originan a través de TPSP (es decir, cuando el remitente no es un cliente directo de la ODFI) pueden incrementar los riesgos BSA/AML, dificultando por lo tanto la tarea de la ODFI de evaluar los riesgos y controlar las transacciones del remitente para verificar el cumplimiento con las normas BSA/AML.[193]

---

[191] Un prestador de servicios externo es un término genérico que abarca a cualquier negocio que preste servicios a un banco. Un procesador de pagos externo es un tipo específico de prestador de servicios que procesa los pagos como cheques, archivos ACH, o archivos o mensajes de tarjetas de crédito y débito. Consulte la sección del esquema general ampliado, "Procesadores de pagos externos", en las páginas 265 a 268, como guía.

[192] Cuando los TPSP independientes celebran un contrato con organizaciones de ventas independientes u otros procesadores de pagos externos, puede haber dos o más niveles entre la ODFI y el Remitente.

[193] La política de colocación de un banco debe definir qué información debe contener cada aplicación. La exhaustividad del control de la aplicación de un remitente debe coincidir con el nivel de riesgo planteado por él. La política de colocación debe exigir una verificación de antecedentes de cada remitente para respaldar la validez del negocio.

Los riesgos se incrementan cuando ni el TPSP ni el ODFI aplican debida diligencia a las compañías para las que están originando pagos.

Ciertas transacciones ACH, como las originadas a través de Internet o por teléfono, pueden ser susceptibles a la manipulación y el uso fraudulento. Ciertas prácticas asociadas con la manera en que la industria bancaria procesa las transacciones ACH pueden exponer a los bancos a riesgos BSA/AML. Estas prácticas incluyen:

- Una ODFI que autoriza a un TPSP a enviar archivos ACH directamente a un Operador ACH, esencialmente eludiendo la ODFI.
- Las ODFI y RDFI que dependen una de la otra para aplicar la debida diligencia adecuada a sus clientes.
- El procesamiento por lotes que permite ocultar la identidad de los remitentes.
- La imposibilidad de compartir información acerca de los remitentes y los receptores inhibe la capacidad de un banco para analizar y gestionar adecuadamente el riesgo asociado con las operaciones de procesamiento de ACH y cuentas corresponsales, supervisar las actividades sospechosas y corroborar el cumplimiento con la OFAC.

Mitigación del riesgo

La BSA exige a los bancos que dispongan de programas de cumplimiento BSA/AML y de políticas, procedimientos y procesos adecuados para supervisar e identificar actividades poco habituales, incluidas las transacciones ACH. La obtención de CDD en todas las operaciones es importante para mitigar el riesgo BSA/AML de las transacciones ACH. Debido al carácter de las transacciones ACH y la dependencia mutua de las ODFI y RDFI para realizar los controles OFAC y obtener otra información de debida diligencia necesaria, es esencial que todas las partes cuenten con un programa de CDD firme para los clientes ACH habituales. En las relaciones con TPSP, la CDD de los TPSP se puede complementar con debida diligencia de los mandantes asociados con el TPSP y, según sea necesario, de los remitentes. Las políticas, los procedimientos y los procesos de CDD adecuados son fundamentales para detectar un patrón de actividades sospechosas o poco habituales debido a que las transacciones ACH individuales generalmente no se controlan. Es igualmente importante contar con un sistema de informe y supervisión de actividades sospechosas eficaz en función del riesgo. En los casos en que un banco dependa en exceso del TPSP, es posible que el banco desee controlar el programa de informe y supervisión de actividades sospechosas del TPSP, ya sea a través de una inspección independiente o por su cuenta. La ODFI puede establecer un acuerdo con el TPSP, que defina pautas generales de TPSP, como el cumplimiento con las exigencias operativas y responsabilidades ACH, y otros reglamentos federales y estatales vigentes. Es posible que los bancos tengan que considerar la implementación de controles que restrinjan o nieguen los servicios ACH a remitentes y receptores potenciales que participen en prácticas comerciales cuestionables o engañosas.

Las transacciones ACH se pueden utilizar en las fases de transformación e integración del lavado de dinero. La detección de actividad poco habitual en las fases de transformación

e integración puede resultar una tarea dificultosa, ya que se puede utilizar ACH para legitimar las transacciones frecuentes y periódicas. Los bancos deben tener en cuenta las fases de transformación e integración del lavado de dinero cuando evalúen o analicen los riesgos de las transacciones ACH de un cliente en particular.

La ODFI debe estar al tanto de la actividad de las IAT y debe evaluarla usando un enfoque basado en el riesgo para asegurar la identificación y la supervisión de cualquier actividad sospechosa. La ODFI, si participa frecuentemente en las IAT, puede desarrollar un proceso separado para controlar las IAT que minimice la interrupción del procesamiento, la conciliación y la liquidación ACH; dicho proceso se puede automatizar.

Las políticas, los procedimientos y los procesos relacionados con ACH del banco deben contemplar el posible riesgo más alto inherente en las IAT. El banco debe considerar sus funciones y sus responsabilidades actuales y potenciales al desarrollar los controles internos para supervisar y mitigar el riesgo asociado con las IAT y para cumplir con las exigencias de gestión de registros de actividades sospechosas del banco.

En el procesamiento de las IAT, el banco debe considerar lo siguiente:

- El volumen y los tipos de transacciones y clientes.
- Las relaciones asociadas con los procesadores de pagos externos.
- Las responsabilidades, las obligaciones y los riesgos de convertirse en un GO.
- Las normas y las prácticas de CIP, CDD y EDD.
- El informe y la supervisión de actividades sospechosas.
- Los MIS adecuados, incluida la posible necesidad de realizar actualizaciones y cambios en los sistemas.
- Los procedimientos de procesamiento (por ejemplo, la identificación y la gestión de las IAT, la resolución de positivos de OFAC, y la gestión de los mensajes rechazados y que no cumplen con lo estipulado).
- Los programas de capacitación para el personal adecuado del banco (por ejemplo, el personal de ACH, operaciones, auditorías de cumplimiento, atención al cliente, etc.).
- Los acuerdos legales, incluyendo aquellos con clientes, procesadores externos y proveedores, y si dichos acuerdos deben ser actualizados o modificados.

Evaluación de la OFAC

Todas las partes involucradas en una transacción ACH están sujetas a las exigencias de la OFAC. (Consulte la sección del esquema general principal, “Oficina de control de activos extranjeros”, en las páginas 165 a 175, como guía). La OFAC ha aclarado la

aplicación de sus normas a las transacciones ACH nacionales y transnacionales, y proporcionó una guía más detallada sobre transacciones ACH internacionales.[194]

Con respecto a las transacciones ACH nacionales, la ODFI es responsable de verificar que el Remitente no sea una parte bloqueada y de esforzarse de buena fe por confirmar que éste no esté transmitiendo fondos bloqueados. Del mismo modo, la RDFI es responsable de verificar que el Receptor no sea una parte bloqueada. De este modo, la ODFI y la RDFI dependen mutuamente la una de la otra para cumplir con los reglamentos de la OFAC.

Si una ODFI recibe transacciones ACH nacionales que su cliente ya ha procesado por lotes, la ODFI no es responsable de anular este procesamiento por lotes para asegurarse de que ninguna transacción viole los reglamentos de la OFAC. Si una ODFI anula el procesamiento por lotes de un archivo recibido del Remitente para procesar transacciones *on-us*, tal ODFI es responsable de que las transacciones *on-us* cumplan con la OFAC, debido a que en este caso estará actuando como la ODFI y la RDFI en dichas transacciones. Las ODFI, actuando en esta calidad, deben conocer a sus clientes con anterioridad a los efectos de la OFAC y otras exigencias normativas. En relación con las transacciones residuales del archivo no procesadas por lotes que sean *on-us*, y a otras situaciones en las que los bancos manejen registros de ACH no procesados por lotes por motivos que no sean para desglosar las transacciones *on-us*, los bancos deben determinar el nivel de riesgo OFAC y desarrollar políticas, procedimientos y procesos adecuados para tratar los riesgos asociados. Dichas políticas atenuantes pueden implicar la revisión de cada registro de ACH no procesado por lotes. Del mismo modo, los bancos que entablan relaciones con prestadores de servicios externos deben analizar el carácter de dichas relaciones y sus transacciones ACH relacionadas para confirmar el nivel de riesgo según la OFAC del banco y para desarrollar políticas, procedimientos y procesos para mitigar ese riesgo.

Con respecto a las evaluaciones transnacionales, existen obligaciones similares aunque más estrictas de la OFAC para las IAT. En el caso de las IAT de entrada, e independientemente de si se establece la bandera de la OFAC en la IAT, una RDFI es responsable del cumplimiento con las exigencias de la OFAC Sin embargo, en el caso de las transacciones IAT de salida, la ODFI no puede depender de la evaluación de la OFAC por parte de una RDFI fuera de los Estados Unidos. En tales situaciones, la ODFI debe ejercer diligencia intensificada para garantizar que no se procesen transacciones ilegales.

La debida diligencia para una IAT de entrada o de salida puede incluir la evaluación de las partes para una transacción, así como la revisión de los detalles de la información del campo de pago de una indicación de violación a una sanción, la investigación de los positivos resultantes, en caso que existan, y, finalmente, el bloqueo o rechazo de la transacción, según corresponda. Consulte la sección del esquema general principal, “Oficina de control de activos extranjeros”, en las páginas 165 a 175, como guía.

---

[194] Consulte la nota explicativa 041214-FACRL-GN-02 en www.treas.gov/offices/enforcement/ofac/rulings/. Las normas NACHA especifican aún más este cumplimiento (consulte la página 8 de la sección sobre búsqueda rápida de *2006 NACHA Operating Rules* [Normas operativas NACHA 2006]).

En una guía emitida el 10 de marzo de 2009, la OFAC autorizó a instituciones en los Estados Unidos, cuando actúen como una ODFI o un GO para débitos de IAT de entrada, a rechazar transacciones que parezcan involucrar intereses de propiedad o propiedad bloqueable.[195] La guía establecía además que en la medida que una ODFI o un GO evalúen los débitos de IAT de entrada para determinar si existen posibles violaciones a la OFAC antes de la ejecución y en el transcurso de dicha evaluación descubren una potencial violación a la OFAC, la transacción sospechosa se deberá eliminar del lote para realizar una investigación más profunda. Si la ODFI o el GO determinan que la transacción no parece violar los reglamentos de la OFAC, deben negarse a procesar la transferencia. El procedimiento se aplica a las transacciones que normalmente serían bloqueadas así como para las transacciones que normalmente serían rechazadas por propósitos de la OFAC en función de la información de los pagos.

Más información sobre los tipos de sistemas de pago al por menor (sistemas de pago ACH) está disponible en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[196]

---

[195] Consulte www.frbservices.org/files/eventseducation/pdf/iat/031809_ofac_update.pdf.

[196] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

Procedimientos de Inspección

Transacciones de compensación automatizada

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con la compensación automatizada (ACH) y las transacciones ACH internacionales (IAT), y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las transacciones ACH, incluidas las IAT. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de transacciones ACH del banco, incluidas las IAT, y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz los clientes de riesgo más alto que efectúan transacciones ACH, incluidas las IAT.

3. Evalúe los riesgos del banco relacionados con las transacciones ACH, incluidas las IAT, analizando la frecuencia y el volumen en dólares y los tipos de transacciones ACH en relación con el tamaño, la ubicación y el carácter de las relaciones asociadas con las cuentas de los clientes del banco, y la ubicación de la fuente y el destino de las IAT con relación a la ubicación del banco.

4. Determine si el sistema del banco para supervisar a los clientes, incluidos los prestadores de servicios externos (TPSP), que efectúan transacciones ACH y IAT y detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco. Determine si los sistemas de control interno incluyen:

   - La identificación de clientes con IAT o transacciones ACH de grandes volúmenes y frecuentes.

   - La supervisión de la actividad de detalles de ACH cuando las transacciones procesadas por lotes se separan para otros fines (por ejemplo, el procesamiento de errores).

   - Según corresponda, la identificación y la aplicación de la debida diligencia intensificada a clientes de mayor riesgo que originan o reciben IAT, en especial cuando una parte de la transacción se encuentra en una ubicación geográfica de mayor riesgo.

   - La utilización de métodos para hacer seguimiento, revisar e investigar los retornos no autorizados o las quejas de los clientes sobre posibles transacciones ACH duplicadas o fraudulentas, incluyendo IAT.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de control de activos extranjeros", en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de los clientes con transacciones ACH, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de clientes de riesgo más alto, incluidos los TPSP, con transacciones ACH o IAT, que puede incluir lo siguiente:

   - Clientes que inician transacciones ACH, incluidas las IAT, que se originan en Internet o por teléfono, particularmente desde una cuenta que se abre en Internet o por teléfono sin interacción personal directa.
   - Clientes cuyos tipos de negocios u ocupaciones no requieren el volumen ni el carácter de la actividad de ACH o IAT.
   - Clientes que hayan participado en el origen o la recepción de IAT o transacciones ACH duplicadas o fraudulentas.
   - Clientes remitentes (clientes de clientes) que generan un alto porcentaje o alto volumen de retorno sobre la inversión inválidos, retorno sobre la inversión no autorizado o u otras transacciones no autorizadas.

7. De la muestra seleccionada, analice las transacciones ACH, incluidas las IAT, para determinar si las cantidades, la frecuencia y las jurisdicciones de origen y destino son coherentes con el tipo de negocio u ocupación del cliente. Un control de la documentación de apertura de la cuenta, incluida la documentación del CIP, puede ser necesario para tomar estas determinaciones. Identifique cualquier actividad sospechosa o poco habitual.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados a las IAT y las transacciones ACH.

Efectivo Electrónico: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con el efectivo electrónico (e-cash), y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

El efectivo electrónico (dinero electrónico) es una representación digital del dinero. El efectivo electrónico adopta diversas formas, entre ellos, medios informáticos, medios de telefonía móvil y tarjetas prepagadas. El efectivo electrónico se almacena en un repositorio en línea y el acceso a este se obtiene vía módem por medio de los discos rígidos de las computadoras personales. El acceso al efectivo electrónico basado en la telefonía móvil se obtiene a través del teléfono móvil de una persona. Las tarjetas prepagadas, descritas más detalladamente a continuación, se utilizan para obtener acceso a fondos retenidos por bancos emisores en cuentas agrupadas.

En el caso del efectivo electrónico por medio de computadora, el valor monetario se deduce electrónicamente de la cuenta bancaria cuando se realiza una compra o se transfieren fondos a otra persona. Hay más información sobre los tipos de productos de efectivo electrónico en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[197]

Factores de riesgo

Las transacciones que utilizan efectivo electrónico pueden plantear al banco los siguientes riesgos particulares:

- Los fondos se pueden transferir desde o hacia un tercero desconocido.
- Los clientes pueden evitar las restricciones impuestas en las fronteras ya que las transacciones tienen la capacidad de hacerse móviles y pueden no estar sujetas a restricciones jurisdiccionales.
- Las transacciones pueden ser instantáneas.
- La actividad específica del titular de la tarjeta puede ser difícil de determinar controlando la actividad a través de una cuenta agrupada.
- El cliente puede percibir que las transacciones son menos transparentes.

Mitigación del riesgo

Los bancos deben establecer una supervisión, identificación y presentación de informes BSA/AML de actividades sospechosas y poco habituales que ocurran a través de efectivo

[197] The FFIEC *Information Technology Examination Handbook* is available at www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

electrónico. Los MIS útiles para detectar las actividades poco habituales en cuentas de riesgo más alto incluyen los informes de actividad de cajeros automáticos (enfocándose en las transacciones extranjeras), informes de transferencias de fondos, informes de actividad de cuentas nuevas, informes de cambio de dirección de Internet, informes de direcciones de Protocolo de Internet (IP, por sus siglas en inglés) e informes para identificar cuentas relacionadas o vinculadas (por ejemplo, direcciones, números telefónicos, direcciones de correo electrónico y números de identificación fiscal comunes). Además, el banco puede implementar otros controles, como el establecimiento de límites en dólares por transacción o cuenta que requieran intervención manual para superar el límite preestablecido.

Tarjetas prepagadas/Tarjetas de valor acumulado

De acuerdo con la práctica de la industria, en este documento se utiliza principalmente el término “tarjeta prepagadas”. Si bien en general algunas fuentes utilizan el término “tarjeta de valor acumulado”, con mayor frecuencia se refiere a las tarjetas en las que el valor monetario está físicamente almacenado en la tarjeta. Por lo general, el término “tarjeta prepagadas” se refiere a un dispositivo de acceso vinculado a fondos retenidos en una cuenta agrupada, que es el tipo de producto que más frecuentemente ofrecen las organizaciones bancarias estadounidenses. Las tarjetas prepagadas pueden cubrir una variedad de productos, funcionalidades y tecnologías, y funcionan dentro de sistemas “abiertos”
o “cerrados”. Las tarjetas prepagadas de sistemas abiertos se pueden utilizar para realizar compras en cualquier intermediario o para obtener acceso a efectivo en cualquier cajero automático (ATM) conectado a la red de pago global afiliada. Algunos ejemplos de tarjetas de sistemas abiertos son las tarjetas de nómina y las tarjetas de regalo que se pueden utilizar en cualquier lugar donde se pueda utilizar una tarjeta de crédito. Algunas tarjetas prepagadas se pueden recargar, lo que permite que el titular de la tarjeta agregue valor. En general, las tarjetas de sistemas cerrados sólo se pueden utilizar para adquirir bienes o servicios del intermediario que expide la tarjeta o de un grupo selecto de intermediarios o prestadores de servicios que participan en una red específica. Algunos ejemplos de tarjetas de sistemas cerrados incluyen las tarjetas de regalo de tiendas minoristas específicas de los intermediarios, las tarjetas de los centros comerciales y las tarjetas de transporte público

Algunos programas de tarjetas prepagadas pueden combinar varias características, como una a tarjeta de gastos flexible que se pueden utilizar para adquirir determinados servicios de salud y productos de una amplia gama de intermediarios. A menudo estos programas se denominan tarjetas “híbridas”.

Las tarjetas prepaga proporcionan una forma compacta y trasladable de mantener y obtener acceso a fondos. Además, ofrecen a las personas que no tienen una cuenta bancaria una alternativa de acceso a efectivo y giros postales. Como un método alternativo de transferencias de fondos transnacionales, los programas de tarjetas prepaga pueden emitir varias tarjetas por cuenta, de modo que otras personas en otro país puedan obtener acceso a los fondos cargados por el titular de la tarjeta mediante extracciones de ATM o compras a intermediarios.

Muchos bancos ofrecen programas de tarjetas prepagadas como bancos emisores. La mayoría de las redes de pago requieren que sus tarjetas prepagadas de marca sean emitidas por un banco que sea miembro de dicha red de pago. Además de emitir tarjetas prepagadas, los bancos pueden participar en otros aspectos de un programa de tarjetas, como la comercialización y la distribución de tarjetas emitidas por otra institución financiera.

Con frecuencia, los bancos dependen de diversos terceros para lograr el diseño, la implementación y el mantenimiento de sus programas de tarjetas prepagadas. Estos terceros pueden incluir administradores de programas, distribuidores, vendedores, intermediarios y procesadores. Conforme a los requisitos de la red de pago, el banco emisor puede tener debida diligencia y otras responsabilidades relacionadas con estos terceros.

Acuerdos contractuales

Cada relación que un banco estadounidense mantenga con terceros o instituciones financieras como parte de un programa de tarjetas prepagadas debe regirse por un acuerdo o contrato que especifique las responsabilidades de cada una de las partes y otros detalles de la relación, como los productos y los servicios provistos. El acuerdo o contrato también debe considerar las exigencias de cumplimiento de OFAC y BSA/AML de cada parte, el tipo de clientela, los procedimientos de debida diligencia y las obligaciones de la red de pago. El banco emisor tiene la responsabilidad final con respecto al cumplimiento BSA/AML, ya sea que el acuerdo contractual se haya establecido o no.

Factores de riesgo

Si no hay controles eficaces implementados, a través de los programas de tarjetas prepagadas se pueden llevar a cabo lavado de dinero, financiamiento del terrorismo y otras actividades delictivas. Mediante investigaciones a cargo de las autoridades de aplicación de la ley, se ha descubierto que algunos titulares de tarjetas prepagadas utilizaban identificaciones falsas y financiaban los depósitos iniciales con tarjetas de crédito robadas o compraban varias tarjetas bajo sobrenombres. En la etapa de colocación del lavado de dinero, dado que muchos bancos nacionales y extraterritoriales ofrecen acceso a efectivo internacionalmente vía ATM, los delincuentes pueden cargar efectivo de fuentes ilícitas en tarjetas prepagadas a través de puntos de carga no regulados y enviar las tarjetas a sus cómplices dentro o fuera del país. Las investigaciones han revelado que las tarjetas prepagadas de sistemas abiertos y cerrados han sido utilizadas junto con, o como un reemplazo de, el contrabando de efectivo en grandes cantidades. Los terceros involucrados en los programas de tarjetas prepagadas pueden o no estar sujetos a exigencias normativas, control y supervisión. Además, estas exigencias pueden variar según las partes.

Los programas de tarjetas prepagadas son extremadamente diversos en la gama de productos y servicios provistos y en las bases de clientes que cubren. Al evaluar el perfil de riesgo de un programa de tarjetas prepagadas, los bancos deben considerar las características y las funcionalidades específicas del programa. No existe un único indicados que sea necesariamente determinante de un riesgo BSA/AML más alto o más bajo. El riesgo de lavado de dinero potencialmente más alto asociado con las tarjetas

prepagadas deriva del anonimato del titular de la tarjeta, la información falsa sobre el titular de la tarjeta, el acceso a efectivo que brinda la tarjeta (en especial internacionalmente)
y el volumen de fondos que pueden tramitarse con la tarjeta. Otros factores de riesgo incluyen el tipo y la frecuencia de las transacciones y las cargas de la tarjeta, la ubicación geográfica de la actividad de la tarjeta, las relaciones con terceros en el programa de la tarjeta, los límites de valor de la tarjeta, los canales de distribución y la naturaleza de las fuentes de financiación.

Mitigación del riesgo

Los bancos que ofrecen tarjetas prepagadas o que de alguna otra forma participan en programas de tarjetas prepagadas deben tener políticas, procedimientos y procesos suficientes para gestionar los riesgos BSA/AML relacionados. La guía que ofrece la Network Branded Prepaid Card Association (Asociación de la red de tarjetas prepagadas de marca) es un recurso adicional para los bancos que prestan servicios de tarjetas prepagadas.[198] La debida diligencia de los clientes es importante para mitigar el riesgo BSA/AML de los programas de tarjetas prepagadas. El programa CDD de un banco debe proporcionar un análisis de riesgos de todos los terceros involucrados en el programa de tarjetas prepagadas que considere todos los factores relevantes y que incluya, según corresponda:

- La identidad y la ubicación de todos los terceros involucrados en el programa de tarjetas prepagadas, incluidos los subagentes.
- La documentación corporativa, las licencias y las referencias (incluidos los servicios de informe independiente) y, si corresponde, la documentación sobre los propietarios principales.
- La naturaleza de las empresas de los terceros, y los intermediarios y las bases de clientes cubiertos.
- La información recopilada para identificar y verificar la identidad del titular de la tarjeta.
- El tipo, el propósito y la actividad prevista del programa de tarjetas prepagadas.
- La naturaleza y la duración de la relación del banco con los terceros en el programa de las tarjetas.
- Las obligaciones según la OFAC y BSA/AML de los terceros.

---

[198] Consulte *Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs* (Prácticas recomendadas para el cumplimiento contra el lavado de dinero para los programas de tarjetas prepagadas basados en los Estados Unidos, del 28 de Febrero de 2008, en www.nbpca.com/docs/NBPCA-AML-Recommended-Practices-080220.pdf.

Como parte de su sistema de controles internos, los bancos deben establecer un medio para supervisar, identificar e informar las actividades sospechosas relacionadas con los programas de tarjetas prepagadas. Esta exigencia de gestión de registros se aplica a todas las transacciones que realiza el banco o que se realizan en o a través del banco, incluidas aquellas en un formulario adicional. Es posible que los bancos necesiten establecer protocolos para obtener periódicamente información de las transacciones con tarjeta por parte de procesadores y otros terceros. Los sistemas de supervisión deben tener la capacidad para identificar la actividad de las tarjetas en el extranjero, las compras de grandes cantidades realizadas por una persona y las compras múltiples realizadas por terceros relacionados. Además, los procedimientos deben incluir la supervisión de patrones de actividad poco habitual, como las cargas de tarjetas de crédito seguidas inmediatamente de extracciones del importe total desde otra ubicación.

Las características de las tarjetas pueden proporcionar una mitigación significativa de los riesgos BSA/AML inherentes a las transacciones y las relaciones de tarjetas prepagadas, y pueden incluir:

- Límites o prohibiciones de carga, acceso o reembolso de efectivo.
- Límites o prohibiciones respecto de los importes de las cargas y la cantidad de cargas/recargas en un plazo dado (velocidad de uso de los fondos).
- Controles sobre la cantidad de tarjetas adquiridas por un individuo.
- Umbrales en dólares máximos en las extracciones de ATM y en la cantidad de extracciones en un plazo dado (velocidad del uso de los fondos).
- Límites o prohibiciones respecto de determinado uso (por ejemplo, tipo de intermediario) y del uso geográfico, como fuera de los Estados Unidos.
- Límites con respecto a los valores de tarjetas agregados.

Procedimientos de Inspección

Efectivo electrónico

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con el efectivo electrónico (e-cash), incluidas las tarjetas prepagadas, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto al efectivo electrónico, incluidas las tarjetas prepagadas. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de efectivo electrónico del banco, incluidas las tarjetas prepagadas, y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las transacciones de banca electrónica de riesgo más alto, incluidas las transacciones con tarjetas prepagadas.

3. Determine si el sistema del banco para supervisar las transacciones de banca electrónica, incluidas las transacciones con tarjetas prepagadas, y para detectar e informar actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de efectivo electrónico, incluidas las transacciones con tarjetas prepagadas, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las transacciones con efectivo electrónico. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta, incluida la del CIP, la debida diligencia continua de los clientes y los antecedentes de transacciones.
   - Compare la actividad prevista con la actividad real.
   - Determine si la actividad es coherente con el tipo de negocio del cliente.
   - Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos con respecto a las relaciones asociadas con efectivo electrónico.

Procesadores de Pagos Externos: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con sus relaciones con los procesadores de pagos externos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Los procesadores de pagos externos o no bancarios (procesadores) son clientes de bancos que prestan servicios de procesamiento de pagos a intermediarios y otras entidades comerciales. Tradicionalmente, los procesadores eran contratados principalmente por vendedores minoristas que tenían ubicaciones físicas para procesar sus transacciones. Estas transacciones de intermediarios incluían principalmente pagos con tarjetas de crédito pero también abarcaban transacciones de ACH, cheques creados remotamente (RCC)[199] y transacciones con tarjetas de débito o prepagadas. Con la expansión de Internet, las fronteras de los minoristas se han eliminado. En la actualidad, los procesadores prestan servicios a una variedad de cuentas de intermediarios, incluidos los comercios en Internet y los minoristas convencionales, las empresas de viajes prepagos, los *telemarketers* y los servicios de apuestas por Internet.

Los procesadores de pagos externos con frecuencia utilizan sus cuentas bancarias comerciales para realizar el procesamiento de pago de sus clientes intermediarios. Por ejemplo, el procesador puede depositar en su cuenta los RCC emitidos a nombre de un cliente intermediario o actuar como un remitente externo de transacciones ACH. En cualquiera de los casos, el banco no tiene una relación directa con el intermediario. El aumento del uso de los RCC por parte de los clientes de los procesadores, en especial los *telemarketers*, también aumenta el riesgo de procesamiento de pagos fraudulentos a través de la cuenta bancaria del procesador. La Corporación Federal de Seguro de Depósitos y la Oficina del Interventor Monetario han publicado una guia con relación a los riesgos, incluyendo los riesgos BSA/AML, asociados con los procesadores bancarios externos.[200]

Factores de riesgo

Generalmente, los procesadores no están sujetos a exigencias normativas BSA/AML. Como resultado, algunos procesadores pueden ser vulnerables al lavado de dinero, el robo de identidad y las estratagemas de fraude, y las transacciones ilícitas o las transacciones prohibidas por la OFAC.

---

[199] Un cheque creado remotamente (algunas veces llamado "giro a la vista") es un cheque que no es creado por el banco pagador (con frecuencia creado por un beneficiario o su prestador de servicios), librado de la cuenta bancaria de un cliente. Con frecuencia, el cliente autoriza el cheque remotamente, por teléfono o en línea y, por lo tanto, no lleva su firma de puño y letra.

[200] *Guidance on Payment Processor Relationships* (Guía sobre las relaciones con procesadores de pagos), FDIC FIL-127-2008, del 7 de Noviembre de 2008, y *Risk Management Guidance: Payment Processors* (Guía de gestión de riegos: procesadores de pagos), Boletín 2008-12 de la OCC, del 24 de Abril de 2008.

Los riesgos BSA/AML del banco al manejar una cuenta del procesador son similares a los riesgos de otras actividades en las que el cliente del banco efectúa transacciones a través del banco en nombre de los clientes del cliente. Cuando el banco no puede identificar ni comprender el carácter y fuente de las transacciones procesadas a través de una cuenta, los riesgos a los que se expone el banco y la probabilidad de actividades sospechosas pueden aumentar. Si un banco no ha implementado un programa de aprobación de procesadores adecuado que vaya más allá de la gestión de riesgos del crédito, podría ser vulnerable al procesamiento de transacciones ilícitas o sancionadas por la OFAC.

Los bancos que tienen clientes de procesadores de pagos externos deben estar al tanto de la mayor probabilidad de riesgo de retornos no autorizados y el uso de servicios por parte de intermediarios de alto riesgo. Algunos intermediarios de alto riesgo utilizan a terceros de forma rutinaria para procesar sus transacciones por la dificultad que tienen para establecer una relación directa con un banco. Estas entidades pueden incluir ciertas compañías de solicitud de pedidos por vía telefónica o por correo, compañías de *telemarketing*, las operaciones de apuestas en línea, los prestamistas de día de pago en línea, las empresas instaladas en el exterior y las empresas de entretenimiento para adultos. Los procesadores de pagos tienen un mayor riesgo de lavado de dinero y fraude si no tienen un medio eficaz para verificar las identidades y las prácticas comerciales de los clientes intermediarios. Los riesgos aumentan cuando el procesador no lleva a cabo la debida diligencia con respecto a los intermediarios para los que están originando los pagos.

Mitigación del riesgo

Los bancos que ofrezcan servicios de cuentas a procesadores deben desarrollar y mantener políticas, procedimientos y procesos adecuados para abordar los riesgos relacionados con estas relaciones. Como mínimo, estas políticas deben legitimar las operaciones comerciales del procesador y analizar su nivel de riesgo. Un banco puede evaluar los riesgos asociados con los procesadores de pagos al considerar:

- La implementación de una política que requiera una verificación de antecedentes inicial del procesador (por ejemplo, mediante el sitio web de la Comisión Federal de Comercio, la Better Business Bureau, departamentos de incorporación estatal, investigaciones por Internet y otros procesos de investigación) y de los intermediarios subyacentes del procesador, en función del riesgo con el objeto de verificar su solvencia y las prácticas comerciales generales.

- La revision de los materiales promocionales del procesador, incluido su sitio web, para determinar la clientela objetivo. Un banco puede desarrollar políticas, procedimientos y procesos que limiten los tipos de entidades permisibles para procesar servicios. Estas entidades pueden incluir entidades de riesgo más alto, como las compañías extraterritoriales, las operaciones relacionadas con el servicio de apuestas en línea, los *telemarketers* y los prestamistas de día de pago en línea. Estas restricciones deben ser claramente comunicadas al procesador al momento de la apertura de la cuenta.

- La determinación de si el procesador revende sus servicios a un tercero que se pueda definir como "agente o proveedor de oportunidades de Organización de ventas independiente" (ISO) o acuerdos de "puerta de enlace".[201]

- El control de las políticas, los procedimientos y los procesos del procesador para determinar la aptitud de sus normas de debida diligencia para los nuevos intermediarios.

- La solicitud al procesador de identificar a sus principales clientes al proporcionar información como el nombre del intermediario, su actividad comercial principal y su ubicación geográfica.

- La verificación directa, a través del procesador, de que el intermediario dirige una empresa legítima al comparar la información de identificación del intermediario con las bases de datos de los registros públicos y las bases de datos de fraude y cheques bancarios.

- La revision de documentación corporativa, incluidos los servicios de informe independiente y, si es aplicable, documentación sobre los propietarios principales.

- Visita al centro de operaciones comerciales del procesador.

Los bancos que prestan servicios de cuentas a procesadores de pagos externos deben supervisar sus relaciones con el procesador para detectar cualquier cambio significativo en las estrategias comerciales de éste que pueda tener efecto sobre su perfil de riesgo. Los bancos deben volver a verificar y actualizar periódicamente los perfiles de los procesadores para garantizar que el análisis de riesgos sea adecuado.

Además de los procedimientos adecuados y eficaces de debida diligencia y de apertura de la cuenta para las cuentas de procesadores, la gerencia debe supervisar estas relaciones para detectar actividades sospechosas o poco habituales. Para supervisar de manera eficaz estas cuentas, el banco debe contar con una comprensión de la siguiente información del procesador:

- Base del intermediario.

- Actividades del intermediario.

- Cantidad promedio de volumen en dólares y cantidad de transacciones.

- Volumen de "lecturas magnéticas" frente a "ingreso de datos" de las transacciones con tarjetas de crédito.

---

[201] Los acuerdos de puerta de enlace son similares a un proveedor de servicios de Internet con mayor capacidad de almacenamiento que vende esta capacidad a un tercero, quien a su vez distribuye servicios informáticos a otras personas diversas desconocidas por el proveedor. El tercero tomará las decisiones sobre quién recibirá el servicio, aunque el proveedor será el que proporcione la capacidad de almacenamiento final. Por lo tanto, el proveedor carga con todos los riesgos y recibe una ganancia menor.

- Antecedentes de reintegro del cobro, incluido el porcentaje de retorno sobre la inversión de las transacciones con débito de ACH y los RCC.

- Quejas de los clientes que sugieran que los clientes intermediarios de un procesador de pagos están obteniendo indebidamente información de cuentas personales y la están usando para generar débitos en ACH o RCC no autorizados.

Con respecto a la supervisión de cuentas, un banco debe investigar minuciosamente los altos niveles de retorno. La decision de aceptar o no altos niveles de retorno no debe ser basada la garantía colateral u otro medio de seguridad proporcionada por el procesador al banco. Un banco debe implementar políticas, procedimientos y procesos adecuados que aborden los riesgos de cumplimiento y fraude. Los altos niveles de débitos en ACH o RCC devueltos por fondos insuficientes o usos no autorizados pueden ser un indicador de fraude o actividad sospechosa.

Procedimientos de Inspección

Procesadores de pagos externos

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con sus relaciones con los procesadores de pagos externos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a los procesadores de pagos externos (procesadores). Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de procesador del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones con los procesadores, particularmente aquellas que presenten un riesgo más alto de lavado de dinero.

3. Determine si el sistema de supervisión de las cuentas de los procesadores del banco para detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de control de activos extranjeros", en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de procesador, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de los procesadores de riesgo más alto. De la muestra seleccionada:

   - Revise la documentación de apertura de la cuenta e información de debida diligencia continua.
   - Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones para determinar los resultados de la comparación de las transacciones previstas con la actividad real.
   - Determine si la actividad real es coherente con el carácter de la actividad indicada del procesador.
   - Evalúe los controles relacionados con la identificación de altos índices de retornos no autorizados y el proceso vigente para abordar los riesgos de cumplimiento y fraude.
   - Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las cuentas de los procesadores.

Compraventa de Instrumentos Monetarios: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los instrumentos monetarios, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe. Esta sección amplía la revisión principal de las exigencias normativas y legales para la compraventa de instrumentos monetarios para proporcionar un análisis más minucioso de los riesgos de lavado de dinero asociados con esta actividad.*

Los instrumentos monetarios son productos proporcionados por bancos e incluyen cheques de caja, cheques de viajeros y giros postales. Generalmente, los instrumentos monetarios se compran para pagar transacciones personales o comerciales y, en el caso de los cheques de viajeros, como forma de valor acumulado para futuras compras.

Factores de riesgo

La compra o cambio de instrumentos monetarios en las fases de colocación y transformación del lavado de dinero puede ocultar la fuente de ingresos ilícitos. Como resultado, los bancos han sido objetivos importantes en las operaciones de lavado debido a que proporcionan y procesan instrumentos monetarios a través de depósitos. Por ejemplo, se sabe que tanto clientes como quienes no son clientes han comprado instrumentos monetarios en sumas por debajo del umbral de USD 3.000 para evitar tener que proporcionar la identificación adecuada. Posteriormente, los instrumentos monetarios se colocan en las cuentas de depósito para eludir el umbral de presentación de CTR.

Mitigación del riesgo

Los bancos que vendan instrumentos monetarios deben disponer de políticas, procedimientos y procesos adecuados para mitigar el riesgo. Las políticas deben definir:

- Las transacciones con instrumentos monetarios aceptables y no aceptables (por ejemplo, transacciones de individuos que no son clientes, instrumentos monetarios con beneficiarios en blanco, instrumentos monetarios sin firma, exigencias de identificación para transacciones fraccionadas o la compra de múltiples instrumentos monetarios numerados en secuencia para el mismo beneficiario).

- Procedimientos para el control y detección de actividades sospechosas o poco habituales, incluida la derivación de cualquier inquietud a la gerencia.

- Los criterios de cese de las relaciones o negación a realizar negocios con individuos que no son clientes que hayan estado involucrados ininterrumpida y flagrantemente en actividades sospechosas.

Procedimientos de Inspección

Compraventa de instrumentos monetarios

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los instrumentos monetarios, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe. Esta sección amplía la revisión principal de las exigencias normativas y legales para la compraventa de instrumentos monetarios para proporcionar un análisis más minucioso de los riesgos de lavado de dinero asociados con esta actividad.*

1. Revise las políticas, los procedimientos y los procesos con respecto a la venta de instrumentos monetarios. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de instrumentos monetarios del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger de manera razonable al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir del volumen de ventas y la cantidad de ubicaciones en las que se venden instrumentos monetarios, determine si el banco gestiona de manera adecuada el riesgo asociado con las ventas de instrumentos monetarios.

3. Determine si el sistema de supervisión de los instrumentos monetarios del banco para detectar e informar de actividades sospechosas, es adecuado dados el volumen de ventas de instrumentos monetarios, el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco. Determine si los sistemas de supervisión e informe de actividades sospechosas (manuales o automatizados) incluyen un control de:

   - Las ventas de instrumentos monetarios numerados en secuencia del mismo comprador o compradores diferentes para el mismo beneficiario y en un mismo día.
   - Las ventas de instrumentos monetarios al mismo comprador o ventas de instrumentos monetarios a compradores diferentes a nombre del mismo emisor.
   - Las compras de instrumentos monetarios por parte de quienes no son clientes.
   - Los compradores, beneficiarios y domicilios comunes, compras numeradas en secuencia y símbolos poco habituales.[202]

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

[202] Se sabe que quienes lavan dinero identifican la propiedad o fuente de los fondos ilegales a través del uso de impresiones únicas y poco habituales.

Pruebas de transacciones

5. En función del análisis de riesgos del banco, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de transacciones con instrumentos monetarios tanto para clientes como para quienes no son clientes de:

   - Registros de ventas de instrumentos monetarios.
   - Copias de instrumentos monetarios compensados comprados en efectivo.

6. De la muestra seleccionada, analice la información de transacción para determinar si las sumas, la frecuencia de las compras y los beneficiarios involucrados son consistentes con la actividad prevista de los clientes o quienes no son clientes (por ejemplo, pago de servicios públicos o compras domésticas). Identifique cualquier actividad sospechosa o poco habitual.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con los instrumentos monetarios.

Depósitos Mediante Agentes: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones con respecto a depósitos mediante agentes, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Para muchos bancos, el uso de depósitos mediante agentes es una fuente común de financiamiento. Los avances recientes en la tecnología permiten que los agentes proporcionen a los banqueros un mayor acceso a una gran variedad de inversionistas potenciales que no están relacionados con el banco. Los depósitos se pueden obtener en Internet, a través servicios de cotización de certificados de depósito o a través de otros métodos publicitarios.

Los agentes de depósitos proporcionan servicios intermediarios para bancos e inversionistas. Esta actividad se considera de alto riesgo debido a que cada agente de depósito opera bajo sus propias pautas para obtener depósitos. El nivel de supervisión regulatoria de los agentes de depósito varía, como también la aplicabilidad directa de las exigencias BSA/AML a estos. Sin embargo, el agente de depósito está sujeto a las exigencias de la OFAC independientemente de su nivel regulatorio. Por consiguiente, es posible que el agente de depósito no esté llevando a cabo debida diligencia de los clientes o una evaluación de la OFAC adecuadas. Para obtener más información, consulte la sección del esquema general principal "Oficina de Control de Activos Extranjeros," en las páginas 165 a 175, o los procedimientos de inspección de la sección principal "Programa de identificación de clientes", en las páginas 65 a 68.[203] El banco que acepte depósitos mediante agentes dependerá del agente de depósitos para llevar a cabo de manera suficiente los procedimientos de apertura de la cuenta exigidos y cumplir con las exigencias de BSA/AML aplicables.

Factores de riesgo

Los riesgos de lavado de dinero y financiamiento del terrorismo surgen debido a que el banco puede no tener conocimiento de los usufructuarios finales o del origen de los fondos. El agente de depósito puede representar a una variedad de clientes que puede plantear un riesgo más alto de lavado de dinero y financiamiento del terrorismo (por ejemplo, clientes no residentes o extraterritoriales, personalidades sujetas a exposición política [PEP] o bancos fantasmas extranjeros).

[203] A los efectos de la reglamentación del CIP, en el caso de los depósitos mediante agentes, el "cliente" será el agente que abre la cuenta. Un banco no necesitará examinar la cuenta del agente de depósito para determinar la identidad de cada cotitular de cuenta en particular, sólo necesitará verificar la identidad del titular de la cuenta designado.

Mitigación del riesgo

Los bancos que acepten las cuentas o fondos de agentes de depósito deben desarrollar políticas, procedimientos y procesos adecuados que establezcan procedimientos de CDD mínimos para todos los agentes de depósito que provean depósitos al banco. El nivel de debida diligencia que un banco lleve a cabo debe ser acorde a su conocimiento del agente de depósito y las prácticas comerciales y base de clientes conocidas del agente de depósito.

En un intento por ocuparse del riesgo inherente en ciertas relaciones asociadas con agentes de depósito, los bancos pueden contemplar la celebración de un contrato firmado que establezca los papeles y responsabilidades de cada parte y las restricciones de ciertos tipos de clientes (por ejemplo, clientes no residentes o extraterritoriales, PEP o bancos fantasmas extranjeros). Los bancos deben realizar debida diligencia suficiente a los agentes de depósitos, en especial a los no regulados, desconocidos, extranjeros o independientes. Para gestionar los riesgos BSA/AML asociados con depósitos mediante agentes, el banco debe:

- Determinar si el agente de depósito constituye una empresa legítima en todas las ubicaciones operativas donde opera.
- Controlar las estrategias comerciales del agente de depósito, incluidos los mercados de clientes objetivo (por ejemplo, clientes nacionales y extranjeros) y los métodos de persuasión de los clientes.
- Determinar si el agente de depósito está sujeto a supervisión regulatoria.
- Evaluar si las políticas, los procedimientos y los procesos BSA/AML y según la OFAC del agente de depósito son adecuados (por ejemplo, confirmar si el agente de depósito lleva a cabo CDD suficiente, incluidos procedimientos del CIP).
- Determinar si el agente de depósito evalúa a los clientes para detectar coincidencias con la lista de la OFAC.
- Evaluar la aptitud de las auditorías BSA/AML y según la OFAC del agente de depósito y asegurarse de que cumplan con las exigencias y los reglamentos vigentes.

Los bancos deben tener suma cautela al supervisar a los agentes de depósito que no constituyan entidades reguladas y:

- Sean desconocidos para el banco.
- Realicen negocios u obtengan depósitos principalmente en otras jurisdicciones.
- Usen negocios o bancos desconocidos o difíciles de contactar para verificar las referencias.
- Presten otros servicios que puedan ser sospechosos, como la creación de compañías fantasmas para clientes extranjeros.

- Se rehúsen a proporcionar la información de auditoría y debida diligencia solicitada o insistan en colocar depósitos antes de proporcionar dicha información.

- Usen tecnología que proporcione anonimato a los clientes.

Los bancos también deben supervisar las relaciones con los agentes de depósito existentes para detectar cualquier cambio significativo en las estrategias comerciales que pueda tener efecto sobre el perfil de riesgo del agente. Como tales, los bancos deben volver a verificar y actualizar periódicamente los perfiles de cada agente de depósito para garantizar que el análisis de riesgos sea adecuado.

Procedimientos de Inspección

Depósitos mediante agentes

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones con respecto a depósitos mediante agentes y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos respecto a las relaciones de depósitos mediante agentes. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades del agente de depósito del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. De un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con los depósitos mediante agentes, particularmente aquellas que planteen un mayor riesgo de lavado de dinero.

3. Determine si el sistema del banco para supervisar las relaciones del agente de depósito en busca de actividades sospechosas e informar de actividades sospechosas, es adecuado a su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con los clientes.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de depósitos mediante agentes, así como inspecciones previas e informes de auditoría, seleccione una muestra de las cuentas del agente de depósito de mayor riesgo. Cuando seleccionen una muestra, los inspectores deben considerar lo siguiente:

   - Nuevas relaciones con los agentes de depósito.
   - El método de generación de fondos (p. ej., agentes vía Internet).
   - Tipos de clientes (p. ej., clientes no residentes o fuera del país, personalidades sujetas a exposición política o bancos fantasmas extranjeros).
   - Un agente de depósito que haya aparecido en los Informes de actividades sospechosas (SAR).
   - Notificación de citaciones al banco por un agente de depósito en particular.
   - Proveedores de fondos extranjeros.
   - Actividad poco habitual.

6. Revise la información de debida diligencia de los clientes del agente de depósito. Respecto a los agentes de depósitos que son considerados de mayor riesgo (p. ej., solicitan fondos extranjeros, comercializan a través de Internet o son agentes independientes), analice si la siguiente información está disponible:

   - Antecedentes y referencias.
   - Negocios y métodos de comercialización.
   - Prácticas de debida diligencia y aceptación de clientes.
   - El método o fundamento del programa de bonificación o compensación del agente.
   - La fuente de los fondos del agente.
   - Su actividad prevista o tipos y niveles de transacciones (p. ej., transferencias de fondos).

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados a los agentes de depósitos.

Cajeros Automáticos de Propiedad Privada: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones con cajeros automáticos de propiedad privada (ATM) y Organizaciones de ventas independientes (ISO), y de la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Los cajeros automáticos de propiedad privada son particularmente susceptibles al lavado de dinero y al fraude. Los operadores de estos cajeros automáticos con frecuencia están incluidos en la definición de ISO.[204]

Los cajeros automáticos de propiedad privada generalmente se encuentran en minimercados, bares, restaurantes, tiendas de comestibles o establecimientos de cobro de cheques. Algunas ISO operan a gran escala, por otra parte, los propietarios de muchos cajeros automáticos de propiedad privada son los dueños de los establecimientos en los que están ubicados. La mayoría otorgan dinero en efectivo, mientras que algunos sólo otorgan un recibo impreso (vale) que el cliente cambia por dinero o mercadería. Los honorarios y recargos por las extracciones, junto a los negocios adicionales generados por el acceso de un cliente a un cajero automático, hacen que operar un cajero automático de propiedad privada sea rentable.

Las ISO vinculan sus cajeros automáticos a una red de transacciones de cajeros automáticos. Esta red envía los datos de las transacciones al banco del cliente para debitarlos de la cuenta de éste y finalmente acreditar los montos a la cuenta de la ISO, que puede estar ubicada en cualquier banco del mundo. Por lo general, los pagos a la cuenta de la ISO se hacen a través del sistema ACH. Más información sobre los tipos de sistemas de pago de operaciones al por menor está disponible en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC[205]

Banco patrocinador

Algunas transferencias electrónicas de fondos (EFT, por su siglas en inglés) o redes de puntos de venta (POS) requieren que la ISO esté patrocinada por algún miembro de la red (banco patrocinador). El banco patrocinador y la ISO están sujetos a todas las normas de

[204] Una ISO generalmente actúa como agente de los intermediarios, incluidos los propietarios de los cajeros automáticos, para procesar transacciones electrónicas. En algunos casos, el propietario de un cajero automático puede actuar como su propio procesador ISO. Los bancos pueden contratar los servicios de una ISO para buscar intermediarios y cajeros automáticos de propiedad privada; sin embargo, en muchas situaciones, las ISO contratan con los intermediarios y los propietarios de los cajeros automáticos sin el control ni la aprobación del banco de compensación.

[205] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

la red. El banco patrocinador también está encargado de garantizar que la ISO cumpla con todas las normas de la red. Por lo tanto, el banco patrocinador debe realizar una debida diligencia apropiada a la ISO y mantener la documentación adecuada para asegurar que la ISO patrocinada cumpla con las normas de la red.

Factores de riesgo

Actualmente, la mayoría de los estados no registra, no establece límites a la propiedad, como tampoco supervisa o inspecciona los cajeros automáticos de propiedad privada ni a sus ISO.[206] Si bien el proveedor de la red de transacciones de cajeros automáticos y el banco patrocinador deberían llevar a cabo la debida diligencia con respecto a las ISO, en la práctica esto puede variar. Además, es posible que el prestador no se entere de los cambios que se produzcan en la propiedad del ATM o de la ISO una vez que el contrato de ATM haya entrado en vigencia. Como resultado, muchos cajeros automáticos de propiedad privada han participado en estratagemas de lavado de dinero, robo de identidad, robo directo del dinero del ATM y fraude, o son vulnerables a la comisión de los mencionados delitos. Por lo tanto, los cajeros automáticos de propiedad privada y sus ISO implican un mayor riesgo y deben ser tratados en consecuencia por los bancos que negocian con ellos.

La debida diligencia comienza a ser un desafío mayor cuando las ISO venden cajeros automáticos a compañías de tercer y cuarto nivel ("sub-ISO") cuya existencia puede ser desconocida por el banco patrocinador, o realizan una subcontratación con dichas compañías. Cuando una ISO contrata o vende cajeros automáticos a una sub-ISO, el banco patrocinador puede desconocer quién es realmente el dueño del cajero automático. Por ende, las sub-ISO pueden ser dueñas y operar cajeros automáticos que permanezcan virtualmente invisibles al banco patrocinador.

Algunos cajeros automáticos de propiedad privada son administrados por servidores de efectivo para bóvedas, los cuales transportan el dinero en un vehículo blindado, reabastecen los cajeros automáticos, y los aseguran contra robos y daños. Sin embargo, muchas ISO administran y mantienen a sus propias máquinas, e incluso las abastecen con dinero en efectivo. Los bancos también pueden proporcionar dinero a las ISO mediante contratos de préstamo, lo que expone a esos bancos a diferentes riesgos, inclusive el riesgo de afectar su reputación y su crédito.

El lavado de dinero puede ocurrir a través de cajeros automáticos de propiedad privada cuando algunos de éstos se reabastecen con dinero obtenido ilícitamente que luego es retirado por clientes legítimos. Este proceso deriva en depósitos de ACH en la cuenta ISO que aparentan ser transacciones comerciales legítimas. Por lo tanto, las tres fases del lavado

[206] El 3 de Diciembre de 2007, la FinCEN publicó la guía interpretativa *Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services* (Aplicación de la definición de negocios de servicios monetarios a determinados propietarios y operadores de cajeros automáticos que ofrecen servicios limitados), FIN-2007-G006, en la cual aclara las circunstancias en las que un propietario, no bancario, y operador de un cajero automático constituiría un negocio de servicios monetarios a los efectos de la Ley de Secreto Bancario y sus reglamentos de ejecución.

de dinero (colocación, transformación e integración) pueden darse simultáneamente. Los lavadores de dinero pueden también confabularse con los intermediarios y las ISO que antes eran legítimas, para abastecer los cajeros automáticos con dinero ilícito a cambio de un descuento.

Mitigación del riesgo

Los bancos deben implementar políticas, procedimientos y procesos apropiados, que incluyan debida diligencia adecuada y supervisión de actividades sospechosas, para tratar los riesgos que presentan los clientes ISO. Como mínimo, estas políticas, procedimientos y procesos deben incluir:

- Debida diligencia adecuada en función del riesgo respecto a la ISO, mediante un control de la documentación, las licencias, los permisos, los contratos o las referencias de la corporación.
- Control de las bases de datos públicas para identificar problemas o preocupaciones potenciales relacionados con la ISO o sus propietarios principales.
- La comprensión de los controles de la ISO sobre los acuerdos para el suministro de dinero a los ATM de propiedad privada, incluida la fuente de reabastecimiento de las máquinas.
- Documentación de la ubicación de los cajeros automáticos de propiedad privada y determinación del mercado geográfico objetivo de la ISO.
- Actividad prevista de la cuenta, incluidas las extracciones de dinero en efectivo.

A causa de estos riesgos, es fundamental realizar una debida diligencia a las ISO que vaya más allá de las exigencias mínimas del CIP. Los bancos también deben realizar la debida diligencia a los propietarios de los cajeros automáticos y a las sub-ISO, según sea pertinente. Esta debida diligencia puede incluir:

- El control de la documentación, las licencias, los permisos, los contratos o las referencias de la corporación, incluido el contrato de prestación de transacciones del ATM
- El control de las bases de datos públicas en busca de información sobre los propietarios de los cajeros automáticos.
- La obtención de las direcciones de todas las ubicaciones de los cajeros automáticos, determinando los tipos de negocios donde estén ubicados, e identificando la población objetivo.
- La determinación de los niveles de actividad previstos del cajero automático, incluidas las extracciones de dinero.
- La determinación de las fuentes de dinero en efectivo de los cajeros automáticos mediante el control de copias de los contratos con el vehículo blindado, los contratos de préstamos o cualquier otra documentación, según sea pertinente.

- La obtención de información sobre la ISO respecto a la debida diligencia en sus acuerdos sub-ISO, como la cantidad de cajeros automáticos y su ubicación, el volumen de las transacciones, el volumen en dólares y la fuente de reabastecimiento de dinero en efectivo.

Procedimientos de Inspección

Cajeros automáticos de propiedad privada

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones con cajeros automáticos de propiedad privada (ATM) y Organizaciones de ventas independientes (ISO), y de la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las cuentas de cajeros automáticos de propiedad privada. Evalúe la aptitud de las políticas, los procedimientos y los procesos respecto a las relaciones con los ATM de propiedad privada y las ISO, y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de los cajeros automáticos de propiedad privada.

3. Determine si el sistema del banco para supervisar las cuentas de los cajeros automáticos de propiedad privada en busca de actividades sospechosas, y para informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Determine si el banco patrocina membresías de la red para las ISO. Si el banco es un banco patrocinador, revise los acuerdos contractuales con las redes y las ISO para determinar si los procedimientos y los controles de debida diligencia están diseñados para garantizar que las ISO cumplen con las normas de red. Determine si el banco obtiene información de las ISO con respecto a la debida diligencia en sus acuerdos sub-ISO.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus relaciones con cajeros automáticos de propiedad privada y con las ISO, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de cajeros automáticos de propiedad privada. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la información referente a la CDD del banco. Determine si la información verifica de manera adecuada la identidad de las ISO y describe:

     – Sus antecedentes.

     – La fuente de sus fondos.

     – Su actividad prevista o tipos y niveles de transacciones (p. ej., transferencias de fondos).

- Sus ATM (tamaño y ubicación).
- Su acuerdo de entrega de dinero en efectivo, de ser aplicable.

- Revise cualquier informe MIS que el banco utilice para supervisar las cuentas ISO. Determine si el flujo de fondos o la actividad prevista es coherente con la información de CDD.

6. Determine si una ISO patrocinada utiliza proveedores o prestadores de servicios externos para cargar dinero, mantener los cajeros automáticos o solicitar ubicaciones de intermediarios. De ser así, revise una muestra de los acuerdos de servicios externos para verificar la aplicación de procedimientos de debida diligencia y control adecuados.
7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las ISO.

Productos de Inversión que no son para Depositar: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con productos de inversión que no son para depositar (NDIP, por sus siglas en inglés) internos y en red, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

Los NDIP incluyen un amplio rango de productos de inversión (p. ej., valores, bonos, y rentas vitalicias fijas o variables). Los programas de venta también pueden incluir cuentas de administración de dinero en efectivo con servicio de barrido para clientes minoristas y comerciales; los bancos ofrecen esto programas directamente. Los bancos ofrecen estas inversiones para aumentar sus ingresos por honorarios y proporcionar a los clientes productos y servicios adicionales. La manera en que está estructurada la relación con los NDIP y los métodos mediante los cuales se ofrecen, afecta sustancialmente los riesgos y responsabilidades BSA/AML del banco.

Acuerdos de operación en red

Los bancos generalmente realizan acuerdos de operación en red con agentes bursatiles para ofrecer NDIP en las instalaciones del banco. A los efectos de BSA/AML, bajo un acuerdo de operación en red el cliente es cliente del agente de valores o de bolsa, aunque también puede ser cliente del banco respecto a otros servicios financieros. Los inspectores del banco reconocen que la Comisión de Valores y Bolsa de los EE. UU. (SEC, por sus siglas en inglés) es el principal regulador de la oferta de NDIP por medio de agentes bursatiles, y las agencias observarán las exigencias de supervisión funcional de la Ley Gramm–Leach–Bliley.[207] Las agencias bancarias federales están encargadas de supervisar las actividades NDIP realizadas directamente por los bancos. Los diferentes tipos de acuerdos de operación en red pueden incluir productos de marca conjunta, acuerdos para compartir empleados o acuerdos con terceros.

[207] La regulación funcional limita las circunstancias en las cuales las agencias bancarias federales pueden inspeccionar directamente o exigir informes de una subsidiaria o filial bancaria cuyo regulador principal es la SEC, la Comisión de Operaciones de Futuros Productos o las autoridades estatales de emisión. Las agencias bancarias federales por lo general tienen vedada la inspeccionar de esas entidades, a menos que se requiera más información para determinar si la subsidiaria o filial bancaria representa un riesgo material para el banco, para determinar el cumplimiento de alguna a exigencia legal bajo la jurisdicción de la agencia bancaria federal, o para analizar el sistema de gestión de riesgos del banco que cubre las actividades funcionalmente reguladas. Estos estándares requieren mayor dependencia del regulador funcional y más colaboración entre los reguladores.

Productos de marca conjunta

Los productos de marca conjunta son ofrecidos por otra empresa o corporación de servicios financieros[208] en patrocinio conjunto con el banco. Por ejemplo, una corporación de servicios financieros adapta un producto de fondo común para la venta en un banco específico. El producto es vendido exclusivamente en ese banco y lleva el nombre tanto del banco como de la corporación de servicios financieros.

Debido a esta relación de marca conjunta, la responsabilidad del cumplimiento con BSA/AML se vuelve conjunta. Puesto que estas cuentas no están únicamente bajo el control del banco o de la entidad financiera, puede variar la responsabilidad de llevar a cabo el CIP, la CDD, y la supervisión y el informe de actividades sospechosas. El banco debe conocer plenamente las responsabilidades contractuales de cada parte y garantizar que todas las partes realicen los controles adecuados.

Acuerdos para compartir empleados

En un acuerdo para compartir empleados, el banco y una corporación de servicios financieros, como una agencia de seguros o un agente de valores o de bolsa registrado, tienen un empleado en común (compartido). El empleado compartido puede encargarse de realizar negocios bancarios y también de vender NDIP, o bien vender NDIP a tiempo completo. Debido a este acuerdo para compartir empleados, el banco conserva sus responsabilidades respecto a las actividades relacionadas con los NDIP. Incluso en el caso de que los acuerdos contractuales establezcan que la corporación de servicios financieros será responsable del cumplimiento BSA/AML, el banco debe garantizar una supervisión adecuada de todos sus empleados, incluidos los empleados compartidos, y su cumplimiento con todas las exigencias normativas.[209]

Bajo algunos acuerdos de operación en red, los representantes registrados de ventas de valores son empleados compartidos entre el banco y el agente de bolsa o de valores. Cuando el empleado compartido ofrece productos y servicios de inversión, el agente de bolsa o de valores es responsable de supervisar el cumplimiento del representante registrado con la normativa vigente sobre valores aplicable. Cuando el empleado compartido ofrece productos y servicios bancarios, el banco tiene la responsabilidad de supervisar el desempeño del empleado y su cumplimiento con la BSA/AML.

Acuerdos con un tercero

Los acuerdos con terceros pueden comprender el alquiler del espacio que se encuentra en el vestíbulo del banco a una corporación de servicios financieros para vender NDIP. En

---

[208] Una corporación de servicios financieros incluye a aquellas entidades que ofrecen NDIP, que pueden ser, por ejemplo, empresas de inversión, instituciones financieras, agentes bursatiles, y compañías de seguros.

[209] Si el banco aplica la disposición sobre dependencia del CIP, la responsabilidad por el CIP se traslada al proveedor externo. Consulte la sección del esquema general principal, “Programa de identificación de clientes” en las páginas 57 a 64, para obtener información adicional.

este caso, el tercero debe diferenciarse a sí mismo claramente del banco. Si el acuerdo se implementa correctamente, los acuerdos con terceros no afectan las exigencias de cumplimiento BSA/AML del banco. Como una práctica responsable, se recomienda a los bancos comprobar si el prestador de servicios financieros cuenta con un programa de cumplimiento BSA/AML adecuado como parte de su debida diligencia.

Ventas realizadas internamente y productos de propiedad exclusiva

A diferencia de los acuerdos de operación en red, el banco es plenamente responsable por las transacciones NDIP realizadas internamente a nombre de sus clientes, impliquen o no el beneficio de un empleado interno del agente de bolsa o de valores.[210] Además, el banco también puede ofrecer sus NDIP de propiedad exclusiva, los cuales pueden ser creados y ofrecidos por el banco, su subsidiaria o una filial.

Con respecto a las ventas realizadas internamente y los productos de propiedad exclusiva, es posible que la totalidad de las relaciones con el cliente y todos los riesgos BSA/AML deban ser gestionados por el banco, según la manera en que se vendan los productos. A diferencia de los acuerdos de operación en red, en los cuales todas o algunas responsabilidades pueden ser asumidas por el agente de bolsa o de valores de terceros respecto a ventas realizadas internamente y productos de propiedad exclusiva, el banco debe gestionar todo lo relativo a las ventas de NDIP realizadas internamente y de NDIP de propiedad exclusiva, no sólo en todos sus departamentos, sino en toda la institución.

Factores de riesgo

Los riesgos BSA/AML se presentan porque los NDIP pueden implicar acuerdos legales complejos, grandes volúmenes en dólares y rápidos movimientos de fondos. Las carteras NDIP que administran y controlan directamente los clientes plantean un mayor riesgo de lavado de dinero que los que administran los bancos o prestadores de servicios financieros. Los clientes experimentados pueden llegar a estructurar sus propiedades de tal forma que queden ocultos la propiedad y el control finales de estas inversiones. Por ejemplo, los clientes pueden conservar cierto nivel de anonimato constituyendo Compañías de inversión privada (PIC),[211] fideicomisos fuera del país u otras entidades de inversión que oculten su propiedad o derecho de usufructo.

---

[210] En algunas circunstancias, no se considerará a los bancos como agentes de bolsa o de valores, y no se requerirá que el empleado sea registrado como agente de bolsa o de valores. Para ver una lista completa, consulte 15 USC 78c(a)(4).

[211] Consulte la sección del esquema general ampliado, “Entidades comerciales (nacionales y extranjeras)”, en las páginas 357 a 364, como guía para las PIC.

Mitigación del riesgo

La gerencia debe desarrollar políticas, procedimientos y procesos en función del riesgo, que le permitan al banco identificar relaciones y circunstancias de cuenta poco habituales, activos y fuentes de fondos cuestionables y otras áreas potenciales de riesgo (p. ej., cuentas fuera del país, cuentas en agencias y beneficiarios no identificados). La gerencia debe mantenerse alerta a las situaciones que requieran un control o una investigación adicional.

Acuerdos de operación en red

Antes de establecer un acuerdo de operación en red, los bancos deben realizar un control adecuado del agente de bolsa o de valores. El control debe incluir un análisis del estado financiero del mismo y de su experiencia gerencial, del carácter de su vinculación con la Asociación Nacional de Operadores de Valores o Bolsa (NASD, por sus siglas en inglés), de su reputación y de su capacidad para observar las responsabilidades de cumplimiento BSA/AML con respecto a los clientes del banco. Una debida diligencia adecuada debería incluir la determinación de que el agente de bolsa o de valores cuenta con políticas, procedimientos y procesos adecuados para cumplir con sus obligaciones legales. El banco debe mantener documentación sobre la debida diligencia del agente de bolsa o de valores. Además, todos los aspectos relacionados con las responsabilidades BSA/AML del agente de bolsa o de valores y de sus representantes registrados, incluyendo las relativas a la supervisión e informe de actividades sospechosas, deben estar contempladas en detalle en contratos escritos.

Un banco también puede querer mitigar su exposición al riesgo limitando ciertos productos de inversión ofrecidos a sus clientes. Los productos de inversión tales como las PIC, los fideicomisos, o los fondos de cobertura fuera del país, pueden implicar transferencias internacionales de fondos u ofrecer a los clientes formas de ocultar la titularidad de las propiedades.

La gerencia del banco debe hacer esfuerzos razonables para actualizar la información de debida diligencia de los agentes de bolsa o de valores. Dichos esfuerzos pueden incluir controles periódicos de la información sobre el cumplimiento de los agentes de bolsa o de valores con sus responsabilidades BSA/AML, verificación de sus antecedentes de cumplimiento con los requisitos de las pruebas y un control de las quejas de los clientes. También se recomienda a la gerencia, siempre que sea posible, controlar los informes BSA/AML generados por el agente de bolsa o de valores. Este control puede incluir información sobre apertura de cuentas, transacciones, productos de inversión vendidos y supervisión e informe de actividades sospechosas.

Ventas realizadas internamente y productos de propiedad exclusiva

La gerencia del banco debe analizar el riesgo considerando diferentes factores tales como:

- Tipo de NDIP comprados y el tamaño de las transacciones.
- Los tipos y la frecuencia de las transacciones.

- País de residencia de los mandantes o beneficiarios, o el país de constitución, o la fuente de los fondos.
- Las cuentas y transacciones que no sean habituales o acostumbradas para el cliente o el banco.

Respecto a los clientes que la gerencia considera de mayor riesgo de lavado de dinero y financiamiento del terrorismo, se deben establecer requisitos de documentación más estrictos, verificación y procedimientos de supervisión de las transacciones. Posiblemente sea adecuado llevar a cabo una EDD en las siguientes situaciones:

- Al iniciar el banco una relación con un cliente nuevo.
- Cuando las cuentas no discrecionales registren activos cuantiosos o transacciones frecuentes.
- El cliente reside en una jurisdicción extranjera.
- El cliente es una PIC u otra estructura corporativa establecida en una jurisdicción de mayor riesgo.
- Los activos y las transacciones son atípicas para el cliente.
- El tipo de inversiones, el tamaño, los activos o las transacciones son atípicas para el banco.
- Las transferencias internacionales de fondos se realizan especialmente desde fuentes de fondos ubicadas fuera del país.
- Las identidades de los mandantes o beneficiarios de inversiones o relaciones no se conocen o no se pueden determinar fácilmente.
- Las personalidades sujetas a exposición política (PEP) son parte en las inversiones o transacciones.

Procedimientos de Inspección

Productos de inversión que no son para depositar

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con productos de inversión que no son para depositar (NDIP, por sus siglas en inglés) internos y en red, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a los NDIP. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades con NDIP del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Si procede, revise los acuerdos contractuales con prestadores de servicios financieros. Determine la responsabilidad en el cumplimiento BSA/AML de cada parte. Determine si estos acuerdos proporcionan una supervisión BSA/AML adecuada.

3. A partir de un control de los informes de los MIS (p. ej., informes de excepciones, informes de transferencias de fondos e informes de supervisión de actividades) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz los NDIP, particularmente aquellos que planteen un mayor riesgo de lavado de dinero.

4. Determine de qué manera incluye el banco las actividades de ventas de NDIP en sus sistemas de acumulación BSA/AML aplicables a todo el banco o, según corresponda, a toda la institución.

5. Determine si el sistema del banco para supervisar los NDIP e informar sobre actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

Si el banco o su subsidiaria de participación mayoritaria son responsables de la venta o supervisión directa de los NDIP, los inspectores deben llevar a cabo los siguientes procedimientos de prueba de transacciones en las cuentas de clientes establecidas por el banco:

7. En función del análisis de riesgos del banco de sus actividades con NDIP, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de los NDIP de mayor riesgo. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

- Revise la documentación adecuada, incluidos los CIP, para asegurarse de que se haya practicado la debida diligencia adecuada y se hayan mantenido los registros adecuados.
- Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones para verificar:
  - Las transacciones previstas con la actividad real.
  - Conjunto de activos que excedan el valor neto del cliente.
  - Patrones de operaciones bursátiles irregulares (p. ej., transferencias de fondos entrantes para comprar valores seguidas de la entrega de los valores a otro custodio poco tiempo después).
- Determine si la actividad real es coherente con el tipo de negocio del cliente y el propósito declarado de la cuenta. Identifique cualquier actividad sospechosa o poco habitual.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las actividades de ventas de NDIP.

Seguros: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con la venta de productos de seguros cubiertos y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

Los bancos venden seguros para aumentar su rentabilidad, principalmente a través de la ampliación y diversificación de los ingresos por servicios. Generalmente, los productos de seguros se venden a los clientes del banco a través de acuerdos en red con una filial, una subsidiaria en operación u otros proveedores externos de seguros. Los bancos también están interesados en proporcionar oportunidades de ventas cruzadas para los clientes ampliando los productos de seguros que ofrecen. Por lo general, los bancos asumen el papel de agente de terceros en la venta de productos de seguros cubiertos. Los tipos de productos de seguros vendidos pueden incluir los de vida, médico, sobre la propiedad, contra accidentes, y de renta vitalicia fija o variable.

Exigencias de presentación de informes de actividades sospechosas y de programas de cumplimiento AML para compañías de seguros

Las normas de la FinCEN imponen a las compañías de seguros exigencias del programa de cumplimiento AML y obligaciones con respecto a los SAR similares a las impuestas a los bancos.[212] Los reglamentos sobre los seguros se aplican sólo a las compañías de seguros; no existen obligaciones independientes para los productores y agentes de seguros. Sin embargo, la compañía de seguros es responsable de la realización y eficacia de su programa de cumplimiento AML, que incluye las actividades de productores y agentes. Los reglamentos de seguros sólo son aplicables a un rango limitado de productos que pueden plantear un mayor riesgo de abuso por parte de los lavadores de dinero y los financistas del terrorismo. Un producto cubierto, a los efectos de un programa de cumplimiento AML, es:

- Una póliza de seguro de vida permanente, que no sea una póliza de seguro de vida grupal.
- Cualquier contrato de renta vitalicia, que no sea un contrato de renta vitalicia grupal.
- Cualquier otro producto de seguros con servicios de valor de contado o inversión.

Cuando se le exige a un agente o productor de seguros establecer un programa de cumplimiento BSA/AML bajo otra exigencia de los reglamentos de la BSA (p. ej., las exigencias para los agentes de valores o del banco), generalmente la compañía de seguros puede depender de ese programa de cumplimiento para ocuparse de los asuntos en el

[212] 31 CFR 103.137 y 31 CFR 103.16.

momento de la venta del producto cubierto.[213] Sin embargo, el banco puede necesitar establecer políticas, procedimientos y procesos específicos para sus ventas de seguros a fin de enviar la información a la compañía de seguros para que ésta cumpla con el programa AML.

Asimismo, si un banco, como agente de la compañía de seguros, detecta actividades sospechosas o poco habituales relacionadas con las ventas de seguros, puede presentar un SAR en conjunto con la compañía de seguros sobre la actividad en común.[214]

En Abril de 2008, la FinCEN publicó un informe analítico y estratégico que proporciona información sobre determinadas tendencias, patrones y tipologías de lavado de dinero en relación con los productos de seguros. Consulte *Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings* (Informes de actividades sospechosas en la industria de los seguros: Una evaluación de las presentaciones de informes de actividades sospechosas), en www.fincen.gov.

Factores de riesgo

Los productos de seguros se pueden utilizar para facilitar el lavado de dinero. Por ejemplo, se puede utilizar dinero para comprar una o más pólizas de seguro de vida, que un asegurado posteriormente puede cancelar rápidamente (también conocida como "amortización anticipada") siendo pasible de una sanción. La compañía de seguros reembolsa el dinero al comprador en la forma de un cheque. Las pólizas de seguro sin servicios de valor de contado o inversión plantean riesgos menores, pero pueden utilizarse para lavar dinero o financiar el terrorismo a través de la presentación de quejas falsas o exageradas por parte del asegurado a su compañía aseguradora, que de ser pagadas, permitirían al asegurado recuperar una parte o la totalidad de los pagos otorgados originalmente. Otras maneras en que se pueden utilizar los productos de seguros para lavar dinero incluyen:

- Pedir prestado el valor de rescate de las pólizas de seguro de vida permanentes.
- Vender unidades en productos vinculados con inversiones (como renta vitalicia).

---

[213] 70 Registro Federal 66758 (3 de Noviembre de 2005). Consulte también la Guía del FFIEC FIN-2006-G015, las *Frequently Asked Question, Customer Identification Programs and Banks Serving as Insurance Agents*, (Preguntas frecuentes, los Programas de identificación de clientes y Bancos que prestan servicios como agentes de seguros), del 12 de Diciembre de 2006, en www.fincen.gov/final_bank_insurance_agent_faq_12122006.pdf.

[214] La FinCEN ha publicado un documento de preguntas frecuentes, *Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies* (Exigencias de presentación de informes de actividades sospechosas y programa antilavado de dinero para compañías de seguros), en (www.fincen.gov)). A menos que el formulario del SAR incorpore múltiples responsables de la presentación del informe, sólo una institución se identifica como la responsable de la presentación del informe en la sección "*Filer Identification*" (Identificación del responsable de la presentación del informe) del formulario del SAR. En esos casos, la descripción debe incluir las palabras "*joint filing*" (presentación del informe en conjunto) e identificar a las otras instituciones en nombre de las cuales se presenta el informe.

- Utilizar ingresos de seguros provenientes de una amortización anticipada de la póliza para comprar otros activos financieros.
- Comprar pólizas que permitan la transferencia de derechos de usufructo sin el conocimiento ni el consentimiento del emisor (p. ej., póliza de seguro total de segunda mano y pólizas de seguros al portador).[215]
- Comprar productos de seguros a través de métodos poco habituales como moneda o equivalentes a la moneda.
- Comprar productos con servicios de interrupción del seguro sin tener en cuenta el rendimiento de la inversión del producto.

Mitigación del riesgo

Para mitigar los riesgos del lavado de dinero, el banco debe adoptar políticas, procedimientos y procesos que incluyan:

- La identificación de las cuentas de mayor riesgo.
- Debida diligencia de los clientes, incluida la debida diligencia especial para las cuentas de mayor riesgo.
- Diseño y uso del producto, tipos de servicios prestados y aspectos o riesgos particulares que presenten los mercados objetivo.
- Compensación de empleados y acuerdos de bonificación relacionados con las ventas.
- Supervisión, incluido el control de la terminación anticipada de pólizas y la presentación de informes de transacciones sospechosas y poco habituales (p. ej., un pago de prima único y elevado, la compra de un producto por parte de un cliente que parece salirse del rango normal de las transacciones financieras de ese cliente, rescate o redención anticipada, múltiples transacciones, pagos a terceros aparentemente no relacionados y préstamos respaldados con garantía).
- Exigencias en cuanto a la gestión de registros.

---

[215] Consulte *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* (Documento orientativo contra el lavado de dinero y la lucha contra el financiamiento del terrorismo) de la Asociación Internacional de Supervisores de Seguros, de Octubre de 2004, disponible en www.iaisweb.org.

Procedimientos de Inspección

Seguros

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con la venta de productos de seguros cubiertos y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las ventas de seguros. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de ventas de seguros del banco, su papel en las ventas de seguros y los riesgos que dichas ventas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Revise los contratos y acuerdos para los acuerdos en red del banco con las filiales, subsidiarias en operación u otros proveedores externos de seguros que lleven a cabo actividades de ventas dentro de las instalaciones de un banco y en nombre de éste.

3. Dependiendo de las responsabilidades del banco que se establezcan en los contratos y acuerdos, revise los informes de los MIS (p. ej., informes de grandes volúmenes, pagos únicos de la prima, registros de cancelación anticipada de pólizas, pagos de primas que excedan los valores de éstas y cesiones de derechos sobre pago) y los factores de valoración de riesgos internos. Determine si el banco identifica y supervisa de manera eficaz las ventas de productos de seguros cubiertos.

4. Dependiendo de las responsabilidades del banco que se establezcan en los contratos y acuerdos, determine si el sistema del banco para la supervisión de los productos de seguros cubiertos para detectar y elaborar informes de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

Si el banco o su subsidiaria de participación mayoritaria son responsables de la venta o supervisión directa de los seguros, los inspectores deben llevar a cabo los siguientes procedimientos de prueba de transacciones.

6. En función del análisis de riesgos del banco de sus actividades de ventas de seguros, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de los productos de seguros cubiertos. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta e información de debida diligencia continua.

- Revise la actividad de la cuenta. Compare las transacciones anticipadas con las transacciones reales.
- Determine si la actividad es sospechosa o poco habitual.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las ventas de seguros.

Cuentas de Concentración: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las cuentas de concentración y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

Las cuentas de concentración son cuentas internas establecidas para facilitar el procesamiento y liquidación de transacciones múltiples o individuales de los clientes dentro del banco, generalmente el mismo día. Estas cuentas también se conocen como cuentas de uso especial, cuentas ómnibus, cuentas puente o de tránsito, de liquidación, intradía, de barrido o de cobro. A menudo se utilizan para facilitar las transacciones de la banca privada, cuentas fiduciarias y de custodia de valores, transferencias de fondos y filiales internacionales.

Factores de riesgo

El riesgo de lavado de dinero puede surgir en las cuentas de concentración si la información de identificación de clientes —como el nombre, la suma de la transacción y el número de cuenta— se separa de la transacción financiera. Si ocurre la separación, se pierde el rastro de auditoría y es posible que las cuentas se usen o administren de manera indebida. Los bancos que usen cuentas de concentración deben implementar políticas, procedimientos y procesos que cubran la operación y gestión de registros de estas cuentas. Las políticas deben establecer pautas para identificar, medir, supervisar y controlar los riesgos.

Mitigación del riesgo

Debido a los riesgos planteados, la gerencia debe familiarizarse con el tipo de negocio de sus clientes y con las transacciones que pasen por las cuentas de concentración del banco. Además, la supervisión de las transacciones de las cuentas de concentración es necesaria para identificar e informar sobre transacciones sospechosas o poco habituales.

Los controles internos son necesarios para garantizar que las transacciones procesadas incluyan la información de identificación de clientes. La conservación de información completa es esencial para garantizar el cumplimiento con las exigencias normativas y la supervisión adecuada de las transacciones. Los controles internos adecuados pueden incluir:

- Mantener un sistema integral que identifique, en todo el banco, las cuentas del libro mayor utilizadas como cuentas de concentración, así como los departamentos e individuos autorizados para usar esas cuentas.
- Exigir dos firmas en los tiquetes del libro mayor.
- Prohibir a los clientes el acceso directo a las cuentas de concentración.
- Capturar las transacciones de los clientes en los estados de cuenta de los mismos.

- Prohibir que los clientes que tengan conocimiento de las cuentas de concentración o que puedan impartir instrucciones a los empleados para que éstos realicen transacciones a través de esas cuentas.
- Conservar la información adecuada relativa a transacciones e identificación de clientes.
- Asignar a una persona no relacionada con las transacciones para que se encargue de conciliar frecuentemente las cuentas.
- Establecer un proceso oportuno para solucionar discrepancias.
- Identificar los nombres de los clientes habituales.

Procedimientos de Inspección

Cuentas de concentración

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las cuentas de concentración y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las cuentas de concentración. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de cuentas de concentración del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de concentración.

3. Revise el libro mayor e identifique todas las cuentas de concentración existentes. Luego de tratar las cuentas de concentración con la gerencia y de realizar investigaciones adicionales necesarias, obtenga y revise una lista de todas las cuentas de concentración y las conciliaciones bancarias más recientes.

4. Determine si el sistema del banco para supervisar las cuentas de concentración, detectar e informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de sus actividades de cuentas de concentración, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de concentración. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Obtenga informes de actividad de cuenta relativos a las cuentas de concentración seleccionadas.
   - Evalúe la actividad y seleccione una muestra de las transacciones que pasen por diferentes cuentas de concentración para un control adicional.
   - Concéntrese en la actividad de mayor riesgo (p. ej., transferencias de fondos o compras de instrumentos monetarios) y en las transacciones provenientes de jurisdicciones de mayor riesgo.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas a las transacciones, formule una conclusión sobre la adecuación de las políticas, los procedimientos y los procesos asociados con las cuentas de concentración.

Actividades de Préstamo: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de préstamo y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Las actividades de préstamo incluyen, entre otras, bienes inmuebles,[216] financiación del comercio internacional,[217] préstamos garantizados con efectivo, tarjetas de crédito, actividades comerciales agrícolas y de particulares. En las actividades de préstamo pueden intervenir varias partes (p. ej., garantes, firmantes, mandantes o participantes del préstamo).

Factores de riesgo

El hecho de que haya varias partes involucradas puede incrementar el riesgo de lavado de dinero o financiamiento del terrorismo cuando la fuente y el uso de los fondos no son transparentes. Esta falta de transparencia puede generar oportunidades en cualquiera de las tres fases de las operaciones de lavado de dinero o estratagemas de financiamiento del terrorismo. Estas estratagemas pueden incluir lo siguiente:

- Para obtener un préstamo, una persona adquiere un certificado de depósito con fondos ilícitos.
- Los préstamos tienen un propósito ambiguo o ilegal.
- Los préstamos se realizan o se pagan a nombre de un tercero.
- El banco o el cliente intentan eliminar la evidencia escrita sobre el solicitante del préstamo y los fondos ilícitos.
- Se otorgan préstamos a personas que residen fuera de los Estados Unidos, especialmente en jurisdicciones y ubicaciones geográficas de mayor riesgo. Los préstamos también pueden incluir garantías ubicadas fuera de los Estados Unidos.

Mitigación del riesgo

Todos los préstamos se consideran cuentas para los propósitos de los reglamentos del Programa de identificación de clientes (CIP). Respecto a los préstamos que implican mayor riesgo de lavado de dinero y financiamiento del terrorismo, incluidos los préstamos

[216] La FinCEN ha publicado informes analíticos y estratégicos sobre las tendencias y los patrones relacionados con el fraude asociado a los créditos hipotecarios, así como el lavado de dinero a través de bienes inmuebles residenciales y comerciales. Consulte www.fincen.gov/news_room/rp/strategic_analytical.html.

[217] Consulte la sección del esquema principal, “Actividades de financiación del comercio internacional” en las páginas 302 a 307, como guía.

enumerados arriba, el banco debe realizar la debida diligencia de las partes relacionadas con la cuenta (p. ej., garantes, firmantes o mandantes). La debida diligencia adicional que se exige para una actividad de préstamo en particular, variará según los riesgos de BSA/AML que se presenten, pero puede incluir la verificación de referencias, la obtención de referencias de crédito, la verificación de la fuente de las garantías y la obtención de extractos de los estados financieros o de la declaración impositiva del solicitante del crédito, así como de todas o varias de las diversas partes involucradas en el préstamo.

Los bancos deben contar con políticas, procedimientos y procesos para supervisar, identificar e informar de actividades poco habituales o sospechosas. La sofisticación de los sistemas empleados para supervisar la actividad de las cuentas de préstamos debe ser acorde al tamaño y complejidad de la actividad de préstamos del banco. Por ejemplo, los bancos pueden controlar los informes de préstamos tales como pagos anticipados, cuentas morosas, fraude o préstamos garantizados con efectivo.

Procedimientos de Inspección

Actividades de préstamo

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de préstamo y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a los préstamos. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de préstamo del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de préstamos de mayor riesgo.

3. Determine si el sistema del banco para supervisar las cuentas de préstamos, detectar e informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de préstamo, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de préstamos de mayor riesgo. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta, incluidos los CIP, para asegurarse de que se haya llevado a cabo la debida diligencia adecuada y mantenido los registros adecuados.

   - Revise, según sea necesario, los antecedentes de préstamo.

   - Compare las transacciones previstas con la actividad real.

   - Determine si la actividad real es coherente con el tipo de negocio del cliente y el propósito declarado del préstamo. Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las relaciones de préstamos.

Actividades de Financiación del Comercio Internacional: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de financiación del comercio internacional y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

La financiación del comercio internacional, generalmente comprende la financiación a corto plazo para facilitar la importación y exportación de bienes. Estas operaciones pueden incluir el pago si se cumplen las exigencias documentales (p. ej., carta de crédito), o incluir únicamente el pago si el deudor originario no cumple con los términos comerciales de las transacciones (p. ej., garantías o cartas de crédito contingentes). En ambos casos, la participación del banco en la financiación del comercio internacional minimiza los riesgos de la falta de pago tanto para importadores como para exportadores. Sin embargo, el carácter de las actividades de financiación del comercio internacional, exige participación activa de varias partes en ambos extremos de la transacción. Además de la relación básica entre exportador e importador, que está en el centro de toda actividad particular de comercio internacional, pueden existir relaciones entre el exportador y los proveedores, y entre el importador y sus clientes.

Tanto el exportador como el importador pueden tener otras relaciones bancarias. Asimismo, muchas otras instituciones intermediarias financieras y no financieras pueden proporcionar servicios y canales para agilizar los documentos subyacentes y los flujos de pago asociados con las transacciones de comercio internacional. Los bancos pueden participar en la financiación del comercio internacional proporcionando financiación previa a la exportación, ayudando en el proceso de cobro, confirmando o emitiendo cartas de crédito, descontando giros y aprobaciones u ofreciendo servicios por los que se abonan honorarios, tales como brindar información sobre el país y el crédito de los compradores; entre otras alternativas. A pesar de que, en su mayoría, la financiación del comercio internacional es a corto plazo y de carácter autoliquidable, los préstamos a mediano plazo (uno a cinco años) o a largo plazo (más de cinco años) pueden utilizarse para financiar la importación y exportación de bienes de inversión como maquinarias y equipos.

En las transacciones cubiertas por cartas de crédito, los participantes pueden desempeñar los siguientes papeles:

- **Solicitante.** El comprador o la parte que solicita la emisión de una carta de crédito.
- **Banco emisor.** El banco que emite la carta de crédito en nombre del Solicitante y notifica al respecto al Beneficiario, ya sea directamente o a través de un Banco notificador. El Solicitante es cliente del Banco emisor.
- **Banco confirmador.** Generalmente en el país de origen del Beneficiario, a pedido del Banco emisor, el banco que aporta su compromiso de respetar los retiros realizados por el Beneficiario, siempre que se cumplan los términos y las condiciones de la carta de crédito.

- **Banco notificador.** El banco que notifica el crédito ante la solicitud del Banco emisor. El Banco emisor envía el crédito original al Banco notificador para que lo remita al Beneficiario. El Banco notificador autentica el crédito y notifica al respecto al Beneficiario. En una transacción que involucra una carta de crédito pueden intervenir más de un Banco notificador. El Banco notificador también puede ser un Banco confirmador.

- **Beneficiario.** El vendedor o la parte a quien se dirige la carta de crédito.

- **Negociación.** La adquisición por parte del banco designado de giros (librados en otro banco que no sea el banco designado) o documentos presentados conforme a los términos y condiciones del crédito, mediante el adelanto efectivo o el acuerdo de proporcionar un adelanto de los fondos al beneficiario antes o el mismo día hábil en que debe realizarse el reembolso al banco designado.

- **Banco designado.** El banco en el cual el crédito está disponible o cualquier banco en el caso de un crédito disponible en cualquier banco.

- **Banco aceptante.** El banco que acepta un giro, siempre y cuando el crédito exija realizar un giro. Los giros son librados en el Banco aceptante, que pone fecha y firma el instrumento.

- **Banco de descuentos.** El banco que descuenta un giro para el Beneficiario luego de que el Banco notificador lo haya aceptado. Generalmente, el Banco de descuentos es el Banco aceptante.

- **Banco de reembolso.** El banco autorizado por el Banco emisor a reembolsar al Banco pagador presentando reclamos en virtud de la carta de crédito.

- **Banco pagador.** El banco que realiza el pago al Beneficiario de la carta de crédito.

A manera de ejemplo, en un acuerdo de carta de crédito, el banco puede servir como Banco emisor y permitir a su cliente (el comprador) adquirir bienes en el país o el extranjero, o puede actuar como Banco notificador y permitir a su cliente (el exportador) vender sus artículos en el país o el extranjero. La relación entre los dos bancos puede variar y en algunos casos puede incluir cualquiera de las funciones de la lista anterior.

Factores de riesgo

El sistema del comercio internacional está sujeto a una amplia variedad de riesgos y susceptibilidades que ofrecen a las organizaciones criminales la oportunidad de lavar las ganancias provenientes de las actividades delictivas y desplazar los fondos a las organizaciones terroristas con un riesgo de detección relativamente bajo.[218] La

[218] Consulte el informe del Grupo de Acción Financiera sobre *Trade Based Money Laundering* (Lavado de dinero a través de transacciones), del 23 Junio de 2006, en www.fatf-gafi.org/dataoecd/60/25/37038272.pdf.

intervención de varias partes a ambos lados de cualquier transacción de financiación del comercio internacional puede dificultar aun más el proceso de la debida diligencia. Además, como el negocio de la financiación del comercio internacional puede depender más de documentos que otras actividades bancarias, puede ser susceptible a la falsificación de documentos, que puede estar relacionada con el lavado de dinero, el financiamiento del terrorismo o con intentos por evitar sanciones de la OFAC u otras restricciones (p. ej., restricciones de exportación, exigencias de licencias o controles).

A pesar de que los bancos deben estar alertas a las transacciones de bienes de mayor riesgo (p. ej., comercio de armas o equipos nucleares), deben tener en cuenta que los bienes pueden estar sobrevalorados o subvalorados para evadir los reglamentos AML o aduaneros, o para transferir los fondos o valores fuera de las fronteras nacionales. Por ejemplo, un importador puede pagar una alta suma de dinero con ingresos provenientes de actividades ilícitas para adquirir bienes que esencialmente carecen de valor y posteriormente son desechados. Como alternativa, los documentos del comercio internacional, como las facturas, pueden ser adulterados mediante fraude para ocultar el engaño. Las variaciones sobre este tema incluyen facturas dobles o incorrectas, envío parcial de bienes (envío incompleto) y el uso de bienes ficticios. Los fondos ilegales transferidos en dichas transacciones consecuentemente aparecen blanqueados e ingresan al terreno del comercio legítimo. Además, en muchas transacciones sospechosas de financiación del comercio internacional también media connivencia entre compradores y vendedores.

La verdadera identidad o titularidad del Solicitante puede encubrirse mediante la adopción de determinadas formas corporativas, como las compañías fantasma o las compañías testaferro emplazadas en el extranjero. La adopción de estos tipos de entidades deriva en una falta de transparencia, ocultando la identidad de la parte compradora de manera eficaz e incrementando así el riesgo de actividad de lavado de dinero y el financiamiento de actividades terroristas.

Mitigación del riesgo

Se deben practicar procedimientos responsables de debida diligencia de los clientes (CDD) para obtener una comprensión exhaustiva del negocio subyacente del cliente y las ubicaciones a las que se prestan servicios. En el proceso relacionado con la carta de crédito, los bancos deben aplicar niveles variables de debida diligencia según su papel en la transacción. Por ejemplo, los Bancos emisores deben llevar a cabo una debida diligencia suficiente con respecto a los posibles clientes antes de otorgar la carta de crédito. La debida diligencia debe incluir la obtención de suficiente información sobre los Solicitantes y Beneficiarios, que incluye su identidad, el carácter del negocio y las fuentes de los fondos. Esto puede requerir la verificación de antecedentes o la realización de investigaciones, especialmente en las jurisdicciones de mayor riesgo. Como tales, los bancos deben realizar un control exhaustivo y conocer de manera razonable a sus clientes antes de facilitar actividades relacionadas con el comercio internacional, y deben comprender exhaustivamente la documentación sobre financiación del comercio internacional. Consulte la sección del esquema general principal, “Debida diligencia de los clientes” en las páginas 69 a 71, como guía.

Del mismo modo, la orientación provista por el *Financial Action Task Force on Money Laundering* (Grupo de Acción Financiera en Contra del Lavado de Dinero; FATF) ha contribuido a establecer importantes normas concernientes a la industria y constituye un recurso para los bancos que prestan servicios de financiación del comercio internacional.[219] El Grupo Wolfsberg también ha publicado pautas y normas propuestas, concernientes a la industria, para los bancos que prestan servicios de financiación del comercio internacional.[220]

Los bancos que desempeñan otros papeles en el proceso relacionado con la carta de crédito deben realizar debida diligencias acorde con sus papeles en cada transacción. Los bancos deben tener en cuenta que, debido a la frecuencia de las transacciones en las que participan varios bancos, los Bancos emisores pueden no tener siempre relaciones corresponsales con el Banco confirmador o notificador.

En la medida de lo posible, los bancos deben revisar la documentación, no sólo para verificar el cumplimiento con las condiciones de la carta de crédito, sino también en busca de anomalías o señales de advertencia que puedan indicar actividades sospechosas o poco habituales. La documentación confiable es fundamental para identificar actividad sospechosa potencial. Al analizar las transacciones de comercio internacional a fin de detectar actividades irregulares o sospechosas, los bancos deben considerar obtener copias de los formularios oficiales de importación y exportación del gobierno extranjero o de los Estados Unidos para evaluar la confiabilidad de la documentación proporcionada.[221] Estas anomalías pueden aparecer en la documentación de envío, fijación irregular de precios evidente, licencias del gobierno (cuando se exijan) o discrepancias en la descripción de los bienes en diversos documentos. La identificación de estos elementos puede, en sí misma, no exigir la presentación de un Informe de actividades sospechosas (SAR), pero puede sugerir la necesidad de una investigación y verificación adicionales. En circunstancias donde se requiera un SAR, no se espera que el banco detenga el comercio internacional ni que interrumpa el procesamiento de la transacción. Sin embargo, se puede requerir detener la transacción para evitar una violación potencial a una sanción de la OFAC.

Con frecuencia, las transacciones de financiación de comercio internacional utilizan mensajes de la Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT, por sus siglas en inglés). Los bancos estadounidenses deben cumplir

---

[219] Consulte *Trade Based Money Laundering*, (Lavado de dinero a través de transacciones), del 23 Junio de 2006, en www.fatf-gafi.org/dataoecd/60/25/37038272.pdf.

[220] Consulte *The Wolfsberg Trade Finance Principles* (Principios de financiación del comercio internacional del Grupo Wolfsberg), de Enero de 2009, en www.wolfsberg-principles.com/pdf/WG_Trade_Finance_Principles_Final_(Jan_09).pdf.

[221] Por ejemplo, el Formulario 7501 de la Oficina de Aduanas y Protección de las Fronteras de los Estados Unidos (Sumario) (http://forms.cbp.gov/pdf/CBP_Form_7501.pdf) y el Formulario 7525-V del Departamento de Comercio de los Estados Unidos (Declaración de exportación de embarque) (www.census.gov/foreign-trade/regulations/forms/new-7525v.pdf) clasifican todas las exportaciones e importaciones estadounidenses mediante códigos de 10 dígitos combinados. (Consulte el www.census.gov/foreign-trade/faq/sb/sb0008.html como guía.)

con los reglamentos de la OFAC, y, cuando sea necesario, expedir licencias antes de entregar fondos. Los bancos deben supervisar los nombres de las partes contenidas en estos mensajes y comparar los nombres con las listas de la OFAC. Consulte la sección del esquema general principal, "Oficina de Control de Activos Extranjeros", en las páginas 165 a 175, como guía. Los bancos con un gran volumen de mensajes de SWIFT deben determinar si sus actividades de supervisión son adecuados para detectar actividades sospechosas, especialmente si el mecanismo de supervisión no es automatizado. Consulte la sección del esquema general principal "Informes de actividades sospechosas", en las páginas 73 a 89, y la sección del esquema general ampliado "Transferencias de Fondos", en las páginas 237 a 244, como guía.

Las políticas, los procedimientos y los procesos deben, asimismo, exigir un control exhaustivo de toda la documentación aplicable a la actividad de financiación de comercio internacional (por ejemplo, declaraciones aduaneras, documentos del comercio internacional, facturas, etc.), para que el banco sea capaz de supervisar e informar acerca de actividades poco habituales o sospechosas, en función del papel que desempeña en el proceso relacionado con la carta de crédito. La sofisticación del proceso de control de la documentación y los sistemas para la información de gestión (MIS) deben ser acordes al tamaño y la complejidad de la cartera de financiación del comercio internacional del banco y su papel en el proceso relacionado con la carta de crédito. Además de los filtros de la OFAC, el proceso de supervisión debe permitir un escrutinio mayor de:

- Envíos de artículos que no se correspondan con el carácter del negocio del cliente (p. ej., una compañía siderúrgica que comienza a comerciar productos de papel, o una compañía de tecnología de información que comienza a comerciar productos farmacéuticos en grandes cantidades.
- Clientes que realicen negocios en jurisdicciones de mayor riesgo.
- Clientes que envíen artículos a través de jurisdicciones de mayor riesgo, incluido el tránsito por países no cooperantes.
- Clientes que participen en actividades de mayor riesgo potencial, incluidas las actividades que puedan están sujetas a restricciones de importación y exportación (p. ej., equipo para organizaciones policiales o militares de gobiernos extranjeros, armas, municiones, mezclas químicas, artículos clasificados de defensa, información técnica confidencial, materiales nucleares, piedras preciosas o determinados recursos naturales tales como metales, mineral metalífero y petróleo crudo).
- Evidente fijación irregular de precios en bienes y servicios.
- Tergiversación evidente de la cantidad o el tipo de bienes importados o exportados.
- El fraccionamiento de las transacciones que parezca innecesariamente complejo y diseñado para disimular el verdadero carácter de la transacción.
- Los casos en los cuales los clientes efectúen pagos de lo recaudado a un tercero no relacionado.

- Ubicaciones de envío o descripciones de bienes que no sean consistentes con la carta de crédito.

- Cartas de crédito significativamente enmendadas sin una justificación razonable o cambios de beneficiario o ubicación de pago. Cualquier cambio en los nombres de las partes debe promover un control adicional de la OFAC.

El 18 de Febrero de 2010, la FinCEN publicó una carta informativa a fin de instruir y asistir a la industria financiera con respecto a la presentación de informes sobre presuntos casos de lavado de dinero a través de transacciones. Este documento comprende ejemplos de "señales de advertencia" en función de las actividades reportadas en los SAR, que tanto la FinCEN como las autoridades a cargo del orden público consideran podrían indicar lavado de dinero a través de transacciones. A fin de colaborar con las autoridades de aplicación de la ley en su esfuerzo por detectar las actividades de lavado de dinero a través de transacciones (TBML) y cambio de "pesos" en el mercado negro (BMPE), en la carta informativa, la FinCEN solicita a las instituciones financieras que marquen la casilla correspondiente en la sección Información sobre actividades sospechosas del formulario SAR e incluyan la abreviación TBML o BMPE en la sección de descripción de dicho formulario. La carta informativa está disponible en www.fincen.gov.

A menos que el comportamiento del cliente o la documentación de la transacción sean poco habitual, no se debe exigir que el banco dedique tiempo o esfuerzo indebido controlando toda la información. Los ejemplos anteriores, especialmente en lo relativo al Banco emisor, pueden estar incluidos como parte de su proceso de CDD de rutina. Los bancos con programas de CDD sólidos, pueden llegar a la conclusión de que las transacciones individuales requieren un menor control, como resultado del conocimiento exhaustivo que tiene el banco de las actividades del cliente.

Procedimientos de Inspección

Actividades de financiación del comercio internacional

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de financiación del comercio internacional y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las actividades de financiación del comercio internacional. Evalúe la aptitud de las políticas, los procedimientos y los procesos que rigen las actividades relacionadas con la financiación del comercio internacional y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Evalúe la aptitud de la información de debida diligencia que el banco obtiene para los archivos del cliente. Determine si el banco dispone de procesos para obtener información al momento de la apertura de la cuenta, además de garantizar que se mantenga la información actualizada del cliente.

3. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz la cartera de financiación del comercio internacional para detectar actividades sospechosas o poco habituales, particularmente aquellas que impongan un mayor riesgo de lavado de dinero.

4. Determine si el sistema del banco para supervisar las actividades de financiación del comercio internacional, detectar e informar sobre actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de su cartera de financiación del comercio internacional, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de financiación del comercio internacional. A partir de la muestra seleccionada, revise la documentación de debida diligencia de los clientes para determinar si la información es acorde al riesgo del cliente. Identifique cualquier actividad sospechosa o poco habitual.

7. Verifique si el banco supervisa la cartera de financiación del comercio internacional para detectar tanto posibles violaciones a la OFAC como patrones de transacciones poco habituales, y si registra los resultados de cualquier tipo de debida diligencia.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las actividades de financiación del comercio internacional.

Banca Privada: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de banca privada y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia. Esta sección amplía la revisión principal de las exigencias normativas y legales de la banca privada para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

Las actividades de la banca privada se definen generalmente como aquellas en que se prestan servicios personalizados a clientes de mayor valor neto (p. ej., planificación del patrimonio, asesoría financiera, préstamos, administración de inversiones, pago de facturas, remisión de correo y mantenimiento de una residencia). La banca privada se ha convertido en un rubro de actividad comercial cada vez más importante para organizaciones bancarias importantes y diversas, así como una mejor fuente de ingresos de honorarios .

Los bancos estadounidenses pueden gestionar las relaciones asociadas con la banca privada, tanto para clientes nacionales como internacionales. Por lo general, los umbrales de servicio de banca privada se basan en la cantidad de activos que se gestionan y en la necesidad de productos o servicios específicos (p. ej., administración de bienes inmuebles, supervisión detallada de empresas, administración de dinero). Los honorarios que se cobran normalmente dependen del umbral de los activos, y del uso de productos y servicios específicos.

Las estrategias de banca privada por lo general se estructuran con un punto de contacto central (es decir, el gerente de relaciones) que actúa de enlace entre el cliente y el banco, y facilita la utilización por parte del cliente de los servicios y productos financieros del banco. El Apéndice N (“Banca privada: estructura común”) proporciona un ejemplo de una estructura típica de banca privada e ilustra la relación entre el cliente y el gerente de relaciones. Los productos y servicios típicos de la relación asociada con la banca privada incluyen los siguientes:

- Administración de dinero en efectivo (p. ej., cuentas corrientes, privilegio de giro en descubierto, barridos de efectivo y servicios de pago de facturas).
- Transferencias de fondos.
- Gestión de activos (p. ej., fideicomisos, asesoría sobre inversiones, administración de inversiones y servicios de custodia e intermediación).[222]

[222] Como guía, consulte el esquema general ampliado y procedimientos de inspección, “Servicios fiduciarios y de gestión de activos”, en las páginas 318 a 322 y 323 a 324, respectivamente.

- Facilitación de entidades instaladas en el exterior y compañías fantasma (p. ej., Compañías de inversión privada [PIC], corporaciones comerciales internacionales [IBC] y fideicomisos).[223]
- Servicios de préstamos (p. ej., hipotecarios, vía tarjetas de crédito, personales, vía cartas de crédito).
- Servicios de planificación financiera incluida la planificación tributaria y patrimonial.
- Servicios de custodia.
- Otros servicios según se requieran (p. ej., servicios de correo).

La privacidad y confidencialidad son elementos importantes en las relaciones asociadas con la banca privada. Aunque los clientes pueden elegir los servicios de banca privada simplemente para gestionar sus activos, puede suceder que también busquen un refugio confidencial, seguro y legítimo para su capital. Cuando actúan como fiduciarios, los bancos tienen obligaciones legales, contractuales y éticas que mantener.

Factores de riesgo

Los servicios de banca privada pueden ser vulnerables a las estratagemas de lavado de dinero y en el pasado los procesos judiciales por lavado de dinero han demostrado esa susceptibilidad. En *Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities* (Banca privada y lavado de dinero: estudio de caso sobre oportunidades y susceptibilidades)[224], del Subcomité Permanente de Investigaciones de 1999, se describieron parcialmente las siguientes susceptibilidades con respecto al lavado de dinero:

- Banqueros privados actuando como defensores de los clientes.
- Clientes poderosos, incluyendo personalidades sujetas a exposición política, industriales y artistas.
- Cultura de confidencialidad y la utilización de jurisdicciones donde se aplica el secreto o compañías fantasma.[225]
- Cultura de banca privada con controles internos laxos.
- Carácter competitivo del negocio.
- Potencial de beneficios significativos para el banco.

---

[223] Como guía, consulte el esquema general ampliado y procedimientos de inspección, "Entidades comerciales (nacionales y extranjeras)", en las páginas 357 a 363 y 364 a 365, respectivamente.

[224] Consulte frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_senate_hearings&docid=f:61699.pdf.

[225] Consulte la sección del esquema general ampliado, "Entidades comerciales (nacionales y extranjeras)", en las páginas 357 a 363, como guía.

Mitigación del riesgo

Contar con políticas, procedimientos y procesos eficaces puede ayudar a los bancos a no convertirse en medios o víctimas del lavado de dinero, la financiación del terrorismo y otros delitos financieros que se cometen a través de las relaciones asociadas con la banca privada. La sección del esquema general principal "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", de la páginas 145 a 150, contiene información adicional relacionada con el análisis de riesgos y la debida diligencia. En último término, las actividades ilícitas realizadas a través de la unidad de banca privada pueden ocasionar costos financieros altos y riesgos que pueden afectar la reputación del banco. El impacto financiero puede incluir sanciones y multas regulatorias, gastos ocasionados por litigios, pérdida de negocios, reducción en la liquidez, confiscaciones y congelamiento de activos, pérdida de préstamos y gastos de reparaciones.

Análisis de riesgos de clientes

Los bancos deben analizar los riesgos que plantean sus actividades de banca privada en función del campo de aplicación de las operaciones y la complejidad las relaciones con sus clientes. La gerencia debe establecer un perfil de riesgo de cada cliente, que servirá para fijar prioridades en los recursos de supervisión y para la supervisión continua de las actividades de la relación. Se deben tomar en cuenta los siguientes factores al identificar las características del riesgo de los clientes de la banca privada:

- **Origen de la riqueza y carácter del negocio del cliente.** La fuente de la riqueza del cliente, el carácter del negocio del cliente y el grado en que sus antecedentes comerciales plantean un mayor riesgo de lavado de dinero y financiamiento del terrorismo. Estos factores deben tenerse en cuenta para las cuentas de banca privada abiertas para personalidades sujetas a exposición política (PEP).[226]

- **Propósito y actividad prevista.** El tamaño, el propósito, los tipos de cuentas, los productos y los servicios involucrados en la relación, y la actividad prevista de la cuenta.

- **Relación.** El carácter y duración de la relación del banco (incluidas las relaciones con las filiales) con el cliente de banca privada.

- **Estructura corporativa del cliente.** Tipo de estructura corporativa (p. ej., IBC, compañías fantasmas [nacionales o internacionales] o PIC).

- **Jurisdicción y ubicación geográfica.** Ubicación geográfica del domicilio del cliente de banca privada y de su negocio (nacional o internacional). En el control se debe tener en cuenta el grado en que la respectiva jurisdicción es reconocida internacionalmente por presentar un mayor riesgo de lavado de dinero o, por el contrario, por contar con normas AML firmes.

[226] Consulte la sección del esquema general principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 145 a 150; y la sección del esquema general ampliado, "Personalidades sujetas a exposición política", en las páginas 329 a 333, como guía.

- **Información pública.** Información conocida o razonablemente disponible al banco acerca del cliente de banca privada. El campo de aplicación y la profundidad de este control deben depender del carácter de la relación y de los riesgos planteados.

Debida diligencia de los clientes

La CDD es fundamental al momento de establecer cualquier relación con ellos, y es vital respecto a los clientes de la banca privada.[227] Los bancos deben tomar medidas razonables para establecer la identidad de sus clientes de la banca privada y, según sea pertinente, de los usufructuarios de las cuentas. La debida diligencia adecuada variará según los factores de riesgo identificados anteriormente. Las políticas, los procedimientos y los procesos deben definir la CDD aceptable para los distintos tipos de productos (p. ej., PIC), servicios y titulares de la cuenta. Como la debida diligencia es un proceso continuo, un banco debe tomar medidas para garantizar que los perfiles de cuenta sean actuales y la supervisión se establezca en función del riesgo. Los bancos deben tener en cuenta si los perfiles de riesgo deben ajustarse o la actividad sospechosa debe informarse cuando ésta no sea coherente con el perfil.

En relación con el CIP, no se exige que el banco revise las cuentas de banca privada para verificar la identidad de los beneficiarios; por el contrario, sólo se exige que verifique la identidad del titular de la cuenta designado. No obstante, la reglamentación del CIP también determina que, en función del análisis de riesgos del banco de una nueva cuenta abierta por un cliente que no es una persona física (p. ej., cuentas de la banca privada abiertas para una PIC), es posible que el banco deba "obtener información sobre" las personas físicas con autoridad o control sobre dicha cuenta, incluidos los firmantes, para verificar la identidad del cliente[228] y determinar si la cuenta se mantiene para ciudadanos no estadounidenses.[229]

Antes de abrir cuentas, los bancos deben recopilar la siguiente información de los clientes de la banca privada:

- Propósito de la cuenta.
- Tipo de productos y servicios que se usarán.
- Actividad prevista de la cuenta.
- Descripción y antecedentes de la fuente de la riqueza del cliente.

---

[227] La sección 312 de la Ley PATRIOTA de los EE. UU. exige que se establezcan políticas, procedimientos y procesos de debida diligencia de las cuentas de banca privada para ciudadanos no estadounidenses. Consulte la sección del esquema general principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 145 a 150, como guía.

[228] 31 CFR 103.121(b)(2)(ii)(C).

[229] Consulte los procedimientos de inspección de la sección principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 151 a 153, como guía.

- El valor estimado del patrimonio neto del cliente, incluidos los estados financieros.
- La fuente actual de los fondos de la cuenta.
- Referencias u otra información para confirmar la reputación del cliente.

Acciones al portador

Algunas compañías fantasmas expiden acciones al portador (es decir, se concede la propiedad a través de acciones al portador, lo que permite que se transfiera la propiedad de la corporación simplemente mediante la transferencia de la posesión física de las acciones). Para mitigar el riesgo, las compañías fantasmas que expiden acciones al portador pueden, por ejemplo, mantener el control de las acciones al portador, encomendar las acciones a un tercero independiente confiable o exigir una certificación periódica de la propiedad. Los bancos deben analizar los riesgos que estas relaciones plantean y determinar los controles adecuados. Por ejemplo, en la mayoría de los casos los bancos deberían optar por mantener (o solicitar a un tercero que mantenga) las acciones al portador de los clientes. En algunos casos poco frecuentes que implican un riesgo menor, es posible que a los bancos les resulte eficaz recertificar periódicamente el usufructo de los clientes conocidos o antiguos. Un firme programa de CDD consiste en un control subyacente eficaz a través del cual los bancos pueden determinar el carácter, el propósito y el uso previsto de las compañías fantasmas, y aplicar normas adecuadas en cuanto a la documentación y supervisión.

Supervisión de la junta directiva y la alta gerencia

La supervisión activa de la junta directiva y la alta gerencia de las actividades de banca privada y la creación de una cultura de supervisión corporativa adecuada son elementos esenciales de una gestión de riesgos y un entorno de control responsables. El propósito y los objetivos de las actividades de banca privada de la organización deben ser identificados y comunicados claramente por la junta y la alta gerencia. Objetivos y metas bien desarrollados deben describir el tipo de clientela en términos de valor neto mínimo, activos invertibles y tipos de productos y servicios que se solicitan. Asimismo, deben también delimitar específicamente los tipos de clientes que el banco aceptará y no aceptará y deben establecer los niveles de autorización adecuados para la aceptación de nuevos clientes. La junta y la alta gerencia también deben participar activamente en el establecimiento de metas de control y gestión de riesgos de las actividades de banca privada, incluidos controles eficaces de auditoría y cumplimiento. Cada banco debe garantizar que sus políticas, procedimientos y procesos para llevar a cabo actividades de banca privada se evalúen y actualicen regularmente, así como también que se delineen claramente los papeles y las responsabilidades.

Los planes de compensación de empleados a menudo se basan en la cantidad de nuevas cuentas establecidas o en el aumento de los activos gestionados. La junta y la alta gerencia deben garantizar que los planes de compensación no incentiven a los empleados a ignorar los procedimientos de debida diligencia y apertura de cuentas adecuados o las posibles actividades sospechosas relacionadas con la cuenta. Los procedimientos que exigen diversos niveles de aprobación para aceptar nuevas cuentas de banca privada pueden minimizar dichas posibilidades.

Dado el carácter delicado de la banca privada y la responsabilidad potencial asociada con ella, los bancos deben investigar exhaustivamente los antecedentes de los gerentes de relaciones asociadas con la banca privada recién contratados. Durante el período de empleo, cualquier indicio de actividad inadecuada debe ser investigado prontamente por el banco.

Además, cuando los gerentes de relaciones asociadas con la banca privada cambian de empleador, a menudo sus clientes se van con ellos. Los bancos tienen la misma responsabilidad potencial respecto a los clientes existentes de funcionarios recién contratados como respecto a cualquier relación nueva asociada con la banca privada. Por lo tanto, dichas cuentas deben revisarse sin demora, utilizando los procedimientos del banco para establecer nuevas relaciones asociadas con las cuentas.

Los sistemas para la información de gestión (MIS) y sus informes también son importantes para supervisar y gestionar de manera eficaz los riesgos y las relaciones asociadas con la banca privada. La junta y la alta gerencia deben controlar los informes de compensación del gerente de relaciones, los informes de comparación de objetivo o presupuesto y los informes de gestión de riesgos aplicables. Los informes de MIS de banqueros privados deben permitir al gerente de relaciones ver y gestionar la totalidad de la relaciones con el cliente y cualquier otra relacionada.

Procedimientos de Inspección

Banca privada

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de banca privada y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia. Esta sección amplía la revisión principal de las exigencias normativas y legales de la banca privada para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las actividades de banca privada. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de banca privada del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los informes de los MIS (p. ej., informes sobre acumulación de los clientes, excepciones a las políticas y documentación faltante, clasificación de riesgos de clientes, actividad poco habitual de cuentas y concentración de clientes) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con la banca privada, particularmente aquellas que planteen un alto riesgo de lavado de dinero.

3. Determine si el sistema del banco para supervisar las relaciones asociadas con la banca privada, detectar e informar sobre actividades sospechosas, es adecuado a su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con los clientes.

4. Revise el programa de compensación de la banca privada. Determine si incluye medidas cualitativas que se proporcionen a los empleados para cumplir con las exigencias de supervisión y elaboración de informes de actividades sospechosas y apertura de cuentas.

5. Revise el programa de supervisión que el banco utiliza para examinar la condición financiera personal del gerente de relaciones de la banca privada y para detectar cualquier actividad inapropiada.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus actividades de banca privada, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de banca privada. La muestra debe incluir los siguientes tipos de cuentas:

   - Personalidades sujetas a exposición política (PEP).

- Compañías de inversión privada (PIC), corporaciones comerciales internacionales (IBC) y compañías fantasmas.
- Entidades instaladas en el exterior.
- Negocios que manejan un alto flujo de efectivo.
- Compañías importadoras y exportadoras.
- Clientes que realizan negocios en una ubicación geográfica de mayor riesgo o que provienen de dicha ubicación geográfica.
- Clientes incluidos en informes de supervisión de actividades poco habituales.
- Clientes que efectúan transacciones de grandes volúmenes en dólares y transferencias de fondos frecuentes.

8. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:
   - Revise la documentación de apertura de la cuenta e información de debida diligencia continua.
   - Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones.
   - Compare las transacciones previstas con la actividad real.
   - Determine si la actividad real es coherente con el tipo de negocio del cliente.
   - Identifique cualquier actividad sospechosa o poco habitual.
9. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos con respecto a las relaciones asociadas con la banca privada.

Servicios Fiduciarios y de Gestión de Activos: Esquema General

Objetivo: *Evaluar la aptitud de las políticas, los procedimientos y los procesos del banco, y los sistemas para gestionar los riesgos asociados con los servicios fiduciarios y de gestión de activos,[230] así como la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Las cuentas fiduciarias[231] generalmente se definen como un acuerdo legal en el cual una parte (el fideicomitente u otorgante) transfiere la propiedad de los activos a una persona o banco (el fiduciario) para que lo conserve o utilice en beneficio de terceros. Estos acuerdos incluyen las categorías amplias de cuentas supervisadas por tribunales (p. ej., albaceazgo o custodias), fideicomisos personales (p. ej., fideicomisos establecidos en vida, fideicomisos testamentarios y fideicomiso benéfico), y los fideicomisos corporativos (p. ej., administración fiduciaria de bonos).

A diferencia de los acuerdos fiduciarios, las cuentas de agencia se establecen por contrato y se rigen por el derecho contractual. Los activos están sujetos a los términos del contrato y el título o la propiedad no se transfieren al banco en calidad de agente. Las cuentas de agencia incluyen las relaciones de custodia, plica, administración de inversiones,[232] y que impliquen cajas de seguridad. Los productos y servicios agenciados pueden ofrecerse en un departamento fiduciario tradicional o a través de otros departamentos del banco.

Programa de identificación de clientes

Las normas del CIP, vigentes a partir del 1.º de Octubre de 2003, son aplicables básicamente a todas las cuentas bancarias abiertas después de esa fecha. La definición de "cuenta" establecida en la norma CIP incluye las relaciones de administración de efectivo, de custodia, fiduciarias y que impliquen cajas de seguridad. Sin embargo, la norma CIP excluye las cuentas de beneficios sociales de empleados establecidas conforme a la Ley de Seguridad de los Ingresos para el Retiro de los Empleados de 1974 (ERISA, por sus siglas en inglés).

---

[230] Las cuentas de administración de activos pueden ser cuentas fiduciarias o de agencia, y son gestionadas por el banco.

[231] La Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro utilizan el término más amplio "relación de carácter fiduciario" en vez de "fideicomiso". En la relación de carácter fiduciario intervienen un fiduciario, un albacea, un administrador, un registrador de acciones y bonos, un agente de transferencia, un depositario, cesionario, un receptor o un curador actuando bajo la ley uniforme de donaciones a menores; un asesor de inversiones, si el banco recibe honorarios por su asesoría sobre inversiones; y cualquier relación bajo la cual el banco posea la capacidad de decidir discrecionalmente sobre inversiones en nombre de otro (12 CFR 9-2(e) y 12 CFR 550.30).

[232] Para los propósitos de los bancos nacionales y las asociaciones de ahorro reguladas por la Oficina de Supervisión de Instituciones de Ahorro, ciertas actividades de administración de inversiones, como proporcionar asesoría de inversión a cambio de honorarios, son de naturaleza "fiduciaria".

A los efectos del CIP, no se exige que un banco revise las cuentas fiduciarias, de depósito en plica o similares para verificar la identidad de los beneficiarios, en cambio, sólo debe verificar la identidad del titular de la cuenta designado (el fideicomiso). En el caso de las cuentas fiduciarias, el cliente es el fideicomiso, sea o no el banco el fiduciario en el fideicomiso. Sin embargo, la norma CIP también estipula que, en función del análisis realizado por el banco del riesgo que implica una cuenta nueva abierta por un cliente que no es persona física, el banco deberá "obtener información acerca" de las personas que tienen el control o la autoridad sobre la cuenta, incluidos los firmantes, para verificar la identidad del cliente.[233] Por ejemplo, en ciertas circunstancias relativas a fideicomisos revocables, el banco deberá obtener información sobre el constituyente, otorgante, fideicomitente u otras personas con autoridad para dar órdenes al fiduciario, y que por lo tanto tienen autoridad o control sobre la cuenta, para establecer la verdadera identidad del cliente.

En el caso de las cuentas de depósito en plica, si un banco abre una cuenta a nombre de un tercero, como un agente inmobiliario, que actúa como agente de depósito en plica, entonces el cliente del banco es el agente de depósito en plica. Si el banco es el agente de depósito en plica, entonces la persona que establece la cuenta es el cliente del banco. Por ejemplo, si un comprador de bienes inmuebles abre directamente una cuenta de depósito en plica y deposita fondos a ser pagados al vendedor una vez satisfechas ciertas condiciones específicas, el cliente del banco será el comprador. Además, si una compañía en formación establece una cuenta de depósito en plica para que los inversionistas depositen sus aportes mientras está pendiente el monto mínimo requerido, el cliente del banco será la compañía en formación (o si aún no tiene personalidad jurídica, la persona que abre la cuenta en su nombre). Sin embargo, la norma CIP también estipula que, en función del análisis de riesgo realizado por el banco de una nueva cuenta abierta por un cliente que no es persona física, es posible que el banco deba "obtener información acerca" de las personas que tienen autoridad o control sobre dicha cuenta, incluidos los firmantes, para verificar la identidad del cliente.[234]

Factores de riesgo

Las cuentas de gestión fiduciaria y de activos, incluidas las relaciones con agencias, presentan riesgos relativos a BSA/AML similares a los que presenta el recibo de depósitos, los préstamos y otras actividades bancarias tradicionales. Las preocupaciones se deben principalmente a las estructuras de relación únicas que se presentan cuando los bancos manejan actividades fiduciarias y agenciadas, como las siguientes:

- Cuentas personales y cuentas supervisadas por tribunales.
- Cuentas fiduciarias generadas en el departamento de banca privada.
- Cuentas de administración de activos y asesoría sobre inversiones.

---

[233] Consulte 31 CFR 103.121(b)(2)(ii)(C).

[234] Id.

- Cuentas nacionales y mundiales de custodia.
- Préstamos en valores.
- Cuentas de beneficios sociales y de retiro de empleados.
- Cuentas fiduciarias corporativas.
- Cuentas de agentes de transferencia.
- Otros rubros de actividad comercial relacionados.

Como en cualquier otra relación de cuenta, el riesgo de lavado de dinero puede presentarse en las actividades de gestión fiduciaria y de activos. Cuando existe uso indebido de las cuentas de gestión fiduciaria y de activos, se puede ocultar el origen y el uso de los fondos, así como la identidad de los usufructuarios y propietarios legales. Los clientes y usufructuarios de las cuentas pueden tratar de permanecer anónimos para transferir fondos ilícitos o evitar escrutinios. Por ejemplo, los clientes pueden buscar cierto nivel de anonimato creando Compañías de inversión privada (PIC),[235] fideicomisos en el exterior u otras entidades de inversión que oculten la propiedad real o el derecho de usufructo del fideicomiso.

Mitigación del riesgo

La gerencia debe establecer políticas, procedimientos y procesos que le permitan al banco identificar relaciones y circunstancias de cuentas poco habituales, activos y origen de activos cuestionables y otras áreas potenciales de riesgo (p. ej., cuentas en el exterior, PIC, planes de protección patrimonial en el extranjero (APT, por sus siglas en inglés),[236] cuentas de agencia y beneficiarios no identificados). A pesar de que la mayoría de cuentas de gestión fiduciaria y de activos tradicionales no necesitarán una EDD, la gerencia debe estar alerta respecto a aquellas situaciones que requieran control o investigación adicional.

Comparación de los clientes con las listas

El banco debe conservar la información del CIP exigida y realizar la comparación por única vez de los nombres de las cuentas fiduciarias con las solicitudes de búsqueda de la sección 314(a). El banco también debe poder identificar a los clientes que puedan ser personalidades sujetas a exposición política (PEP), que negocien o se localicen en jurisdicciones designadas como “de interés principal con respecto al lavado de dinero”

[235] Consulte la sección del esquema general ampliado, “Entidades comerciales (nacionales y extranjeras)”, en las páginas 357 a 363, para obtener orientación adicional sobre las PIC.

[236] Las APT son una forma especial de fideicomiso irrevocable, por lo general creadas (establecidas) fuera del país con el fin principal de preservar y proteger una parte de la riqueza de una persona contra los acreedores. La titularidad del activo se transfiere a una persona denominada el fiduciario. Las APT por lo general son neutrales tributariamente y su función última es la de brindar sustento a los beneficiarios.

bajo la sección 311 de la Ley PATRIOTA de los EE. UU. o que concuerden con las listas de la OFAC.[237] Como práctica responsable, el banco también debe determinar la identidad de las demás partes que puedan tener control sobre la cuenta, como los otorgantes fiduciarios conjuntos. Consulte la sección del esquema general principal, "Intercambio de información", en las páginas 108 a 114, y la sección del esquema general ampliado, "Personalidades sujetas a exposición política", en las páginas 329 a 333, como guía.

Circunstancias que requieren una debida diligencia especial

La gerencia debe analizar el riesgo de una cuenta en función de una variedad de factores, que pueden incluir:

- El tipo de cuenta de agencia o fiduciaria y su tamaño.
- Los tipos y la frecuencia de las transacciones.
- El país de residencia de los titulares o beneficiarios, o el país en el que se establecieron, o la fuente de los fondos.
- Las cuentas y transacciones que no sean habituales o acostumbradas para el cliente o el banco.
- Deben establecerse procedimientos estrictos de documentación, verificación y supervisión de transacciones para las cuentas que la gerencia considere de mayor riesgo. Generalmente, las cuentas de beneficios sociales de los empleados y las cuentas supervisadas por tribunales están entre las de más bajo riesgo BSA/AML.

Los siguientes constituyen ejemplos de situaciones en las cuales posiblemente sea adecuado llevar a cabo la debida diligencia especial:

- Al iniciar el banco una relación con un cliente nuevo.
- Los usufructuarios o beneficiarios de la cuenta residen en una jurisdicción extranjera, o el fideicomiso o sus mecanismos de obtención de fondos están establecidos en el exterior.
- Los activos o las transacciones son inusuales para el tipo y carácter de cliente.
- El tipo de cuenta, el tamaño, los activos o las transacciones son atípicas para el banco.

---

[237] La gerencia y los inspectores deben ser conscientes de que la comparación con las listas de la OFAC no es una exigencia de la BSA. Sin embargo, dado que los sistemas fiduciarios generalmente son diferentes a los sistemas bancarios y están separados de los mismos, esta verificación en el sistema bancario no basta para garantizar que también se lleven a cabo en el departamento de gestión fiduciaria y administración de activos. Por otra parte, la posición de la OFAC es que el beneficiario de una cuenta tiene intereses contingentes o futuros en los fondos de la cuenta y, de manera coherente con el perfil de riesgo del banco, se debe realizar una revisión de los beneficiarios para asegurar el cumplimiento OFAC. Consulte la sección del esquema general principal, "Oficina de Control de Activos Extranjeros", en las páginas 165 a 175, como guía.

- Las transferencias de fondos internacionales se realizan particularmente a través de fuentes de fondos ubicadas en el exterior.
- Las cuentas se financian con activos fácilmente trasladables, como piedras preciosas, metales preciosos, monedas, obras de arte, estampillas poco comunes o instrumentos negociables.
- Se mantienen cuentas o relaciones en las que la identidad de los usufructuarios o beneficiarios o la fuente de los fondos son desconocidos o no se pueden establecer con facilidad.
- Las cuentas benefician a entidades de beneficencia u otras organizaciones no gubernamentales (ONG) que pueden ser utilizadas como conducto para realizar actividades ilegales.[238]
- Cuentas fiduciarias de abogados con rendimiento de interés (IOLTA) que mantienen y procesan montos significativos en dólares.
- Activos de las cuentas que incluyen PIC.
- En las cuentas o transacciones son parte personalidades sujetas a exposición política (PEP).

[238] Como guía adicional, consulte la sección del esquema general ampliado, "Organizaciones no gubernamentales y entidades de beneficencia", en las páginas 353 y 354.

Procedimientos de Inspección

Servicios de gestión de fideicomisos y de activos

Objetivo: *Evaluar la aptitud de las políticas, los procedimientos y los procesos del banco, y los sistemas para gestionar los riesgos asociados con los servicios fiduciarios y de gestión de activos,[239] así como la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Si esta es una inspección de fideicomisos independiente, consulte los procedimientos de inspección de la sección principal "Campo de aplicación y planificación", en las páginas 20 a 22, como guía exhaustiva del campo de aplicación de la inspección BSA/AML. En ese caso, la inspección puede necesitar cubrir áreas adicionales, que incluyen la capacitación, el funcionario de cumplimiento de la BSA, el control independiente y los elementos de seguimiento.

1. Revise las políticas, los procedimientos y los procesos con respecto a los servicios de gestión de fideicomisos y de activos. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de servicios de gestión de fideicomisos y de activos del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Revise los procedimientos del banco para reunir la información de identificación adicional, cuando sea necesario, sobre el constituyente, el otorgante, el fiduciario, u otras personas con autoridad para instruir al fiduciario, y que por lo tanto ejerzan autoridad o control sobre la cuenta, con el objetivo de establecer la verdadera identidad del cliente.

3. De un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con la gestión de activos y fideicomisos, particularmente aquellas que planteen un mayor riesgo de lavado de dinero.

4. Determine si el banco incluye las relaciones de gestión de fideicomisos y de activos en todo el banco o, según corresponda, en los sistemas de acumulación BSA/AML de toda la institución.

5. Determine si el sistema del banco para supervisar las relaciones asociadas con la gestión de fideicomisos y de activos, detectar e informar actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de Control de Activos Extranjeros", en las páginas 176 a 178, como guía.

---

[239] Las cuentas de administración de activos pueden ser cuentas fiduciarias o de agencia, y son gestionadas por el banco.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus relaciones con la gestión de fideicomisos y de activos, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las relaciones con los servicios de gestión de fideicomisos y de activos de mayor riesgo. Incluya las relaciones con los otorgantes y los fiduciarios conjuntos, si tienen autoridad o control, así como los activos de mayor riesgo como las Compañías de inversión privada (PIC) o los planes de protección patrimonial en el extranjero. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta, incluidos los CIP, para asegurarse de que se haya llevado a cabo la debida diligencia adecuada y mantenido los registros adecuados.
   - Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones. Compare las transacciones previstas con la actividad real.
   - Determine si la actividad real es coherente con el tipo de negocio del cliente y el propósito declarado de la cuenta.
   - Identifique cualquier actividad sospechosa o poco habitual.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las relaciones de gestión de fideicomisos y de activos.

ESQUEMA GENERAL AMPLIADO Y PROCEDIMIENTOS PARA PERSONAS Y ENTIDADES

Extranjeros no Residentes y Ciudadanos Extranjeros: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transacciones que involucren cuentas mantenidas por extranjeros no residentes (NRA) y ciudadanos extranjeros, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Los ciudadanos extranjeros que mantienen relaciones con los bancos estadounidenses pueden dividirse en dos categorías: extranjeros residentes y extranjeros no residentes. Por definición, un NRA es una persona que no tiene ciudadanía estadounidense que: (i) no es residente permanente legal de los Estados Unidos durante el año calendario y no cumple con la prueba de presencia física,[240] o (ii) no se le ha otorgado una tarjeta de recibo de registro como extranjero, también conocida como tarjeta verde. El Servicio de Impuestos Internos (IRS) determina las responsabilidades tributarias del ciudadano extranjero y oficialmente lo define como "residente" o "no residente".

Aunque los NRA no sean residentes permanentes, pueden tener una necesidad legítima de establecer una relación de cuenta con un banco estadounidense. Los NRA utilizan productos y servicios del banco para resguardar activos (p. ej., para mitigar pérdidas debidas a fluctuaciones en la tasa de cambio), expandir negocios e inversión. El monto de los depósitos de NRA colocado en el sistema bancario estadounidense se ha calculado entre cientos de miles de millones de dólares a aproximadamente un trillón de dólares. Aun en el extremo más bajo del rango, la magnitud es significativa, tanto para el sistema bancario estadounidense como para la economía.

---

[240] Un ciudadano extranjero es un extranjero residente si está físicamente presente en los Estados Unidos durante al menos 31 días del año calendario actual y está presente 183 días o más según el siguiente conteo: todos los días en que estuvo presente durante el año actual, más un tercio de los días que estuvo presente durante el año anterior, más un sexto de los días en que estuvo presente el año anterior a ése. Algunos días de presencia no se tienen en cuenta, tales como (i) los días transcurridos en los Estados Unidos debido una enfermedad que haya evolucionado mientras el extranjero se encontraba en los Estados Unidos, impidiéndole irse, (ii) los días que los viajeros frecuentes transcurren en los Estados Unidos trasladándose hacia o desde Canadá o México, (iii) un día de menos de 24 horas transcurrido en tránsito entre dos localidades fuera de los Estados Unidos, y (iv) los días en que el extranjero era persona exenta. El individuo es considerado extranjero residente para los fines de los impuestos federales e impuestos laborales desde el primer día de su presencia física en los Estados Unidos en el año que se cumple con la prueba. Consulte el sitio Web del Servicio de Impuestos Internos en www.irs.gov.

Factores de riesgo

Puede resultar más difícil para los bancos verificar y autenticar la identificación del NRA que es titular de una cuenta, así como la fuente de sus fondos y de su riqueza, y ello puede implicar riesgos con respecto a BSA/AML. El país de origen del NRA también puede aumentar el riesgo de la cuenta, conforme a las leyes de secreto que existan en ese país. Debido a que se espera que los NRA residan fuera de los Estados Unidos, las transferencias de fondos o el uso de cajeros automáticos extranjeros pueden ser más frecuentes. El riesgo BSA/AML puede ser mayor si el NRA es una personalidad sujeta a exposición política (PEP). Consulte los procedimientos de inspección ampliada, "Personalidades sujetas a exposición política", en las páginas 334 a 335, para obtener más información.

Mitigación del riesgo

Los bancos deben fijar políticas, procedimientos y procesos que permitan una debida diligencia y prácticas de verificación seguras, análisis de riesgos de las cuentas de los NRA, y supervisión e informe de actividades poco habituales o sospechosas. Los siguientes factores deben ser considerados al determinar el nivel de riesgo de una cuenta de un NRA:

- El país de origen del titular de la cuenta.
- Los tipos de los productos y servicios utilizados.
- Los tipos de identificación.
- Origen de los fondos y de la riqueza.
- Una actividad poco habitual en la cuenta.

Los clientes NRA pueden solicitar el estado W-8 para la retención de impuestos en los Estados Unidos. En tales casos, el cliente NRA completa el formulario W-8, el cual certifica su condición de exento de impuestos en los Estados Unidos y en el extranjero. Si bien este formulario W-8 es emitido por el IRS, no se envía a esa dependencia; se archiva en el banco para sustentar la falta de retención de impuestos sobre las ganancias a dicho extranjero.[241]

El Programa de identificación de clientes (CIP) del banco debe detallar las exigencias de identificación para la apertura de una cuenta de un ciudadano no estadounidense, incluido un NRA. El programa debe incluir métodos documentales y no documentales para verificar la identidad de los clientes. Además, los bancos deben mantener procedimientos de debida diligencia para cuentas de banca privada de ciudadanos no estadounidenses, incluidas aquellas mantenidas por PEP o políticos extranjeros de alto nivel. Consulte la sección del esquema general principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 145 a 150, y la sección del esquema general ampliado y procedimientos de inspección, "Personalidades sujetas a exposición política", en las páginas 329 a 335, como guía.

---

[241] Se puede obtener más información en www.irs.gov/formspubs. Consulte también el boletín 515 del IRS *Withholding of Tax on Nonresident Aliens and Foreign Entities* (Retención de impuestos de extranjeros no residentes y entidades extranjeras).

Procedimientos de Inspección

Extranjeros no residentes y ciudadanos extranjeros

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transacciones que involucren cuentas mantenidas por extranjeros no residentes (NRA) y ciudadanos extranjeros, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las cuentas de los NRA y los ciudadanos extranjeros. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de los extranjeros no residentes y los ciudadanos extranjeros del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de NRA y ciudadanos extranjeros de mayor riesgo.

3. Determine si el sistema de supervisión de las cuentas de los NRA y los ciudadanos extranjeros del banco en busca de actividades sospechosas y para elaborar informes de actividades sospechosas, es adecuado en función de la complejidad de las relaciones de los extranjeros no residentes y los ciudadanos extranjeros con el banco, los tipos y productos utilizados por ellos, sus países de origen, y la fuente de su riqueza y sus fondos.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, para obtener más información.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de las cuentas de NRA y ciudadanos extranjeros, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de los NRA y los ciudadanos extranjeros de mayor riesgo. Incluya los siguientes factores de riesgo:

   - Una cuenta de residente o ciudadano de una jurisdicción de mayor riesgo.
   - La actividad de cuenta está basada sustancialmente en moneda.
   - Un NRA o ciudadano extranjero que utiliza un amplio rango de servicios bancarios, especialmente servicios corresponsales.
   - Un NRA o ciudadano extranjero con respecto al cual el banco ha emitido un SAR.

6. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la información de debida diligencia del cliente, incluida la información del Programa de identificación de clientes (CIP), si corresponde.
   - Revise los estados de cuenta y, según sea necesario, los detalles de las transacciones para determinar si la actividad real de la cuenta es coherente con la actividad prevista. Analice si las transacciones parecen poco habituales o sospechosas.
   - Para las cuentas W-8, verifique que los formularios adecuados hayan sido completados y actualizados, según sea necesario. Revise la actividad transaccional e identifique los patrones que indiquen la condición de residente estadounidense u otra actividad sospechosa y poco habitual.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las cuentas de los NRA.

Personalidades Sujetas a Exposición Política: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las figuras políticas de alto nivel, con frecuencia denominadas "personalidades sujetas a exposición política" (PEP) y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia en función del riesgo. Si la relación es una cuenta de banca privada[242], consulte la sección del esquema general principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 145 a 150, como guía.*

Los bancos deben tomar todas las medidas razonables para asegurar que no participan deliberada o involuntariamente del encubrimiento o transferencia de ganancias provenientes de actos de corrupción por parte de figuras políticas de alto nivel, sus familiares y su círculo de colaboradores. Debido a que los riesgos planteados por las PEP varían según el cliente, el producto o servicio, el país y la industria; la identificación, la supervisión y el diseño de controles de estas cuentas y transacciones deben ser en función del riesgo.

Generalmente, el término "personalidad sujeta a exposición política" hace referencia a un individuo que es o fue figura política de alto nivel o a sus familiares más cercanos y su círculo de colaboradores inmediato. La guía entre agencias publicada en Enero de 2001 ofrece a los bancos recursos que puede ayudarlos a determinar si un individuo es una PEP.[243] Concretamente:

- Una "figura política de alto nivel" es un alto funcionario importante de un órgano ejecutivo, legislativo, judicial, administrativo o militar de un gobierno extranjero (haya sido elegido o no), un miembro de alto nivel de un partido político extranjero importante o un ejecutivo de alto nivel de una corporación que sea propiedad de un

---

[242] A los fines de 31 CFR 103.178, una "cuenta de banca privada" es una cuenta (o una combinación de cuentas) mantenida en un banco que satisface los tres criterios siguientes:

- Exige un depósito de fondos acumulado mínimo u otros activos de no menos de USD 1.000.000;
- Está establecida en nombre o en beneficio de uno o más ciudadanos no estadounidenses que sean propietarios directos o usufructuarios de la cuenta; y
- Está asignada o administrada, en parte o en su totalidad, por un funcionario, empleado o agente del banco que actúa como contacto entre la institución financiera y el propietario directo o usufructuario de la cuenta.

[243] *Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds for Foreign Official Corruption* (Guía para la investigación detallada de las transacciones que puedan incluir fondos derivados de instancias de corrupción oficial extranjera) publicada por el Tesoro de los Estados Unidos, la Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Oficina del Interventor Monetario, la Oficina de Supervisión de Instituciones de Ahorro y el Departamento de Estado de los EE. UU., de Enero de 2001.

gobierno extranjero.[244] Además, el concepto de figura política de alto nivel incluye a cualquier corporación, negocio u otra entidad que haya sido creada por dicho funcionario o en su beneficio.

- En el concepto de "familiares cercanos" se incluye por lo general a los padres, hermanos, cónyuge, hijos o parientes políticos de la figura política de alto nivel.

- Un "íntimo asociado" de una figura política de alto nivel es una persona pública y comúnmente conocida por su íntima asociación respecto a la figura política de alto nivel, e incluye a quienes están en posición de realizar transacciones financieras nacionales e internacionales en grandes volúmenes en nombre de la figura política de alto nivel.

La definición de alto funcionario o ejecutivo debe ser lo suficientemente flexible como para incluir al rango de individuos que, en virtud de su cargo o puesto, plantean potencialmente un riesgo de que sus fondos sean ingresos derivados de corrupción extranjera.[245] Los rangos por sí solos pueden no proporcionar información suficiente para determinar si un individuo es una PEP, ya que la organización de los gobiernos es diferente de una jurisdicción a otra. En aquellos casos en los que un banco emite un SAR concerniente a una transacción que puede involucrar ganancias provenientes de corrupción extranjera, la FinCEN ha ordenado a los bancos incluir el término "corrupción extranjera" en la sección de descripción del SAR.[246] Los bancos deben establecer controles y procedimientos en función del riesgo que incluyan medidas razonables para confirmar la condición de PEP de un individuo y llevar a cabo un escrutinio en función del riesgo de las cuentas mantenidas por dichos individuos. El riesgo variará conforme a otros factores, tales como los productos y los servicios utilizados, y el tamaño o la complejidad de la relación asociada con la cuenta. Los bancos también deben tener en cuenta diversos factores al determinar si un individuo es una PEP, incluidos:

- Responsabilidades oficiales del cargo del individuo.

- El carácter del cargo (es decir, si es honorario o asalariado).

- Nivel y carácter de la autoridad o influencia sobre las actividades gubernamentales u otros funcionarios.

- Acceso a activos o fondos gubernamentales significativos.

---

[244] Es importante tener en cuenta que aunque las corporaciones que sean propiedad de un gobierno pueden plantear riesgos propios, estas corporaciones en sí mismas no están incluidas en la definición de "político extranjero de alto nivel".

[245] 71 Registro Federal 495–515.

[246] Consulte la carta informativa FIN-2008-G005, *Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption* (Guía para las instituciones financieras sobre la presentación informes de actividades sospechosas relacionadas con los fondos provenientes de corrupción extranjera), del 17 de Abril de 2008, en www.fincen.gov.

Para la determinación de la aceptabilidad de cuentas de mayor riesgo, un banco debe ser capaz de obtener información suficiente para determinar si un individuo constituye una PEP o no. Por ejemplo, al llevar a cabo debida diligencia en una cuenta de mayor riesgo, es habitual que un banco revise las fuentes de los ingresos, la información financiera y los antecedentes profesionales de un cliente. Estos factores probablemente exigirán algún tipo de revisión del empleo actual y pasado como también de las referencias generales que pueden identificar la condición de PEP de un cliente. Por otra parte, un banco debe siempre tener en cuenta que la identificación de la condición de PEP de un cliente no debe automáticamente derivar en una determinación del mismo como de mayor riesgo; éste es un solo factor que el banco debe tener en cuenta al analizar el riesgo de una relación.

Confirmar si un cliente tiene una íntima asociación respecto a una figura política de alto nivel puede ser difícil, aunque centrar la atención en aquellas relaciones que son "públicas y comúnmente conocidas" proporciona una limitación razonable a las expectativas de identificar a los miembros del círculo íntimo de colaboradores como PEP. Sin embargo, los bancos que tienen conocimiento cierto de la existencia de una íntima asociación deben considerar a su cliente como PEP, incluso si dicha relación no se conoce públicamente. Se espera que los bancos tomen medidas razonables para confirmar la condición de un individuo y que las agencias bancarias federales y la FinCEN reconozcan que dichas medidas pueden no revelar todas las íntimas asociaciones.

Factores de riesgo

En casos de gran notoriedad ocurridos en años anteriores, las PEP han utilizado bancos como canales para llevar a cabo actividades ilegales, incluidas la corrupción, los actos de cohecho y el lavado de dinero. Sin embargo, no todas las PEP plantean el mismo nivel de riesgo. El riesgo variará dependiendo de numerosos factores, incluso la ubicación geográfica de la PEP, la industria, el sector, el cargo y el nivel o carácter de la influencia o autoridad de las PEP. También variará conforme a otros factores, tales como el propósito de la cuenta, la actividad real o prevista, los productos o servicios utilizados, y el tamaño o la complejidad de la relación asociada con la cuenta.

Como resultado de estos factores, algunas PEP pueden plantear riesgos menores o mayores de corrupción extranjera o lavado de dinero. Los bancos que realizan negocios con PEP deshonestas enfrentan riesgos que pueden afectar sustancialmente la reputación de dichos bancos y someterlos a mayor escrutinio regulatorio y posibles medidas de supervisión. Las señales de advertencia con respecto a las transacciones que pueden estar relacionadas con los ingresos derivados de corrupción extranjera se enumeran en la guía entre agencias de Enero de 2001. Los bancos también deben estar atentos con respecto al acceso, el control o la influencia de las PEP sobre cuentas corporativas o de propiedad del estado; el nivel de participación de intermediarios, proveedores, expedidores y agentes en la industria o el sector en el que opera la PEP; y el uso indebido de organizaciones corporativas y otras personas jurídicas a fin de ocultar la titularidad de las propiedades.

Mitigación del riesgo

Los bancos deben tomar decisiones razonables al diseñar e implementar políticas, procedimientos y procesos con respecto a las PEP. Deben obtener información de debida diligencia en función del riesgo de las PEP y establecer políticas, procedimientos y procesos que hagan posible el escrutinio y la supervisión. Contar con procedimientos apropiados de apertura de cuenta en función del riesgo para productos y servicios de mayor riesgo o que involucren grandes volúmenes en dólares es esencial. La apertura de una cuenta constituye la primera oportunidad que tiene el banco de recopilar información acerca de todos los clientes, incluidas las PEP. De acuerdo con el nivel identificado de riesgo, los procedimientos de debida diligencia deben incluir, entre otros, lo siguientes requisitos:

- Identificación del titular de la cuenta y usufructuario, incluso los propietarios nominales y los usufructuarios de compañías, fideicomisos, sociedades, compañías de inversión privada u otras personas jurídicas que sean titulares de cuentas.

- Obtención de información directamente del titular de la cuenta o el usufructuario relacionada a su posible condición de PEP.

- La identificación del país de residencia del titular de la cuenta y el usufructuario, así como el nivel de riesgo de corrupción y lavado de dinero asociado con dicha jurisdicción.

- Obtención de información respecto al empleo, incluso la industria y el sector, así como el nivel de riesgo de corrupción asociado con dicha industria y sector.

- Verificación de referencias, según sea pertinente, para determinar si el titular de la cuenta y el usufructuario son o han sido una PEP.

- Identificación de la fuente de los fondos y la riqueza del titular de la cuenta y el usufructuario.

- Obtención de información sobre los familiares cercanos o personas que tengan una íntima asociación con autoridad para efectuar transacciones en la cuenta o que se beneficien con las transacciones llevadas a cabo mediante la cuenta.

- Determinación del propósito de la cuenta y del volumen previsto y el carácter de la actividad de la cuenta.

- Dedicación de esfuerzos para revisar las fuentes públicas de información. Estas fuentes variarán en función de cada situación; sin embargo, los bancos deben buscar al titular de cuenta y cualquier usufructuario de personas jurídicas en fuentes de información de acceso público (p. ej., bases de datos gubernamentales, publicaciones informativas importantes, bases de datos comerciales u otra disponibles en Internet, según sea pertinente).

Las cuentas de PEP no se limitan a los bancos importantes o que se especialicen en operaciones internacionales. Una PEP puede abrir una cuenta en cualquier banco, independientemente de su tamaño o ubicación. Los bancos deben contar con

procedimientos en función del riesgo para identificar cuentas de PEP y analizar el grado de riesgo variable planteado. La gerencia debe participar de la decisión de aceptar o no una cuenta de PEP. Si la gerencia determina a posteriori que se trata de una cuenta de PEP, debe evaluar los riesgos y tomar las medidas adecuadas. El banco debe ejercer debida diligencia adicional y razonable con respecto a dichas cuentas. Por ejemplo, el banco puede incrementar las averiguaciones de referencias, obtener información adicional de antecedentes de la PEP proveniente de las sucursales o los corresponsales que operan en el país de origen del cliente y realizar esfuerzos razonables para consultar fuentes de información disponibles públicamente. La supervisión continua en función del riesgo de las cuentas de PEP es esencial para garantizar que las cuentas se estén utilizando de acuerdo con lo previsto. Consulte la sección del esquema general principal, “Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)”, en las páginas 145 a 150, para conocer qué debe esperarse de las relacionadas asociadas con la banca privada y las PEP.

Procedimientos de Inspección

Personalidades sujetas a exposición política

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las figuras políticas de alto nivel, con frecuencia denominadas "personalidades sujetas a exposición política" (PEP) y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia en función del riesgo. Si la relación es una cuenta de banca privada[247], consulte la sección del esquema general principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 145 a 150, como guía.*

1. Revise las políticas, los procedimientos y los procesos en función del riesgo con respecto a las PEP. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las cuentas de PEP del banco y los riesgos que éstas plantean. Analice si los controles en función del riesgo son adecuados para proteger razonablemente al banco a fin de que no sea utilizado como un medio para llevar a cabo el lavado de dinero, actos de corrupción y el financiamiento del terrorismo.

2. Revise los procedimientos para abrir cuentas de PEP. Identifique el papel de la gerencia en la aprobación y supervisión continua en función del riesgo de las cuentas de PEP.

3. De un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con las PEP, particularmente aquellas que planteen un mayor riesgo de lavado de dinero, corrupción y financiamiento del terrorismo.

4. Determine si el sistema del banco para supervisar las actividades sospechosas de PEP y para informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de Control de Activos Extranjeros", en las páginas 176 a 178, como guía.

---

[247] A los fines de 31 CFR 103.178, una "cuenta de banca privada" es una cuenta (o una combinación de cuentas) mantenida en un banco que satisface los tres criterios siguientes:

- Exige un depósito acumulado de fondos mínimo u otros activos de no menos de US$ 1.000.000.
- Está establecida en nombre o en beneficio de uno o más ciudadanos no estadounidenses que sean propietarios directos o usufructuarios de la cuenta; y
- Está asignada o administrada, en parte o en su totalidad, por un funcionario, empleado o agente del banco que actúa como contacto entre la institución financiera y el propietario directo o usufructuario de la cuenta.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de sus relaciones asociadas con PEP, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de PEP. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Determine el cumplimiento con las exigencias normativas y con las políticas, los procedimientos y los procesos establecidos por el banco en relación con las PEP.
   - Revise la actividad transaccional de las cuentas seleccionadas. Si fuera necesario, solicite y revise transacciones específicas.
   - Si el análisis de la información de debida diligencia de los clientes y de actividad plantea inquietudes, dialogue con la gerencia del banco.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con la PEP.

Cuentas de Embajadas y Consulados Extranjeros: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transacciones que involucren cuentas de embajadas y consulados extranjeros, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Las embajadas comprenden las oficinas del embajador extranjero, el representante diplomático y su personal. La embajada, dirigida por el embajador, es la representación oficial de un gobierno extranjero en los Estados Unidos (u otro país). Las oficinas de los consulados extranjeros actúan como sucursales de la embajada y cumplen con diversas funciones administrativas y gubernamentales (p. ej., expedir visas y gestionar asuntos inmigratorios). Las oficinas de los consulados extranjeros están generalmente localizadas en áreas metropolitanas importantes. Además, los representantes diplomáticos de los embajadores extranjeros, sus familias y colaboradores pueden ser considerados como personalidades sujetas a exposición política (PEP) bajo ciertas circunstancias.[248]

Las embajadas y los consulados extranjeros en los Estados Unidos necesitan acceder al sistema bancario para cumplir con muchas de sus responsabilidades financieras cotidianas. Dichos servicios pueden incluir desde relaciones asociadas con cuentas para gastos operativos (p. ej., nómina, locaciones y servicios públicos) hasta transacciones inter- e intragubernamentales (p. ej., compras comerciales y militares). Además de las cuentas oficiales de la embajada, algunos bancos prestan servicios o cuentas auxiliares al personal de las embajadas y a sus familias, así como a funcionarios del gobierno extranjero actual o de gobiernos anteriores. Cada una de estas relaciones plantea respecto al banco un nivel de riesgo diferente.

Las cuentas de las embajadas, incluidas las cuentas de oficinas específicas de las embajadas como las de un ministerio de cultura o educación, agregado militar o ministerio de defensa, o cualquier otra cuenta, deben tener un propósito operativo específico que indique la función oficial de la oficina del gobierno extranjero. Conforme a las prácticas establecidas para las relaciones comerciales, estas cuentas de embajadas deben contar con una autorización por escrito del gobierno extranjero.

Factores de riesgo

Para poder prestar servicios a embajadas y consulados extranjeros, es posible que los bancos estadounidenses deban mantener una relación de corresponsalía extranjera con el banco de la embajada o el consulado extranjero. Los bancos que realizan negocios con embajadas o consulados extranjeros deben analizar y conocer los riesgos potenciales que

[248] Como guía adicional, consulte la sección del esquema general ampliado, "Personalidades sujetas a exposición política", en las páginas 329 a 333.

presentan estas cuentas y desarrollar políticas, procedimientos y procesos adecuados. Estas cuentas pueden plantear un mayor riesgo bajo las siguientes circunstancias:

- Las cuentas son de países que han sido designados como de mayor riesgo.
- Se hacen transacciones en efectivo sustanciales en las cuentas.
- La actividad de la cuenta no es coherente con el propósito de la misma (p. ej., actividad de depósitos vía maletines/bolsos o transacciones pagaderas mediante presentación de identificación apropiada).
- Las cuentas financian directamente los gastos personales de extranjeros, incluidos, entre otros, los gastos de estudiantes universitarios.
- Los negocios oficiales de la embajada se realizan a través de cuentas personales.

Mitigación del riesgo

Los bancos deben obtener información de debida diligencia exhaustiva sobre las relaciones asociadas con las cuentas de embajadas y consulados extranjeros. Concretamente, para las cuentas de banca privada de ciudadanos no estadounidenses, los bancos deben obtener la información de debida diligencia según lo exige 31 CFR 103.178.[249] La debida diligencia del banco respecto a las relaciones asociadas con las cuentas de embajadas y consulados extranjeros debe ser acorde a los niveles de riesgo planteados. Además, se espera que los bancos establezcan políticas, procedimientos y procesos que permitan un mayor escrutinio y supervisión de todas las relaciones asociadas con las cuentas de embajadas y consulados extranjeros. La gerencia debe comprender plenamente el propósito de la cuenta, el volumen previsto y el carácter de la actividad de cuenta. La supervisión continua de las relaciones asociadas con las cuentas de embajadas y consulados extranjeros es esencial para garantizar que las cuentas se estén utilizando según lo previsto.

[249] Como guía adicional, consulte la sección del esquema general principal, “Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)”, en las páginas 145 a 150.

Procedimientos de Inspección

Cuentas de embajadas y consulados extranjeros

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transacciones que involucren cuentas de embajadas y consulados extranjeros, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las cuentas de embajadas y consulados extranjeros. Evalúe la aptitud de las políticas, los procedimientos y los procesos dadas las cuentas de embajadas y consulados extranjeros del banco y los riesgos que éstas plantean (p. ej., la cantidad de cuentas, el volumen de la actividad y las ubicaciones geográficas). Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Identifique el papel de la alta gerencia en la aprobación y supervisión continua de las cuentas de embajadas y consulados extranjeros. Determine si la junta conoce las actividades bancarias de las embajadas y si recibe informes periódicos sobre dichas actividades.

3. De un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con cuentas de embajadas y consulados extranjeros, particularmente aquellas que planteen un mayor riesgo de lavado de dinero.

4. Determine si el sistema del banco para supervisar las cuentas de embajadas y consulados extranjeros, detectar e informar sobre actividades sospechosas, es adecuado a su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con sus clientes.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de sus cuentas de embajadas y consulados extranjeros, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de embajadas y consulados extranjeros. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Determine el cumplimiento con las exigencias normativas y con las políticas, los procedimientos y los procesos establecidos por el banco.

   - Revise la documentación que autoriza al embajador o al consulado extranjero a efectuar operaciones bancarias en los Estados Unidos.

- Revise la actividad transaccional de las cuentas seleccionadas. Si fuera necesario, solicite y revise transacciones específicas.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las cuentas de embajadas y consulados extranjeros.

Instituciones Financieras no Bancarias: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con cuentas de instituciones financieras no bancarias (NBFI), y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

Las NBFI se definen en términos generales como instituciones que no son bancos y que prestan servicios financieros. La Ley PATRIOTA de los EE.UU. define una variedad de entidades como instituciones financieras.[250] Los ejemplos más frecuentes de instituciones financieras no bancarias (NBFI) son los siguientes, sin limitarse únicamente a ellos:

- Casinos y clubes de juego.
- Compañías de valores y productos (p. ej., agentes de valores y de bolsa, asesores de inversión, fondos comunes de inversión, fondos de cobertura o comerciantes de productos).
- Negocios de servicios monetarios (MSB).[251]
- Compañías de seguro.
- Otras instituciones financieras (p. ej., comerciantes de metales preciosos, piedras o joyas, prestamistas, compañías financieras o de préstamo).

A algunas NBFI se les exige actualmente crear un programa AML, cumplir con las exigencias de presentación y gestión de registros de la BSA e informar de actividades sospechosas, al igual que a los bancos. *Las NBFI generalmente necesitan del acceso a una cuenta bancaria para poder operar.* Aunque las NBFI mantengan cuentas operativas en bancos, la BSA no exige que los bancos actúen como entidades reguladoras *de facto* de cualquier industria de NBFI o de clientes NBFI individuales. Por su parte, la FinCEN y las agencias bancarias federales, tampoco esperan que los bancos adopten ese rol. Además, a pesar de que se espera que los bancos gestionen el riesgo que pueden presentar todas las cuentas, incluidas las de las NBFI, no serán considerados responsables de que sus clientes cumplan con la BSA y otras normativas federales y estatales aplicables.

---

[250] Consulte el Apéndice D ("Definición legal de institución financiera") como guía.

[251] Los MSB incluyen cinco tipos diferentes de prestadores de servicios financieros y el Servicio Postal de los Estados Unidos: (1) negocio de intercambio de moneda o casas de cambio; (2) cobradores de cheques; (3) emisores de cheques de viajero, giros postales o valor acumulado; (4) vendedores de cheques de viajero, giros postales o valor acumulado y los encargados de intercambiarlos por dinero (5) transmisores de dinero. Existe un umbral establecido de exigencias para los negocios de las primeras cuatro categorías: un negocio que participa en dichas transacciones no será considerado un MSB si su participación no supera los USD 1.000 para cualquier persona en cualquier día en una o más transacciones (31 CFR 103.11(uu)). Regularmente, la FinCEN publica dictámenes sobre cartas administrativas que abordan consultas sobre si las personas que participan de determinadas actividades comerciales específicas son MSB. Consulte www.fincen.gov/financial_institutions/rulings.html.

Factores de riesgo

Las industrias de NBFI son extremadamente variadas e incluyen desde grandes corporaciones multinacionales hasta pequeñas empresas independientes que ofrecen servicios financieros únicamente como un componente auxiliar en su negocio principal (p. ej., tienda de comestibles que también preste el servicio de cobro de cheques). El rango de productos y servicios ofrecidos, y los tipos de clientes que utilizan los servicios de las NBFI, son igualmente variados. Como resultado de esta diversidad, las NBFI pueden plantear riesgos menores o mayores de lavado de dinero.

Los bancos que mantienen relaciones de cuenta con las NBFI pueden estar expuestos a actividades potenciales de lavado de dinero porque muchas NBFI:

- No mantienen relaciones continuas con sus clientes y requieren mínima o ninguna identificación por parte de éstos.
- Llevan registros limitados o inconsistentes sobre sus clientes y sus transacciones.
- Realizan transacciones en efectivo con frecuencia.
- Están sujetas a niveles variables de exigencias regulatorias y de supervisión.
- Pueden cambiar su combinación de productos o su ubicación con facilidad e ingresar a una operación o abandonarla rápidamente.
- Algunas veces operan sin el debido registro o licencia.

Mitigación del riesgo

Los bancos que mantienen relaciones de cuenta con las NBFI deben fijar políticas, procedimientos y procesos para:

- Identificar las relaciones con las NBFI.
- Analizar los riesgos potenciales que presentan las relaciones con las NBFI.
- Realizar una debida diligencia adecuada y continua a las relaciones con las NBFI cuando sea necesario.
- Asegurar que las relaciones con las NBFI se tengan en cuenta debidamente en los sistemas del banco de supervisión e informe de actividades sospechosas.

Factores del análisis de riesgos

Los bancos deben analizar los riesgos que plantean sus clientes NBFI y dirigir sus recursos de manera tal que apunten a aquellas cuentas que plantean un mayor riesgo de lavado de dinero.

Los siguientes factores pueden utilizarse para ayudar a identificar los riesgos relativos que pueden presentarse en la cartera de las NBFI. No obstante, la gerencia debe ponderar

y evaluar todos los factores de análisis de riesgos para determinar cuál es el nivel de riesgo que implica cada cliente y priorizar recursos de supervisión. Los factores de riesgo relevantes incluyen:

- Tipos de productos y servicios ofrecidos por las NBFI.
- Ubicaciones y mercado servidos por las NBFI.
- Actividad prevista de la cuenta.
- Propósito de la cuenta.

La debida diligencia del banco debe ser acorde al nivel de riesgo que presenta el cliente NBFI, identificado por medio del análisis de riesgos. Si el análisis de riesgos del banco indica una alta probabilidad de riesgo de lavado de dinero o financiamiento de terrorismo, se esperará que realice debida diligencia adicional de una manera acorde al alto riesgo.

Prestación de servicios bancarios a negocios de servicios de dinero

La FinCEN y las agencias bancarias federales emitieron guías interpretativas el 26 de Abril de 2005, para clarificar las exigencias de la BSA y las expectativas de supervisión respecto a cuentas abiertas o mantenidas para los MSB.[252] Con limitadas excepciones, muchos MSB están sujetos al rango completo de las exigencias normativas de la BSA, que incluye las reglamentaciones del programa contra el lavado de dinero, de la presentación de informes de transacciones en efectivo y actividades sospechosas, y otras reglamentaciones sobre identificación y gestión de registros.[253] Los reglamentos existentes de la FinCEN exigen que algunos se registren ante la FinCEN.[254] Finalmente,

[252] Consulte "Guía interpretativa aplicable entre agencias sobre la prestación de servicios bancarios a negocios de servicios de dinero que operan el los Estados Unidos" (en inglés, *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United Status*), del 26 de Abril de 2005, disponible en www.fincen.gov.

[253] Consulte 31 CFR 103.125 (exigencia de que los negocios de servicios de dinero (MSB) establezcan y mantengan un programa contra el lavado de dinero); 31 CFR 103.22 (exigencia de que los MSB presenten Informes de Transacciones en Efectivo); 31 CFR 103.20 (exigencia de que los MSB presenten Informes de Actividades Sospechosas, que no sean sobre el cobro de cheques y las transacciones de valor acumulado); 31 CFR 103.29 (exigencia de que los MSB que vendan giros postales, cheques de viajeros u otros instrumentos monetarios a cambio de dinero verifiquen la identidad del cliente y creen y mantengan un registro de cada compra en moneda de entre US$ 3.000 y US$ 10.000, inclusive); 31 CFR 103.33(f) y (g) (normas aplicables a transmisiones de fondos específicas); y 31 CFR 103.37 (exigencias adicionales sobre gestión de registros para casas de cambio, incluida la exigencia de crear y mantener un registro de cada cambio de moneda superior a USD 1.000).

[254] Consulte 31 CFR 103.41. Todos los MSB deben registrarse en la FinCEN (tengan o no licencia de MSB en algún estado), excepto: un negocio que sea únicamente un MSB por prestar servicios de agente a otro MSB; un negocio que sea un MSB únicamente como emisor o vendedor de valores acumulados o como encargado de intercambiarlos por dinero; el Servicio Postal de los Estados Unidos y agencias de los Estados Unidos, de cualquiera de sus estados, o de cualquier otra subdivisión política de cualquier estado. Un negocio que actúe como agente de un mandante o mandantes que participen en actividades de MSB, y

muchos estados han establecido exigencias de supervisión, que a menudo incluyen el requisito de que los MSB obtengan licencia en todos los estados en los que estén incorporados o realicen negocios.

Las siguientes expectativas regulatorias se aplican a bancos que tienen MSB como clientes:

- La BSA no exige que los bancos actúen como entidades reguladoras *de facto* de ningún tipo de industria de NBFI o de clientes NBFI individuales. Por su parte, la FinCEN y las agencias bancarias federales tampoco esperan que los bancos adopten ese rol.

- A pesar de que se espera que los bancos gestionen el riesgo asociado con todas las cuentas, incluidas las cuentas de MSB, los bancos no serán responsables del programa BSA/AML de los MSB.

- No todos los MSB plantean el mismo nivel de riesgo, y no todos ellos requieren el mismo nivel de debida diligencia. Consecuentemente, si el análisis de riesgos del banco de una relación particular con MSB indica un riesgo menor de lavado de dinero u otra actividad ilícita, no se espera automáticamente que el banco realice debida diligencia adicional (como revisar información sobre el programa BSA/AML de los MSB) más allá de las expectativas mínimas de debida diligencia. A menos que el análisis de riesgos lo indique, no se exige que los bancos controlen automáticamente un programa BSA/AML de los MSB.

Análisis de riesgos de los MSB

Un análisis de riesgos eficaz debe estar compuesto por múltiples factores y, según las circunstancias, ciertos factores pueden influir más que otros. Los siguientes factores se pueden utilizar para ayudar a identificar el nivel de riesgo presentado por cada cliente MSB:

- Propósito de la cuenta.

- Actividad prevista de la cuenta (tipo y volumen).

- Tipos de productos y servicios ofrecidos por los MSB.

- Ubicaciones y mercados en los cuales presten servicios los MSB.

La gerencia debe adaptar estos factores en función de su base de clientes o de las ubicaciones geográficas en las que el banco opera. La gerencia debe ponderar y evaluar cada factor de análisis de riesgos para llegar a una determinación sobre el riesgo que implica cada cliente. Una debida diligencia del banco debe ser acorde al nivel de riesgo asignado a cada cliente que sea un MBS, luego de considerar estos factores. Si el análisis

---

que no realice en su nombre ningún otro servicio de un carácter o valor tal como para calificarlo de MSB, no necesita registrarse en la FinCEN. La FinCEN ha emitido pautas sobre el registro y el cese del registro de los MSB. Consulte FIN-2006-G006, *Registration and De-Registration of Money Services Businesses*, (Registro y cese del registro de los negocios de servicios de dinero), del 3 de Febrero de 2006, en www.fincen.gov.

de riesgos del banco indica una alta probabilidad de riesgo de lavado de dinero o financiamiento de terrorismo, se esperará que el banco realice debida diligencia adicional de una manera acorde al alto riesgo.

Mitigación del riesgo de los MSB

Las políticas, los procedimientos y los procesos del banco deben establecer prácticas de debida diligencia y verificación responsables, análisis de riesgos adecuado de las cuentas de MSB, y supervisión e informe continuos de actividades poco habituales o sospechosas. Un banco que establece y mantiene cuentas para MSB debe aplicar políticas, procedimientos y controles de debida diligencia que sean apropiados, específicos, basados en el riesgo y, cuando sea necesario, especiales (EDD).

Los factores enumerados a continuación, a pesar de no incluir a todos los existentes, pueden reducir o mitigar el riesgo en algunas cuentas de MSB:

- El MSB está registrado ante la FinCEN y obtuvo licencia en el estado o estados adecuados, si así se exige.
- El MSB confirma estar sujeto a inspección para verificar el cumplimiento AML por parte del Servicio de Impuestos Internos (IRS) o el estado o estados, si corresponde.[255]
- El MSB afirma que existe de un programa BSA/AML escrito y proporciona el nombre del funcionario de la BSA y la información de contacto.
- EL MSB tiene una relación bancaria establecida y/o actividad de cuenta coherente con las expectativas.
- El MSB está debidamente establecido y tiene antecedentes de operación.
- El MSB actúa como mandante respecto a uno o varios agentes o actúa como un agente de un mandante.
- El MSB presta servicios sólo a residentes locales.
- La mayoría de los clientes de los MSB realizan transacciones de rutina en montos bajos en dólares.

---

[255] El 9 de Diciembre de 2008, la FinCEN y el Servicio de Impuestos Internos (IRS) publicaron el *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses* (MSB Exam Manual) (Manual de Inspección Contra el Lavado de Dinero/Ley de Secreto Bancario para los Negocios de Servicios Monetarios; [Manual de Inspección para MSB]), que fue desarrollado en colaboración con la *Conference of State Bank Supervisors* (Conferencia de supervisores de bancos estatales), la *Money Transmitter Regulators Association* (Asociación de reguladores de los entes transmisores de dinero) y las agencias estatales responsables de la regulación de los MSB. Consulte el Manual de Inspección para MSB, disponible en www.fincen.gov.

- La actividad transaccional prevista (de menor riesgo) para las operaciones comerciales del MSB es coherente con la información obtenida por el banco en el momento de la apertura de la cuenta. Los ejemplos incluyen lo siguiente:
    - La actividad de cobro de cheques se limita a cheques del gobierno o de nómina (de cualquier monto en dólares).
    - El servicio de cobro de cheques se ofrece respecto a cheques de otro estado o de terceros.
- Las actividades de transmisión de dinero se limitan a entidades nacionales (p. ej., pagos de facturas nacionales) o a montos más bajos en dólares (nacionales o internacionales).

Expectativas de debida diligencia de MSB

Las obligaciones más básicas que deben cumplir los MSB son el registro ante la FinCEN, si es obligatorio, y el cumplimiento de cualquier exigencia de licencia de los estados. Como resultado, es razonable y adecuado para un banco exigir que un MSB proporcione evidencia del cumplimiento con dichas exigencias, o que demuestre que no está sujeto a ellas debido al carácter de sus servicios financieros o a su condición exclusiva de agente de otro MSB u otros MSB.

Dada la importancia de las exigencias de registro y licencia, un banco debe presentar un SAR si toma conocimiento de que un cliente opera infringiendo la exigencia sobre registración u obtención de licencia en el estado. No existe exigencia en los reglamentos de la BSA de que un banco cierre una cuenta que está sujeta a un SAR. La decisión de mantener o cerrar una cuenta debe tomarla la gerencia del banco de acuerdo con los estándares y las pautas aprobados por su junta directiva.

El grado en que el banco deba realizar debida diligencia adicional, más allá de las obligaciones mínimas de debida diligencia establecidas a continuación, será determinado por el nivel de riesgo planteado por el cliente MSB individual. Debido a que no todos los MSB presentan el mismo nivel de riesgo, no todos ellos requerirán debida diligencia adicional. Por ejemplo, el dueño de una tienda de comestibles local que también cobra cheques de nómina para clientes que compren allí, puede no presentar el mismo nivel de riesgo que un transmisor de dinero que se especializa en transferencias de fondos transnacionales. Por lo tanto, las exigencias de debida diligencia de los clientes diferirán en función del riesgo que plantee cada cliente que sea un MSB. En función de las exigencias de la BSA existentes aplicables a los bancos, las expectativas mínimas de debida diligencia asociada con la apertura y el mantenimiento de cuentas para cualquier MSB[256] son:

[256] Consulte *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United Status* (Guía interpretativa aplicable entre agencias sobre la prestación de servicios bancarios a negocios de servicios de dinero que operan en los Estados Unidos), del 26 de Abril de 2005, disponible en www.fincen.gov.

- Aplicar el Programa de identificación de clientes (CIP) del banco.[257]
- Confirmar el registro ante la FinCEN, si se exige. (Tenga en cuenta: el registro debe ser renovado cada dos años).
- Confirmar el cumplimiento con las exigencias de licencia locales o estatales, si corresponde.
- Confirmar la condición de agente, si corresponde.
- Realizar un análisis de riesgos BSA/AML básico para determinar el nivel de riesgo asociado con la cuenta y si se requiere debida diligencia adicional.

Si el banco determina que el cliente MSB presenta un nivel mayor de riesgo de lavado de dinero o financiamiento del terrorismo, se deberán tomar medidas de debida diligencia especial, además de llevar a cabo los procedimientos mínimos de debida diligencia. Teniendo en cuenta el nivel de riesgo percibido y el tamaño y la complejidad de cada MSB en particular, las organizaciones bancarias pueden poner en práctica algunas de las siguientes acciones o todas, como parte de un control adecuado de debida diligencia especial (EDD):

- Revisar el programa BSA/AML de los MSB.
- Revisar los resultados de las pruebas independiente de los MSB de su programa AML.
- Revisar los procedimientos escritos relativos a la operación de los MSB.
- Realizar visitas en el sitio.
- Revisar la lista de agentes, incluidas las ubicaciones, dentro o fuera de los Estados Unidos, que recibirán servicios directa o indirectamente a través de una cuenta de MSB.
- Revisar las prácticas escritas sobre gestión de agentes y terminación aplicables a los MSB.
- Revisar las prácticas escritas de revisión de los empleados aplicables a los MSB.

La FinCEN y las agencias bancarias federales no esperan que los bancos exijan uniformemente todas o cualquiera de las acciones identificadas anteriormente para todos los MSB.

---

[257] Consulte 31 CFR 103.121 (FinCEN); 12 CFR 21.21 (Oficina del Interventor Monetario); 12 CFR 208.63(b), 211.5(m), 211.24(j) (Junta de Gobernadores del Sistema de Reserva Federal); 12 CFR 326.8(b)(2) (Corporación Federal de Seguro de Depósitos); 12 CFR 563.177(b) (Oficina de Supervisión de Instituciones de Ahorro); 12 CFR 748.2(b) (Administración Nacional de Cooperativas de Crédito).

Procedimientos de Inspección

Instituciones financieras no bancarias

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con cuentas de instituciones financieras no bancarias (NBFI), y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Determine el grado de las relaciones del banco con las NBFI y, respecto a los bancos con relaciones significativas con NBFI, revise el análisis de riesgos del banco de estas actividades.

2. Revise las políticas, los procedimientos y los procesos con respecto a las cuentas de las NBFI. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de las NBFI del banco y los riesgos que plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

3. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de NBFI.

4. Determine si el sistema del banco para supervisar las cuentas de las NBFI, e informar sobre actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

Negocios de Servicios de Dinero

5. De conformidad con la guía aplicable entre agencias publicada el 26 de Abril de 2005, determine si el banco cuenta con políticas, procedimientos y procesos aplicables a las cuentas abiertas o mantenidas para los negocios de servicios de dinero (MSB) para:

   - Confirmar el registro ante la FinCEN, si se exige. (Tenga en cuenta: el registro debe ser renovado cada dos años).
   - Confirmar que se obtuvo la licencia en el estado, si corresponde.
   - Confirmar la condición de agente, si corresponde.
   - Realizar un análisis de riesgos para determinar el nivel de riesgo asociado con cada cuenta y si se requiere debida diligencia adicional.

6. Determine si las políticas, los procedimientos y los procesos del banco para analizar los riesgos planteados por clientes que son MSB identifican de manera eficaz las cuentas de alto riesgo y la cantidad de debida diligencia adicional necesaria.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus cuentas de NBFI, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de NBFI de mayor riesgo. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revisar la documentación de apertura de la cuenta e información de debida diligencia continua.
   - Revisar los estados de cuenta y, según sea necesario, detalles específicos de las transacciones. Comparar las transacciones previstas con la actividad real.
   - Determinar si la actividad real es coherente con el carácter del negocio del cliente e identificar cualquier actividad sospechosa o poco habitual.
   - En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las relaciones con las NBFI.

Prestadores de Servicios Profesionales: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones asociadas a los prestadores de servicios profesionales y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Un prestador de servicios profesionales actúa como intermediario entre su cliente y el banco. Los prestadores de servicios profesionales pueden ser abogados, contadores, agentes de inversión y otros terceros que sirven de contacto financiero a sus clientes. Estos prestadores pueden realizar negocios financieros para sus clientes. Por ejemplo, un abogado puede prestar servicios a un cliente o hacer arreglos para que éstos se presten en nombre del cliente, como cierre de transacciones sobre bienes inmuebles, transferencias de activos, administración de los dineros del cliente, servicios de inversión y acuerdos fiduciarios.

Un ejemplo típico es el interés que producen las cuentas fiduciarias de abogados (IOLTA). Estas cuentas tienen fondos de distintos clientes de abogados pero actúan como cuenta bancaria estándar con una característica particular: El interés que produce la cuenta se cede a la asociación de abogados del estado u otra entidad para el bien público o fines *pro bono*.

Factores de riesgo

En contraste con las cuentas de depósito en plica que se establecen para servir a clientes individuales, las cuentas de prestadores de servicios profesionales permiten transacciones comerciales continuas con múltiples clientes. Generalmente, el banco no tiene una relación directa con los usufructuarios de estas cuentas ni los conoce, y éstos pueden ser un grupo de personas físicas o jurídicas que cambian constantemente.

Como sucede con cualquier cuenta que presenta riesgos por parte de terceros, el banco puede ser más vulnerable al potencial abuso del lavado de dinero. Algunos ejemplos potenciales de abuso incluyen:

- Lavado de dineros ilícitos.
- Estructuración de los depósitos en moneda y retiros.
- Apertura de cuenta para un tercero con el propósito principal de ocultar la identidad del cliente subyacente.

Como tal, el banco debe establecer un programa de debida diligencia eficaz para el prestador de servicios profesionales como se resume a continuación.

Mitigación del riesgo

Al establecer y mantener relaciones con prestadores de servicios profesionales, los bancos deben evaluar de manera adecuada los riesgos de las cuentas y supervisar la relación para detectar actividades poco habituales o sospechosas. En el momento de apertura de una cuenta, el banco debe conocer el uso deseado de la misma, incluidos el volumen previsto de transacciones, los productos y servicios utilizados y las ubicaciones geográficas implicados en la relación. Como se indica en la sección del esquema general principal, "Exenciones del Informe de transacciones en efectivo" en las páginas 100 a 105, no es posible eximir a los prestadores de servicios profesionales de las exigencias de presentación de informes de transacciones en efectivo.

Procedimientos de Inspección

Prestadores de servicios profesionales

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones asociadas a los prestadores de servicios profesionales y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las relaciones asociadas con los prestadores de servicios profesionales. Evalúe la aptitud de las políticas, los procedimientos y los procesos en función de las relaciones del banco con los proveedores de servicios profesionales y los riesgos que dichas relaciones plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con los prestadores de servicios profesionales. (Los informes de MIS deben incluir información sobre la relación en su totalidad. Por ejemplo, una Cuenta Fiduciaria de Abogado con Rendimiento de Interés (IOLTA) puede estar a nombre de una firma de abogados en lugar de a nombre de un individuo. Sin embargo, el informe del banco sobre la relación debe incluir la cuenta de la firma de abogados *y* los nombres y cuentas de los abogados asociados con la IOLTA.

3. Determine si el sistema del banco para supervisar las relaciones asociadas con los prestadores de servicios profesionales, detectar e informar sobre actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus relaciones con prestadores de servicios profesionales, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las relaciones de mayor riesgo. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta y una muestra de la actividad transaccional.

   - Determine si la actividad real de la cuenta es coherente con la actividad prevista de la cuenta (de acuerdo a la documentación). Identifique las tendencias en el

carácter, el tamaño o el campo de aplicación de las transacciones, prestando especial atención a las transacciones en efectivo.

- Determine si la supervisión continua es suficiente para identificar las actividades potencialmente sospechosas.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos con respecto a las relacionadas asociadas con los prestadores de servicios profesionales.

Organizaciones no Gubernamentales y Entidades de Beneficencia: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las organizaciones no gubernamentales (ONG) y las entidades de beneficencia y la capacidad de la gerencia de implementar sistemas eficaces de* supervisión, informe y debida diligencia.

Las ONG son organizaciones privadas sin fines de lucro que se dedican a actividades cuyo propósito es contribuir al bien público. Las ONG pueden prestar servicios sociales básicos, trabajar para aliviar el sufrimiento, promover los intereses de los pobres, acercar a los gobiernos los problemas de los ciudadanos, incentivar la participación política, proteger el medio ambiente o encargarse del desarrollo de la comunidad para atender las necesidades de ciudadanos, organizaciones o grupos en una o más de las comunidades donde trabajan. Una ONG puede ser cualquier organización sin fines de lucro que no dependa del gobierno.

Las ONG pueden ser desde grandes entidades de beneficencia regionales, nacionales o internacionales hasta grupos comunitarios de autoayuda. También comprenden institutos de investigación, iglesias, asociaciones profesionales y grupos de presión. Económicamente las ONG típicamente dependen, parcial o totalmente, de donaciones benéficas y del trabajo voluntario.

Factores de riesgo

Debido a que las ONG pueden ser usadas para obtener fondos para organizaciones de beneficencia, el flujo de fondos saliente o entrante de las ONG puede ser complejo, tornándolas susceptibles al abuso por parte de lavadores de dinero y terroristas. El Tesoro de los Estados Unidos publicó pautas para asistir a las entidades de beneficencia en la adopción de prácticas para disminuir el riesgo de abuso o financiamiento del terrorismo.[258]

Mitigación del riesgo

Para analizar el riesgo de los clientes que sean ONG, los bancos deben aplicar una debida diligencia adecuada a la organización. Además de obtener la información del Programa de Identificación de Clientes (CIP), la debida diligencia de las ONG debe enfocarse en otros aspectos de la organización, tales como los siguientes:

- Propósitos y objetivos de sus actividades declaradas.

---

[258] *Anti-Terrorist Financing Guidelines*: *Voluntary Best Practices for U.S.-Based Charities* (Guía de financiación contra el terrorismo: Prácticas adecuadas para voluntarios de entidades de beneficencia estadounidenses), de Septiembre de 2006, está disponible en www.treasury.gov/offices/enforcement/key-issues/protecting/index.shtml.

- Las ubicaciones geográficas a las que prestan servicios (incluidas la sede principal y las áreas operativas).
- La estructura organizativa.
- La base de donantes y voluntarios.
- Criterios de obtención de fondos y desembolso (incluida la información básica sobre el beneficiario).
- Exigencias en cuanto a la gestión de registros.
- Afiliaciones con otras ONG, gobiernos o grupos.
- Controles internos y auditorías.

Respecto a las cuentas que la gerencia del banco considere de mayor riesgo, se deben establecer procedimientos estrictos en cuanto a la documentación, la verificación y la supervisión de las transacciones. Las cuentas de ONG con mayor riesgo BSA/AML incluyen aquellas que operan o prestan servicios a nivel internacional, llevan a cabo actividades sospechosas o poco habituales o carecen de la documentación adecuada. La debida diligencia especial (EDD) de estas cuentas debe incluir lo siguiente:

- La evaluación de los mandantes.
- La obtención y el control de los estados financieros y auditorias.
- La verificación de la fuente y el uso de los fondos.
- La evaluación de los grandes colaboradores o contribuyentes de la ONG.
- La verificación de referencias.

Procedimientos de Inspección

Organizaciones no gubernamentales y entidades de beneficencia

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las organizaciones no gubernamentales (ONG) y las entidades de beneficencia y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las ONG. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación a las cuentas de ONG del banco y los riesgos que plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de ONG de mayor riesgo.

3. Determine si el sistema del banco para supervisar las actividades sospechosas de cuentas de las ONG, detectar e informar sobre actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco, sus cuentas de ONG y entidades de beneficencia, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de ONG de mayor riesgo. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta e información de debida diligencia continua.
   - Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones.
   - Compare las transacciones previstas con la actividad real.
   - Determine si la actividad real es coherente con el tipo de negocio del cliente.
   - Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las cuentas de ONG.

Entidades Comerciales (Nacionales y Extranjeras): Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transacciones que involucren entidades comerciales nacionales y extranjeras y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

El término "entidades comerciales" incluye a compañías de responsabilidad limitada, corporaciones, fideicomisos y otras entidades que pueden utilizarse con diversos fines, como por ejemplo la planificación tributaria y patrimonial. Es relativamente fácil constituir una entidad comercial. Los individuos, las sociedades y las corporaciones ya constituidas pueden establecer entidades comerciales por razones legítimas, pero dichas entidades pueden ser vulnerables al abuso de lavado de dinero y el financiamiento del terrorismo.

Entidades comerciales nacionales

Todos los estados cuentan con leyes que rigen la organización y operación de las entidades comerciales, incluidas las compañías de responsabilidad limitada, las corporaciones, las sociedades colectivas, las sociedades limitadas y los fideicomisos. Las compañías fantasma registradas en los Estados Unidos constituyen un tipo de entidad comercial nacional[259] que puede plantear un mayor riesgo.[260] Una compañía fantasma se puede utilizar para el lavado de dinero y otros delitos debido a que se las puede constituir y operar de manera económica y sencilla. Además, la información transaccional y de propiedad se puede ocultar a las agencias regulatorias y autoridades de aplicación de la ley, en gran medida debido a que la mayoría de las leyes estatales exigen una divulgación mínima de dicha información durante el proceso de constitución. Según un informe de la Oficina de Contabilidad del Gobierno estadounidense (GAO, por sus siglas en inglés), a las autoridades de aplicación de la ley les preocupa que los criminales utilicen cada vez más las compañías fantasma estadounidenses para ocultar su identidad y sus actividades ilícitas.[261]

---

[259] El término "nacional" hace referencia a entidades formadas u organizadas en los Estados Unidos. Es posible que estas entidades no tengan otra conexión con los Estados Unidos, y la propiedad y administración de dichas entidades puede residir en el extranjero.

[260] El término "compañía fantasma" generalmente se refiere a cualquier entidad sin presencia física en ningún país. La FinCEN ha publicado una guía que alerta a las instituciones financieras sobre los riesgos potenciales asociados con la prestación de servicios financieros a compañías fantasma y les recuerda que es importante gestionar dichos riesgos. Consulte FIN-2006-G014, *Potential Money Laundering Risks Related to Shell Companies* (Riesgos potenciales de lavado de dinero relacionados con compañías fantasma*)*, de Noviembre de 2006, en www.fincen.gov.

[261] Consulte GAO-06-376, *Company Formations — Minimal Ownership Information is Collected and Available* (Constitución de compañías: recopilación y disponibilidad de información de propiedad mínima), de la GAO, de Abril de 2006, en www.gao.gov/new.items/d06376.pdf. Para obtener más información, consulte *Failure to Identify Company Owners Impedes Law Enforcement*, (Falta de identificación sobre los propietarios de compañías impide la aplicación de la ley) Sesión 109-845 del Senado, llevada a cabo

Las compañías fantasma incluyen aquellas que cotizan en la Bolsa de valores o son de propiedad privada. Aunque las compañías fantasma que cotizan en la Bolsa de valores pueden utilizarse con fines ilícitos, la vulnerabilidad de la compañía fantasma se agrava cuando es de propiedad privada y se puede ocultar o disimular con más facilidad el usufructo. La falta de transparencia respecto al usufructo puede constituir una característica atractiva para algunos usos legítimos de las compañías fantasma, pero es también una gran vulnerabilidad que puede convertir a algunas de estas compañías en vehículos ideales para el lavado de dinero y otras actividades financieras ilícitas. En algunas jurisdicciones estatales, sólo se exige información mínima para registrar actas constitutivas o para establecer y mantener "en vigor" a las entidades comerciales, lo que incrementa el potencial de abuso por parte de las organizaciones terroristas y delictivas.

Entidades comerciales extranjeras

Las entidades extranjeras más frecuentemente utilizadas son los fideicomisos, los fondos de inversión y las compañías de seguros. Dos entidades extranjeras que pueden imponer un mayor riesgo de lavado de dinero son las Corporaciones Comerciales Internacionales (IBC) y las Compañías de Inversión Privada (PIC) abiertas en centros financieros instalados en el exterior (OFC). Muchos OFC están sujetos a relativamente pocas exigencias en cuanto a la divulgación institucional y la gestión de registros cuando se establece una entidad comercial extranjera, lo cual crea un entorno oportuno para el lavado de dinero.

Corporaciones comerciales internacionales

Las IBC son entidades constituidas en países distintos al de residencia de la persona, que pueden ser utilizadas para mantener la confidencialidad u ocultar activos. La propiedad de una IBC se puede, en función de la jurisdicción, transferir a través de acciones nominativas o al portador. Utilizarlas implica una serie de ventajas, tales como las siguientes:

- Protección de los activos.
- Planificación patrimonial.
- Privacidad y confidencialidad.
- Reducción de la carga tributaria.

A través de una IBC, un individuo puede realizar lo siguiente:

---

el 14 de Noviembre de 2006, en hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=4478b046-2b7e-4dd0-b061-efabbdbbf844, y *Tax Haven Abuses: The Enablers, The Tools & Secrecy* (Abusos de refugios tributarios: los posibilitadores, las herramientas y el secreto), Sesión 109-797 del Senado, llevada a cabo el 1 de Agosto de 2006, (particularmente el Informe en conjunto de los representantes de grupos mayoritarios y minoritarios del Subcomité Permanente de Investigaciones), en hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=79a104cf-75cb-44aa-ae20-32301fa3c349.

- Abrir y mantener cuentas bancarias.
- Mantener y transferir fondos.
- Hacer negocios internacionales y otras transacciones relacionadas.
- Mantener y manejar inversiones fuera del país (p. ej., acciones, bonos, fondos comunes de inversión y certificados de depósito), muchas de las cuales pueden no estar disponibles a los "individuos" dependiendo de su lugar de residencia.
- Tener tarjetas de débito y crédito corporativas, y disponer así de cómodo acceso a los fondos.

Compañías de inversión privada

Las PIC son personas jurídicas independientes. En esencia son subgrupos de las IBC. Para determinar si una corporación extranjera es una PIC hay que identificar el propósito y el uso del instrumento legal. Típicamente, las PIC se utilizan para mantener fondos e inversiones particulares, y se puede conceder la propiedad a través de acciones nominativas o al portador. Al igual que con otras IBC, las PIC pueden ofrecer confidencialidad a la propiedad, centralizar los activos y es posible que proporcionen servicio de intermediarios entre los clientes de la banca privada y los beneficiarios potenciales de las PIC. Las acciones de una PIC pueden ser agrupadas en un fideicomiso, lo que disimula aun más el usufructo de los activos subyacentes. Las IBC, incluidas las PIC, son constituidas con frecuencia en países que imponen impuestos bajos o nulos a los activos o las operaciones de la compañía, o que constituyen refugios con respecto al secreto bancario.

Servicios de constitución de compañías nominadas

Los intermediarios, denominados servicios de constitución de compañías nominadas (NIS, por sus siglas en inglés), establecen compañías fantasma y cuentas bancarias en nombre de clientes extranjeros. Los NIS se pueden encontrar en los Estados Unidos o fuera del país. Los abogados corporativos de los Estados Unidos con frecuencia utilizan los NIS para organizar compañías en nombre de sus clientes nacionales y extranjeros debido a que dichos servicios pueden organizar de manera eficaz personas jurídicas en cualquier estado. Los NIS deben cumplir con los procedimientos federales y estatales correspondientes como también con cualquier exigencia bancaria específica. Dichas leyes y procedimientos dictan qué información deben compartir los NIS acerca de los propietarios de una persona jurídica. Los lavadores de dinero también han utilizado los NIS para ocultar sus identidades. Al contratar una firma que oficie de intermediaria entre ellos mismos, la jurisdicción que expide la licencia, y el banco, los usufructuarios de una compañía pueden evitar divulgar sus identidades en la presentación de informes corporativos estatales y en la documentación de apertura de la cuenta bancaria corporativa.

Un NIS tiene la capacidad de constituir entidades empresariales, abrir cuentas bancarias de servicio completo para dichas entidades, y actuar como el agente registrado que acepta la notificación de demanda en nombre de dichas entidades en una jurisdicción en la que

éstas no tienen presencia física. Además, un NIS puede desempeñar estos servicios sin tener que identificar el usufructo en la constitución, el registro o los documentos de la cuenta bancaria de la compañía.

Varias firmas de NIS internacionales han formado sociedades o alianzas comerciales con bancos estadounidenses para ofrecer servicios financieros como bancos en Internet y capacidades para transferencias de fondos a compañías fantasma y ciudadanos no estadounidenses. Los bancos estadounidenses que participan en estas alianzas comerciales a través de la apertura de cuentas mediante intermediarios sin exigir la presencia física del titular real de la cuenta, aceptando copias enviadas por correo de fotografías de pasaportes, facturas de servicios públicos y otra información de identificación, pueden asumir mayores niveles de riesgo BSA/AML.[262]

Factores de riesgo

Los riesgos de lavado de dinero y financiamiento del terrorismo surgen debido a que las entidades comerciales pueden ocultar al verdadero propietario de los activos o la propiedad derivada de la actividad delictiva o asociada a ella.[263] La privacidad y la confidencialidad que brindan algunas entidades comerciales pueden ser aprovechadas por criminales, lavadores de dinero y terroristas. La verificación de los contribuyentes y usufructuario(s) de algunas entidades comerciales puede resultar extremadamente difícil, ya que las características de dichas entidades protegen la identidad legal del propietario. Pocos registros públicos revelan quienes son los verdaderos propietarios. En general, la falta de transparencia en la información de propiedad; las exigencias mínimas o nulas respecto a la gestión de registros, la divulgación financiera y la supervisión; y el rango de actividades lícitas, incrementan el riesgo de lavado de dinero.

Aunque las entidades comerciales se pueden establecer en la mayoría de las jurisdicciones internacionales, muchas se constituyen en OFC que proporcionan privacidad en relación a la propiedad e imponen pocas obligaciones tributarias o ninguna. Para mantener el anonimato, muchas entidades comerciales se constituyen con directores nominales, funcionarios nominales y accionistas fiduciarios. En ciertas jurisdicciones, las entidades comerciales también pueden establecerse utilizando acciones al portador; los registros de propiedad no se mantienen, en su lugar, la propiedad se constituye en función de la posesión física de los certificados de acción. Los fideicomisos revocables son otro método utilizado para resguardar al contribuyente y usufructuario y se pueden diseñar para gestionar la entidad comercial y obtener la propiedad de la misma, lo que fija barreras significativas para la aplicación de la ley.

---

[262] Grupo de Trabajo sobre la Evaluación de Amenazas de Lavado de Dinero, *U.S. Money Laundering Threat Assessment* (Evaluación de amenazas de lavado de dinero de Estados Unidos), de Diciembre de 2005.

[263] Para conocer un análisis general de los factores de riesgo asociados con el uso indebido de entidades empresariales, consulte *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers* (El uso indebido de instrumentos corporativos, incluidos los proveedores de servicios a compañías y fideicomisos) del Grupo de Acción Financiera, del 13 de Octubre de 2006, en www.fatf-gafi.org.

Aunque la mayoría de las compañías fantasma en los Estados Unidos prestan servicios legítimos, algunas se han utilizado como canales para el lavado de dinero, ocultar transacciones en el exterior, o para estructurar entidades empresariales nacionales o extranjeras.[264] Por ejemplo, los reguladores han identificado compañías fantasma registradas en los Estados Unidos que efectuaban transacciones sospechosas con contrapartes ubicadas en el extranjero. Estas transacciones, principalmente transferencias de fondos circulares que entraban y salían del sistema bancario estadounidense, demostraban no tener un propósito comercial aparente. Debe sospecharse especialmente de las entidades comerciales nacionales cuyos nombres son similares a los de bancos pero que carecen de autoridad regulatoria para realizar operaciones bancarias.[265]

Los siguientes indicadores de actividades potencialmente sospechosas están comúnmente asociados a las actividades de compañías fantasma:

- Información insuficiente o nula disponible para identificar claramente los remitentes o beneficiarios de transferencias de fondos (a través de Internet, búsquedas en bases de datos comerciales o consultas directas a un banco corresponsal).
- Los pagos no exhiben un propósito declarado, no hacen referencia a ningún bien o servicio, o identifican únicamente a un contrato o número de factura.
- Los bienes o servicios, si se los identifica, no coinciden con el perfil de la compañía proporcionado por el banco respondiente o el carácter de la actividad financiera; una compañía hace referencia a bienes y servicios notablemente diferentes en transferencias de fondos relacionadas; la explicación dada por el banco respondiente extranjero no es coherente con la actividad de transferencias de fondos observada.
- Los comercios involucrados en la transacción comparten la misma dirección o proporcionan sólo la dirección de un agente registrado; o existen otras incoherencias relacionadas con las direcciones.
- Muchas o todas las transferencias de fondos se transmiten en sumas de grandes volúmenes, redondeadas y en cientos o miles de dólares.
- Grandes cantidades y variedades poco habituales de beneficiarios que reciben transferencias de fondos de una sola compañía.
- Participación frecuente de múltiples jurisdicciones o beneficiarios que se encuentran en OFC de mayor riesgo.

---

[264] La falta de identificación sobre los propietarios de compañías impide la aplicación de la ley. Consulte la Sesión 109-845 del Senado, llevada a cabo el 14 de Noviembre de 2006.

[265] Las agencias bancarias federales notifican a los bancos y al público sobre las entidades que participan en actividades bancarias no autorizadas, tanto nacionales como en el exterior. Estas notificaciones se pueden encontrar en los sitios Web de las agencias bancarias federales.

- Un banco corresponsal extranjero excede el volumen previsto en el perfil de su cliente con respecto a las transferencias de fondos, o una compañía particular exhibe un gran volumen y un patrón de transferencias de fondos que no es coherente con su actividad comercial habitual.

- Múltiples pagos o transferencias de grandes sumas entre compañías fantasma sin propósito comercial legítimo aparente.

- El propósito de la compañía fantasma es desconocido o no está claro.

Mitigación del riesgo

La gerencia debe desarrollar políticas, procedimientos y procesos que le permitan al banco identificar las relaciones asociadas con las cuentas, especialmente las cuentas de depósito, de entidades comerciales y vigilar los riesgos asociados con estas cuentas en todos los departamentos del banco. Los clientes de las entidades comerciales pueden abrir cuentas en el departamento de banca privada, el departamento fiduciario o en sucursales locales. La gerencia debe establecer una debida diligencia especial adecuada al momento de la apertura de la cuenta y en tanto la relación dure, para administrar el riesgo de dichas cuentas. El banco debe recopilar suficiente información sobre las entidades comerciales y sus usufructuarios para conocer y analizar los riesgos de la relación asociada con la cuenta. Entre la información más importante para determinar el uso lícito de estas entidades se incluyen: el tipo de negocio, el propósito de la cuenta, la fuente de los fondos y la fuente de la riqueza del propietario o usufructuario.

El Programa de identificación de clientes (CIP) del banco debe detallar las exigencias de identificación para la apertura de una cuenta de una entidad comercial. Al abrir una cuenta a un cliente que no es un individuo, de acuerdo a 31 CFR 103.121 los bancos pueden obtener información sobre los individuos que ejercen autoridad y control sobre dichas cuentas para verificar la identidad del cliente (siendo el cliente la entidad comercial). La información que se requiere para abrir una cuenta puede incluir las actas constitutivas, una resolución corporativa adoptada por sus directores autorizando la apertura de la cuenta, o la designación de una persona para actuar como firmante de la cuenta en representación de la entidad. Debe prestarse especial atención a los estatutos de asociación que permiten la existencia de accionistas fiduciarios, miembros de la junta directiva y acciones al portador.

Si a través de sus departamentos fiduciarios o de banca privada, el banco facilita a clientes nuevos o actuales el establecimiento de entidades comerciales, el riesgo de lavado de dinero por lo general se reduce. Puesto que el banco conoce a las partes (p. ej., contribuyentes, beneficiarios y accionistas) involucradas en la entidad comercial, la debida diligencia inicial y la verificación se realizan más fácilmente. Además, en dichos casos, el banco mantiene con frecuencia relaciones continuas con los clientes que participan en el establecimiento de una entidad comercial.

El análisis de riesgos puede incluir un control de la jurisdicción nacional o internacional en donde se estableció la entidad comercial, el tipo de cuenta (o cuentas) y las actividades previstas comparadas con las actividades transaccionales reales, los tipos de productos

que se utilizarán y si la entidad empresarial fue creada interna o externamente. Si la propiedad se detenta mediante acciones al portador, el banco debe analizar los riesgos que estas relaciones plantean y determinar los controles adecuados. Por ejemplo, en la mayoría de los casos los bancos deberían optar por mantener (o solicitar a un tercero que mantenga) las acciones al portador de los clientes. En algunos casos poco frecuentes que implican un riesgo menor, es posible que a los bancos les resulte eficaz recertificar periódicamente el usufructo de los clientes conocidos ya establecidos. El análisis efectuado por el banco del riesgo que implica una entidad comercial se vuelve más significativo en las constituciones corporativas complejas. Por ejemplo, una IBC extranjera puede constituir una serie estratificada de entidades comerciales, cada una de las cuales nombre a su compañía matriz como su beneficiaria.

Es esencial ejercer una supervisión continua de las cuentas con el objetivo de garantizar que sean controladas para detectar actividades sospechosas o poco habituales. El banco debe conocer las transacciones de mayor riesgo efectuadas en dichas cuentas, como las actividades sin propósito comercial o legítimo aparente, las actividades de transferencias de fondos desde y hacia jurisdicciones de mayor riesgo, las transacciones intensivas en moneda y los cambios frecuentes en la propiedad o el control de las entidades comerciales privadas.

Procedimientos de inspección

Entidades comerciales (nacionales y extranjeras)

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transacciones que involucren entidades comerciales nacionales y extranjeras y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las entidades comerciales. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las transacciones del banco con entidades comerciales y los riesgos que plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Revise las políticas y los procesos para la apertura y la supervisión de cuentas con entidades comerciales. Determine si las políticas analizan el riesgo entre los diferentes tipos de cuentas de manera adecuada.

3. Determine la manera en que el banco identifica y, según sea necesario, aplica debida diligencia adicional a las entidades comerciales. Analice el nivel de debida diligencia que el banco lleva a cabo cuando realiza el análisis de riesgos.

4. De un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa *de manera eficaz* las cuentas de entidades comerciales de alto riesgo.

5. Determine si el sistema del banco para supervisar las entidades comerciales, e informar acerca de actividades sospechosas, es adecuado en función de las actividades asociadas con las entidades comerciales.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus cuentas con entidades comerciales, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de estas cuentas. Incluya los siguientes factores de riesgo:

   - Una entidad organizada en una jurisdicción de más alto riesgo.
   - La actividad de cuenta está basada sustancialmente en moneda.
   - Una entidad cuya actividad de cuenta consiste principalmente en transferencias de fondos con patrones circulares.

- Una entidad comercial cuya propiedad se detenta por medio de acciones al portador, especialmente aquellas que no están bajo el control de un tercero confiable o del banco.
- Una entidad que utiliza un amplio rango de servicios bancarios, particularmente servicios corresponsales y fiduciarios.
- Una entidad de propiedad de otras entidades comerciales privadas o controlada por éstas.
- Las entidades comerciales respecto a las cuales el banco haya presentado SAR.

8. De la muestra seleccionada, obtenga informes de las relaciones asociadas a cada cuenta elegida. Es esencial que se revise la relación completa, y no únicamente una cuenta particular.
9. Revise la información de debida diligencia sobre la entidad comercial. Analice la aptitud de esa información.
10. Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones. Compare las transacciones previstas con la actividad real. Determine si la actividad real es coherente con el carácter y el propósito declarado de la cuenta y si las transacciones parecen sospechosas o poco habituales. Las áreas que plantean un riesgo más alto, como las transferencias de fondos, la banca privada, los fideicomisos y los instrumentos monetarios, deben ser el enfoque principal del control de las transacciones.
11. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados a las relaciones con entidades comerciales.

Negocios Intensivos en Efectivo: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las entidades y los negocios con actividad intensiva en efectivo, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Las entidades y los negocios con actividad intensiva en efectivo están presentes en distintos sectores de la industria. La mayoría de ellos realiza negocios lícitos; sin embargo, algunos aspectos de estos negocios pueden ser susceptibles al lavado de dinero o al financiamiento del terrorismo. Los ejemplos comunes incluyen, entre otros, los siguientes:

- Minimercados.
- Restaurantes.
- Tiendas minoristas.
- Licorerías.
- Distribuidores de cigarrillos.
- Cajeros automáticos (ATM) de propiedad privada.
- Operadores de máquinas expendedoras.
- Garajes de estacionamiento de vehículos.

Factores de riesgo

Algunos negocios y entidades pueden ser mal utilizados por lavadores de dinero para legitimar sus ingresos ilícitos. Por ejemplo, un delincuente puede ser el propietario de un negocio intensivo en efectivo, como un restaurante, y usarlo para lavar dinero proveniente de actividades delictivas ilícitas. Los depósitos de dinero que hace el restaurante en su banco no son en apariencia poco habituales porque el negocio es legítimamente una entidad generadora de efectivo. Sin embargo, el volumen de moneda que maneja un restaurante que se utiliza para lavar dinero será muy probablemente mayor en comparación con restaurantes similares de la zona. El carácter de los negocios intensivos en efectivo y la dificultad para identificar las actividades poco habituales pueden hacer que estos negocios sean considerados de más alto riesgo.

Mitigación del riesgo

Al establecer y mantener relaciones con negocios intensivos en efectivo, los bancos deben fijar políticas, procedimientos y procesos para identificar las relaciones de alto riesgo; analizar el riesgo de lavado de dinero; realizar debida diligencia en el momento de apertura

de cuentas y periódicamente durante la relación; e incluir dichas relaciones en la supervisión adecuada de actividades poco habituales y sospechosas. En el momento de apertura de una cuenta, el banco debe conocer las operaciones comerciales del cliente, el uso deseado de la cuenta, incluidos el volumen previsto de transacciones, los productos y servicios utilizados; y las ubicaciones geográficas implicadas en la relación.

Cuando llevan a cabo el análisis de riesgos de negocios intensivos en efectivo, los bancos deben dirigir sus recursos hacia las cuentas que presenten el mayor riesgo de lavado de dinero y financiamiento del terrorismo. Los siguientes factores pueden utilizarse para identificar los riesgos:

- Propósito de la cuenta.
- Volumen, frecuencia y carácter de las transacciones en efectivo.
- Antecedentes del cliente (por ej. duración de la relación, presentaciones de CTR[266] y presentaciones de SAR).
- Actividad principal del negocio, productos y servicios ofrecidos.
- Tipo de negocio o estructura comercial.
- Ubicaciones geográficas y jurisdicciones donde se realizan las operaciones.
- Disponibilidad de información y cooperación del negocio para suministrar información.

Respecto a aquellos clientes considerados particularmente de alto riesgo, la gerencia del banco puede considerar la implementación de prácticas responsables, tales como visitas periódicas en el sitio, entrevistas con la gerencia del negocio, o controles detallados de la actividad transaccional.

[266] Como se describe en la sección del esquema general principal, “Exenciones al informe de transacciones en efectivo”, en las páginas 100 a 105, algunas entidades no califican para las exenciones a las transacciones en efectivo como empresas que no cotizan en la bolsa

Procedimientos de inspección

Negocios intensivos en efectivo

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las entidades y los negocios con actividad intensiva en efectivo, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos relacionados con los negocios intensivos en efectivo. Evalúe la aptitud de las políticas, los procedimientos y los procesos según las actividades asociadas a negocios intensivos en efectivo del banco relacionados con sus clientes de negocios intensivos en efectivo y los riesgos que representan. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. De un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa *de manera eficaz* las entidades y los negocios intensivos en efectivo.

3. Determine si el sistema del banco para supervisar las actividades sospechosas de los negocios intensivos en efectivo y para informar acerca de actividades sospechosas es adecuado en relación con su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con los clientes.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus relaciones con las entidades y los negocios con actividad intensiva en efectivo, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de negocios intensivos en efectivo. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de cuenta incluida la información del Programa de identificación de clientes (CIP), si corresponde, y una muestra de la actividad transaccional.

   - Determine si la actividad real de la cuenta es coherente con la actividad prevista de la cuenta.

   - Identifique las tendencias en el carácter, el tamaño o el campo de aplicación de las transacciones, prestando especial atención a las transacciones en efectivo.

   - Determine si la supervisión continua es suficiente para identificar las actividades potencialmente sospechosas.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las entidades y los negocios con actividad intensiva en efectivo.

Apéndice A: Normativa de la BSA

Leyes

12 USC 1829b, 12 USC 1951–1959, y 31 USC 5311, *et seq*. "The Bank Secrecy Act" ("La ley de secreto bancario")

12 USC 1818(s): "Compliance with Monetary Recordkeeping and Report Requirements" (Cumplimiento de las exigencias de gestión de registros y presentación de informes monetarios)
Exige que las agencias bancarias federales respectivas emitan reglamentos que insten a las instituciones de depósito aseguradas a establecer y mantener procedimientos razonablemente diseñados para asegurar y supervisar el cumplimiento de dichas instituciones de depósito con las exigencias de la BSA. Además, esta sección exige que cada inspección de institución de depósito asegurada realizada por la agencia bancaria federal apropiada incluya un control de los procedimientos, y que el informe de inspección describa cualquier problema con los procedimientos mantenidos por la institución de depósito asegurada. Finalmente, si la agencia bancaria federal correspondiente determina que una institución de depósito asegurada 1) no ha establecido y mantenido procedimientos razonablemente diseñados para asegurar y supervisar el cumplimiento de la institución con la BSA, o 2) no ha solucionado cualquier problema con los procedimientos que un informe de inspección u otra comunicación escrita de supervisión haya identificado como un asunto que era necesario informar a la junta directiva o la alta gerencia de la institución para su corrección, la agencia debe emitir una orden intimando a dicha institución de depósito a cesar y desistir de esa violación a las leyes y reglamentos establecidos de acuerdo a las mismas. Las secciones 1818(b)(3) y (b)(4) del Título 12 de la sección ampliada 1818(s) del USC además de instituciones de depósito aseguradas.

12 USC 1786(q): "Compliance with Monetary Recordkeeping and Report Requirements" (Cumplimiento de las exigencias de gestión de registros y presentación de informes monetarios)
Exige que la junta de la NCUA emita reglamentos que insten a las cooperativas de crédito aseguradas a establecer y mantener procedimientos razonablemente diseñados para asegurar y supervisar el cumplimiento de dichas cooperativas de crédito con las exigencias de la BSA. Además, esta sección exige que la junta de la NCUA inspeccione y haga cumplir las exigencias de la BSA.

Reglamentos

Tesoro de Estados Unidos/FinCEN

31 CFR 103: "Financial Recordkeeping and Reporting of Currency and Foreign Transactions" (Gestión de registros y presentación de informes en materia de transacciones extranjeras y en moneda)
Establece los reglamentos de la FinCEN que promulgan la BSA. Las disposiciones seleccionadas están descritas a continuación.

31 CFR 103.11: "Meaning of Terms" (Significados de los términos)
Establece las definiciones utilizadas en 31 CFR Parte 103.

31 CFR 103.16: "Reports by Insurance Companies of Suspicious Transactions" (Informes de las compañías de seguros sobre transacciones sospechosas)
Establece las exigencias de que las compañías de seguros informen las transacciones sospechosas de USD 5.000 o más.

31 CFR 103.18: "Reports by Banks of Suspicious Transactions" (Informes de los bancos sobre transacciones sospechosas)
Establece las exigencias de que los bancos informen las transacciones sospechosas de USD 5.000 o más.

31 CFR 103.22: "Reports of Transactions in Currency" (Informes de transacciones en efectivo)
Establece las exigencias de que las instituciones financieras informen las transacciones en efectivo que superen los USD 10.000. Incluye 31 CFR 103.22(d): "Transactions of Exempt Persons" (Transacciones de personas exentas) que establece las exigencias de que las instituciones financieras eximan a las transacciones de determinadas personas de la obligación de informe de transacciones en efectivo.

31 CFR 103.23: "Reports of Transportation of Currency or Monetary Instruments" (Informe sobre el transporte de moneda o instrumentos monetarios)
Establece las exigencias para presentar un informe sobre moneda o sobre instrumentos monetarios (CMIR).

31 CFR 103.24: "Reports of Foreign Financial Accounts" (Informes de cuentas financieras extranjeras)
Establece la exigencia de que cada persona que tenga intereses financieros, o firma, o algún otro tipo de autoridad sobre una cuenta financiera en un país extranjero debe presentar un informe ante el Servicio de Impuestos Internos anualmente.

31 CFR 102.27: "Filing of Reports" (Presentación de informes)
Establece las exigencias de presentación y conservación de registros de los CTR, CMIR, y del Informe de cuentas bancarias y financieras extranjeras (FBAR).

31 CFR 103.28: "Identification Required" (Identificación exigida)
Establece la exigencia de que las instituciones financieras verifiquen la identidad de las personas que realizan transacciones en efectivo que superen los USD 10.000.

31 CFR 103.29: "Purchases of Bank Checks and Drafts, Cashier's Checks, Money Orders, and Traveler's Checks" (Compras de cheques de banco y giros, cheques de caja, giros postales y cheques de viajero)
Establece las exigencias de que las instituciones financieras mantengan registros relacionados con compras de instrumentos monetarios en efectivo por montos de entre USD 3.000 y USD 10.000.

31 CFR 103.32: "Records to Be Made and Retained by Persons Having Financial Interests in Foreign Financial Accounts" (Registros que deben realizar y conservar las personas que tienen intereses financieros en cuentas financieras extranjeras)
Establece la exigencia de que las personas que tengan intereses financieros, o firma o algún otro tipo de autoridad sobre una cuenta financiera en un país extranjero mantengan registros relacionados con las cuentas bancarias financieras extranjeras informadas en un FBAR.

31 CFR 103.33: "Records to Be Made and Retained by Financial Institutions" (Registros que deben realizar y conservar las instituciones financieras)
Establece las exigencias de recuperación y gestión de registros de las instituciones financieras, incluidas las exigencias sobre transmisión y gestión de registros de transferencias de fondos.

31 CFR 103.34: "Additional Records to Be Made and Retained by Banks" (Registros adicionales que deben realizar y conservar los bancos)
Establece exigencias adicionales sobre gestión de registros que deben cumplir los bancos.

31 CFR 103.38: "Nature of Records and Retention Period" (Carácter de los registros y período de conservación)
Establece las formas de registro aceptables que se deben mantener y la exigencia de conservación de registros durante cinco años.

31 CFR 103.41: "Registration of Money Services Businesses" (Registro de negocios de servicios de dinero)
Exigencias de que los negocios de servicios monetarios se registren ante el Tesoro de Estados Unidos/FinCEN.

31 CFR 103.57: "Civil Penalty" (Sanciones civiles)
Establece sanciones civiles potenciales por violaciones dolosas o culposas de 31 CFR Parte 103.

31 CFR 103.59: "Criminal Penalty" (Sanciones penales)
Establece sanciones penales potenciales por violaciones dolosas de 31 CFR Parte 103.

31 CFR 103.63:"Structured Transactions" (Transacciones fraccionadas)
Prohíbe el fraccionamiento de transacciones para evitar la exigencia de declaración de transacciones en efectivo.

31 CFR 103.100: "Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions" (Intercambio de información entre agencias federales de aplicación de la ley e instituciones financieras)
Establece procedimientos para compartir información entre las agencias federales de aplicación de la ley y las instituciones financieras para impedir las actividades terroristas y de lavado de dinero.

31 CFR 103.110: "Voluntary Information Sharing Among Financial Institutions" (Intercambio de información voluntario entre instituciones financieras"
Establece procedimientos aplicables al intercambio de información voluntario entre instituciones financieras para impedir las actividades terroristas y de lavado de dinero.

31 CFR 103.120: "Anti-Money Laundering Program Requirements for Financial Institutions Regulated by a Federal Functional Regulator or a Self-Regulatory Organization, and Casinos" (Exigencias del programa contra el lavado de dinero para las instituciones financieras reguladas por un regulador funcional federal o una organización autoregulada, y casinos)
Establece, en parte, la norma de que una institución financiera regulada únicamente por un regulador funcional federal satisface las exigencias legales para establecer un programa AML si cumple con los reglamentos de su regulador funcional federal, que rigen tales programas.

31 CFR 103.121: "Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks" (Programas de identificación de clientes para bancos, asociaciones de ahorro, cooperativas de crédito y determinados bancos no regulados por agencias federales)
Establece las exigencias de que los bancos, las asociaciones de ahorro, las cooperativas de crédito y determinados bancos no regulados por agencias federales implementen un Programa de identificación de clientes por escrito.

31 CFR 103.137: "Anti-Money Laundering Programs for Insurance Companies" (Programas contra el lavado de dinero para compañías de seguros)
Establece la exigencia de que las compañías de seguros que emitan o garanticen "productos cubiertos" desarrollen e implementen un programa AML escrito que esté razonablemente diseñado para evitar que la compañía de seguros sea utilizada para facilitar actividades de financiamiento del terrorismo y de lavado de dinero.

31 CFR 103.176: "Due Diligence Programs for Correspondent Accounts for Foreign Financial Institutions" (Pogramas de debida diligencia aplicables a cuentas corresponsales para instituciones financieras extranjeras)
Establece la exigencia de determinadas instituciones financieras de establecer y aplicar un programa de debida diligencia que incluya políticas y procedimientos adecuados, específicos, en función del riesgo y, cuando sea necesario, especiales, que estén razonablemente diseñados para permitir que la institución detecte e informe actividades de lavado de dinero de las que se sospeche o tenga conocimiento que involucren o se realicen por medio de cualquier cuenta corresponsal establecida, mantenida, administrada o gestionada por la institución financiera de Estados Unidos para una institución financiera extranjera.

31 CFR 103.177 — "Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process" (Prohibición de cuentas corresponsales para bancos fantasmas extranjeros, registros sobre propietarios de bancos extranjeros y agentes de notificaciones de demanda)
Prohíbe que una institución financiera cubierta establezca, mantenga, administre o gestione una cuenta corresponsal en Estados Unidos con un banco fantasma extranjero o en su nombre y exige que la institución financiera conserve los registros que identifiquen a los propietarios de las instituciones financieras extranjeras y con respecto a la persona que reside en Estados Unidos que está autorizada o acordó ser agente para recibir notificaciones de demanda.

31 CFR 103.178: "Due Diligence Programs for Private Banking Accounts" (Programas de debida diligencia para cuentas de banca privada)
Determina la exigencia de que algunas instituciones financieras establezcan y mantengan un programa de debida diligencia que incluya políticas, procedimientos y controles que estén razonablemente diseñados para detectar e informar cualquier actividad sospechosa o de lavado de dinero de la que se sospeche o tenga conocimiento llevada a cabo a través de cualquier cuenta de banca privada o que involucre cualquier cuenta de banca privada para un ciudadano no estadounidense que esté establecida, mantenida, administrada o gestionada en Estados Unidos.

31 CFR 103.185: "Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship" (Auto de comparecencia o citación relacionada con los registros del banco extranjero; terminación de la relación corresponsal)
Exige que una institución financiera proporcione registros de instituciones financieras extranjeras a solicitud del funcionario de aplicación de la ley correspondiente y que interrumpa la relación corresponsal con una institución financiera extranjera al recibir una notificación por escrito del Secretario del Tesoro de Estados Unidos o del Procurador General de Estados Unidos.

31 CFR 103, Subparte I, Apéndice A: "Certification Regarding Correspondent Accounts for Foreign Banks" (Certificaciones relacionadas con cuentas corresponsales para bancos extranjeros)
Formularios de certificación voluntaria que debe llenar un banco que establece, mantiene, administra o gestiona una cuenta corresponsal en Estados Unidos para un banco extranjero o en su nombre.

31 CFR 103, Subparte I, Apéndice A: "Recertification Regarding Correspondent Accounts for Foreign Banks" (Recertificaciones relacionadas con cuentas corresponsales para bancos extranjeros)
Formularios de recertificación voluntaria que debe llenar un banco que establece, mantiene, administra o gestiona una cuenta corresponsal en Estados Unidos para un banco extranjero o en su nombre.

Junta de Gobernadores del Sistema de Reserva Federal

Reglamento H: 12 CFR 208.62: "Suspicious Activity Reports"
(Informe de actividades sospechosas)
Establece la exigencias para que los bancos que sean miembros estatales presenten un SAR ante las agencias federales de aplicación de la ley correspondientes y el Tesoro de Estados Unidos.

Reglamento H: 12 CFR 208.63: "Procedures for Monitoring Bank Secrecy Act Compliance" (Procedimientos para supervisar el cumplimiento de la ley de secreto bancario)
Establece las exigencias de que los bancos que sean miembros estatales establezcan y mantengan procedimientos para asegurar y supervisar su cumplimiento con la BSA.

Reglamento K: 12 CFR 211.5 (k): "Reports by Edge and Agreement Corporations of Crimes and Suspected Crimes" (Informes por parte de las corporaciones que se rigen por la Ley de organizaciones bancarias extranjeras y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal sobre delitos y sospechas de delitos)
Establece las exigencias de que una corporación que se rige por la Ley de organizaciones bancarias extranjeras y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal o cualquier sucursal o subsidiaria de la misma, presente un SAR ante las agencias federales de aplicación de la ley correspondientes y el Tesoro de Estados Unidos.

Reglamento K: 12 CFR 211.5: "Procedures for Monitoring Bank Secrecy Act Compliance" (Procedimientos para supervisar el cumplimiento de la Ley de secreto bancario)
Establece las exigencias de que una corporación que se rige por la Ley de organizaciones bancarias extranjeras y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal establezca y mantenga procedimientos razonablemente diseñados para asegurar y supervisar el cumplimiento con la BSA y los reglamentos relacionados.

Reglamento K: 12 CFR 211.24 (f): "Reports of Crimes and Suspected Crimes" (Informes de delitos y sospechas de delitos)
Establece la exigencia de que una sucursal no asegurada, una agencia o una oficina representativa de una institución financiera extranjera que opere en los Estados Unidos presente un SAR ante las agencias federales de aplicación de la ley correspondientes y el Tesoro de Estados Unidos.

Reglamento K: 12 CFR 211.24 (j): "Procedures for Monitoring Bank Secrecy Act Compliance" (Procedimientos para supervisar el cumplimiento de la ley de secreto bancario)
Establece la exigencia de que una sucursal no asegurada, una agencia o una oficina representativa de una institución financiera extranjera que opere en Estados Unidos establezca y mantenga procedimientos razonablemente diseñados para asegurar y supervisar el cumplimiento con la BSA y los reglamentos relacionados.

Reglamento Y: 12 CFR 225.4 (f): "Suspicious Activity Report" (Informe de actividades sospechosas)
Establece las exigencias de que una sociedad de control de bancos o cualquier subsidiaria no bancaria de la misma, un banco extranjero que esté sujeto a la Ley de sociedad de control de bancos o cualquier subsidiaria no bancaria de dicho banco extranjero que opere en Estados Unidos presente un SAR ante las agencias federales de aplicación de la ley correspondientes y el Tesoro de Estados Unidos.

Corporación Federal de Seguro de Depósitos

12 CFR 326 Subparte B: "Procedures for Monitoring Bank Secrecy Act Compliance" (Procedimientos para supervisar el cumplimiento de la Ley de secreto bancario)
Establece la exigencia de que los bancos que no son miembros estatales establezcan y mantengan procedimientos para asegurar y supervisar su cumplimiento de la BSA.

12 CFR 353: "Suspicious Activity Reports" (Informes de actividades sospechosas)
Establece la exigencia de que los bancos que no son miembros estatales presenten un SAR cuando sospechen o tengan conocimiento de una violación a la ley federal, una transacción sospechosa relacionada con una actividad de lavado de dinero o una violación a la BSA.

Administración Nacional de Cooperativas de Crédito

12 CFR 748: "Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance" (Programa de seguridad, ley de informe de delitos y catástrofes y cumplimiento de la ley de secreto bancario)
Exige que las cooperativas de crédito con seguro federal mantengan programas de seguridad y cumplan con la BSA.

12 CFR 748.1: "Filing of Reports" (Presentación de informes)
Exige que las cooperativas de crédito con seguro federal presenten informes de actividades sospechosas y sobre cumplimiento.

12 CFR 748.2: "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance" (Procedimientos para supervisar el cumplimiento de la ley de secreto bancario (BSA))

Asegura que todas las cooperativas de crédito con seguro federal establezcan y mantengan procedimientos razonablemente diseñados para asegurar y supervisar el cumplimiento de las exigencias de la BSA sobre gestión de registros y presentación de informes.

Oficina del Interventor Monetario

12 CFR 21.11: "Suspicious Activity Report" (Informe de actividades sospechosas)
Asegura que los bancos nacionales presenten un Informe de actividades sospechosas cuando sospechan o tienen conocimiento de una violación a la ley federal o de una transacción sospechosa relacionada con una actividad de lavado de dinero o una violación a la BSA. Esta sección se aplica a todos los bancos nacionales, así como a cualquier sucursal federal y agencias de bancos financieros extranjeros que obtuvieron licencia o fueron autorizados por la OCC.

12 CFR 21.21: "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance" (Procedimientos para supervisar el cumplimiento de la Ley de secreto bancario)
Establece la exigencia de que todos los bancos nacionales establezcan y mantengan procedimientos razonablemente diseñados para asegurar y supervisar el cumplimiento con los requisitos del subcapítulo II del capítulo 53, título 31, Código de Estados Unidos, y la implementación de reglamentos promulgados de conformidad con los últimos por el Departamento del Tesoro en 31 CFR parte 103.

Oficina de Supervisión de Instituciones de Ahorro

12 CFR 563.177: "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance" (Procedimientos para supervisar el cumplimiento de la Ley de secreto bancario)
Establece la exigencia de que las instituciones de ahorro deben implementar un programa para cumplir con las exigencias de la BSA sobre presentación y mantenimiento de registros.

12 CFR 563.180: "Suspicious Activity Reports and Other Reports and Statements" (Informes de actividades sospechosas y otros informes y declaraciones)
Establece las normas para que las asociaciones de crédito o corporaciones de servicios presenten un SAR ante las agencias federales de aplicación de la ley correspondientes y el Tesoro de Estados Unidos.

Apéndice B: Directivas BSA/AML

Junta de Gobernadores del Sistema de Reserva Federal

Las Cartas de Supervisión y Reglamento, comúnmente conocidas como Cartas de SR, abordan asuntos significativos sobre políticas y procedimientos relacionados con las responsabilidades de supervisión del Sistema de Reserva Federal. Expedidas por la División de Supervisión y Reglamento Bancarios de la Junta de Gobernadores, las Cartas de SR constituyen un medio importante de divulgación de información para el personal de supervisión bancaria de la Junta de Gobernadores y los bancos de la Reserva y, en algunas ocasiones, para organizaciones bancarias supervisadas. Las Cartas de SR BSA/AML aplicables están disponibles en el siguiente sitio Web: www.federalreserve.gov/boarddocs/srletters.

Corporación Federal de Seguro de Depósitos

Las Cartas de Instituciones Financieras (FIL, por sus siglas en inglés) están dirigidas a los directores ejecutivos de las instituciones financieras enumeradas en la lista de distribución de las FIL, que generalmente son bancos supervisados por la FDIC. Las FIL pueden anunciar nuevas políticas y reglamentos, nuevas publicaciones de la FDIC y diversos asuntos de interés principal para quienes son responsables de la operación de un banco o una asociación de ahorro. Las FIL aplicables están disponibles en el siguiente sitio Web: www.fdic.gov/news/news/financial/index.html.

Administración Nacional de Cooperativas de Crédito

La Administración Nacional de Cooperativas de Crédito (NCUA, por sus siglas en inglés) publica Cartas a las Cooperativas de Crédito (LCU, por sus siglas en inglés) y Alertas normativas (RA, por sus siglas en inglés) destinadas a las juntas directivas de cooperativas de crédito. Las LCU y RA se utilizan para compartir información, anunciar nuevas políticas y proporcionar guía a las cooperativas de crédito y al personal de inspección de dichas cooperativas. La Guía del inspector de la NCUA proporciona una guía general para la inspección y supervisión orientadas al riesgo de las cooperativas de crédito con seguro federal. El programa orientado al riesgo de la NCUA evalúa el grado en que la gerencia de las cooperativas de crédito identifica, mide, supervisa y controla (es decir, gestiona) los riesgos potenciales y existentes en sus operaciones, incluidos los riesgos asociados con los programas AML. Las secciones aplicables de la Guía del inspector están disponibles en el siguiente sitio Web: www.ncua.gov.

Oficina del Interventor Monetario

Las alertas de la Oficina del Interventor Monetario (OCC, por sus siglas en inglés) son publicaciones emitidas con urgencia especial para notificar a los banqueros e inspectores sobre asuntos de preocupación apremiante, que son con frecuencia prácticas bancarias ilegales o sospechosas. Los Boletines y Cartas informativas de la OCC contienen información de importancia invariable para banqueros e inspectores. Estos Boletines y

Cartas permanecen en vigencia hasta que se revean o revoquen. Las Alertas, Boletines y Cartas informativas BSA/AML de la OCC específicas están disponibles en el siguiente sitio Web: www.occ.treas.gov.

Oficina de Supervisión de Instituciones de Ahorro

La Oficina de Supervisión de Instituciones de Ahorro expide Boletines normativos y Cartas a los directores ejecutivos para aclarar reglamentos y especificar pautas y procedimientos. Estas instrucciones constituyen un medio importante para poner a los inspectores y las asociaciones de ahorro al corriente de manera continua sobre los asuntos BSA/AML. Las Cartas a los directores ejecutivos y los Boletines normativos BSA/AML específicos están disponibles en el siguiente sitio Web: www.ots.treas.gov.

Apéndice C: Referencias BSA/AML

Sitios Web:

Junta de Gobernadores del Sistema de Reserva Federal
www.federalreserve.gov

Corporación Federal de Seguro de Depósitos
www.fdic.gov

Administración Nacional de Cooperativas de Crédito
www.ncua.gov

Oficina del Interventor Monetario
www.occ.treas.gov

Oficina de Supervisión de Instituciones de Ahorro
www.ots.treas.gov

Red de Lucha contra Delitos Financieros
www.fincen.gov

Oficina de Control de Activos Extranjeros
www.treasury.gov/offices/enforcement/ofac

Consejo Federal de Inspección de Instituciones Financieras
www.ffiec.gov

Manuales o libros de instrucciones

Federal Reserve Commercial Bank Examination Manual (Manual de inspección de bancos comerciales de la Reserva Federal)

Federal Reserve Bank Holding Company Supervision Manual (Manual de supervisión de sociedades de control de bancos de la Reserva Federal)

Federal Reserve Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations (Manual de inspección de la Reserva Federal para sucursales estadounidenses y agencias de organizaciones bancarias extranjeras)

Federal Reserve Guidelines and Instructions for Examinations of Edge Corporations (Pautas e instrucciones de la Reserva Federal para las inspecciones de corporaciones que se rigen por la Ley de organizaciones bancarias extranjeras)

FDIC Manual of Examination Policies (Manual de políticas de inspección de la FDIC)

NCUA Compliance Self-Assessment Manual (Manual de autoevaluación del cumplimiento con la NCUA)

NCUA Examiner's Guide (Guía del inspector de la NCUA)

OCC Comptroller's Handbook — Asset Management (Libro de instrucciones del Interventor de la OCC: gestión de activos)

OCC Comptroller's Handbook — Community Bank Supervision (Libro de instrucciones del Interventor de la OCC: supervisión de bancos comunitarios)

OCC Comptroller's Handbook — Compliance (Libro de instrucciones del Interventor de la OCC: cumplimiento)

OCC Comptroller's Handbook — Large Bank Supervision (Libro de instrucciones del Interventor de la OCC: supervisión de grandes bancos)

OCC Money Laundering: A Banker's Guide to Avoiding Problems (OCC y el Lavado de dinero: una guía para banqueros a fin de que eviten problemas)

OTS Examination Handbook (Libro de instrucciones de inspección de la OTS)

Otros materiales

Consejo Federal de Inspección de Instituciones Financieras (FFIEC)

El sitio Web del FFIEC (www.ffiec.gov) incluye la siguiente información:

- Base de información del Manual de inspección BSA/AML (en inglés, *BSA/AML Examination Manual InfoBase*).
- Base de información del Manual de instrucciones de tecnología de la información (en inglés, *Information Technology Handbook InfoBase*).

Gobierno de los Estados Unidos

Interagency U.S. Money Laundering Threat Assessment (MLTA) (Evaluación Interinstitucional de Estados Unidos sobre Amenazas de Lavado de Dinero) (Diciembre de 2005)

El MLTA es un análisis que se hace en todo el gobierno del lavado de dinero en Estados Unidos. El MLTA ofrece un análisis detallado de los métodos de lavado de dinero, que incluye desde las técnicas más consolidadas para integrar dinero sucio al sistema financiero hasta las innovaciones más modernas para sacar provecho de las redes de pago global, como también de Internet.
(www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf)

Red de Lucha contra Delitos Financieros (FinCEN)

El sitio Web de FinCEN (www.fincen.gov) incluye lo siguiente, entre distintos tipos de material e información:

- Material legal BSA, Reglamentos de la BSA y Notificaciones del Registro Federal; enlaces a legislación, reglamentos y reglamentaciones propuestas.

- Formularios de la BSA: vínculos a los formularios de informes de la BSA e instrucciones para la preparación y presentación.
- Guía de BSA: temas de FinCEN, interpretación de reglamentaciones de BSA, más una guía para que las instituciones financieras cumplan con ellas.
- Informes: FinCEN periódicamente inicia y elabora informes y publicaciones sobre temas de AML, incluso Control de la actividad del SAR.
- Dictámenes: FinCEN emite dictámenes para instituciones financieras sobre temas de lavado de dinero o amenazas de financiamiento a terroristas y vulnerabilidades, a los efectos de que las instituciones financieras puedan protegerse de este tipo de amenazas.
- Medidas coercitivas de cumplimiento: FinCEN publica comunicados sobre la evaluación de sanciones monetarias civiles para instituciones financieras por un incumplimiento sistemático de la BSA.

Comité de Supervisión Bancaria de Basilea (BCBS)

El sitio Web del BCBS (en el sitio Web del Banco de Pagos Internacionales www.bis.org) incluye las siguientes publicaciones:

- *Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers* (Diligencia debida y transparencia en mensajes sobre pagos de cobertura relacionados con transferencias internacionales).
- *Consolidated Know Your Customer Risk Management* (Gestión de riesgos conozca su cliente consolidada).
- *Sharing of Financial Records Between Jurisdictions in Connection with the Fight Against Terrorist Financing* (Intercambio de registros financieros entre jurisdicciones en relación con la lucha contra el financiamiento del terrorismo).
- *General Guide to Account Opening and Customer Identification* (Guía general para apertura de cuentas e identificación de clientes).
- *Customer Due Diligence for Banks* (Debida diligencia de los clientes para bancos).
- *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* (Prevención del uso delictivo del sistema bancario para fines de lavado de dinero).
- *Banking Secrecy and International Cooperation in Banking Supervision* (Secreto bancario y cooperación internacional en la supervisión bancaria).

Grupo de Acción Financiera en Contra del Lavado de Dinero (FATF)

El sitio Web del FATF (www.fatf-gafi.org) incluye las siguientes publicaciones:

- *Forty Recommendations to Combat Money Laundering and Terrorism* (Cuarenta recomendaciones para combatir el lavado de dinero y el terrorismo).

- *Special Recommendations Against Terrorist Financing* (Recomendaciones especiales contra el financiamiento del terrorismo).
- *Interpretive Notes to FATF Recommendations* (Notas explicativas a las recomendaciones del FATF).
- *Noncooperative Countries or Territories* (Países o territorios que no cooperan).
- *Typologies on Money Laundering Risk* (Tipologías de los riesgos de lavado de dinero).
- *Trade Based Money Laundering* (Lavado de dinero a través de transacciones comerciales).
- *New Payment Methods* (Nuevos métodos de pago).
- *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers* (El uso indebido de instrumentos corporativos, incluidos los prestadores de servicios a compañías y fideicomisos).
- *Complex Money Laundering Techniques — Regional Perspectives Report* (Técnicas complejas de lavado de dinero: informe de perspectivas regionales).

The Clearing House Payments Co., LLC

El sitio web de The Clearing House (www.theclearinghouse.org) contiene esta publicación: *Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking* (Pautas para las políticas y procedimientos contra el lavado de dinero en los bancos corresponsales).

NACHA: The Electronic Payments Association (NACHA) (Asociación de Pagos Electrónicos)

El sitio Web de la NACHA (www.nacha.org) incluye lo siguiente:

- *The Next Generation ACH Task Force: Future Vision of the ACH Network* (La próxima generación del grupo de acción financiera de la ACH: visión de futuro de la red de ACH).
- *NACHA Operating Rules* (Normas operativas de la NACHA).

El Grupo Wolfsberg

El sitio Web del Grupo Wolfsberg (www.wolfsberg-principles.com) incluye lo siguiente:

- *Wolfsberg AML Principles on Private Banking* (Principios de Wolfsberg contra el lavado de dinero en la banca privada).
- *Wolfsberg Statement on the Suppression of the Financing of Terrorism* (Declaración de Wolfsberg sobre la supresión de la financiación del terrorismo).
- *Wolfsberg Statement on Payment Message Standards* (Declaración de Wolfsberg sobre las normas de mensajes de pago).

- *Wolfsberg AML Principles for Correspondent Banking* (Principios AML de Wolfsberg para los bancos corresponsales).
- *Wolfsberg Statement on Monitoring, Screening, and Searching* (Declaración de Wolfsberg sobre la supervisión, revisión y realización de búsquedas).
- *Wolfsberg Guidance on Risk Based Approach for Managing Money Laundering Risks* (Guía de Wolfsberg sobre el enfoque en función del riesgo para gestionar los riesgos de lavado de dinero).
- *Wolfsberg FAQs on Correspondent Banking* (Preguntas frecuentes de Wolfsberg sobre los bancos corresponsales).
- *Wolfsberg Trade Finance Principles* (Principios de financiación de comercio internacional de Wolfsberg).
- *Wolfsberg Statement on Monitoring, Screening, and Searching* (Declaración de Wolfsberg sobre la supervisión, revisión y realización de búsquedas).

Apéndice D: Definición Legal de Institución Financiera

Según se define en 31 USC 5312(a)(2) de la BSA, el término "institución financiera" incluye los siguientes:

- Un banco asegurado (según se define en la sección 3(h) de la Ley FDI (12 USC 1813(h))).
- Un banco comercial o compañía fiduciaria.
- Un banquero privado.
- Una agencia o sucursal de un banco extranjero en Estados Unidos.
- Cualquier cooperativa de crédito.
- Una institución de ahorro.
- Un agente de valores o comisionista registrado en la Comisión de Valores y Bolsa bajo la Ley del Mercado de Valores de 1934 (15 USC 78a *et seq.).*
- Un agente de valores o comisionista de valores o productos.
- Un banquero de inversión o compañía de inversión.
- Un cambio de moneda.
- Un emisor, cajero, o quien cambia por dinero cheques de viajeros, cheques, giros postales o instrumentos similares.
- Un operador de sistemas de tarjetas de crédito.
- Una compañía de seguros.
- Un comerciante de piedras, metales preciosos o joyas.
- Un prestamista.
- Una compañía de préstamo o de financiamiento.
- Una agencia de viajes.
- Un remitente de dinero licenciado o cualquier otra persona que participa en transferencias de fondos como negocio, incluida cualquier persona que participa en un sistema de transferencia de dinero informal como negocio o cualquier red de personas que participa en la facilitación de transferencias de dinero nacional o internacionalmente como negocio fuera del sistema de instituciones financieras convencionales.

- Una compañía telegráfica.
- Un negocio que participa en ventas de vehículos, incluidas las ventas de automóviles, aviones y barcos.
- Personas que participan en el cierre de operaciones y acuerdos que impliquen bienes inmuebles.
- El Servicio Postal de Estados Unidos.
- Una agencia del gobierno de Estados Unidos o de un gobierno local o estatal que realice una tarea o tenga control sobre un negocio descrito en este párrafo.
- Un casino, casino de apuestas o establecimiento de apuestas con un ingreso anual por apuestas de más de USD 1.000.000 que:
  - cuente con licencia de casino, casino de apuestas o establecimiento de apuestas bajo las leyes de cualquier estado o subdivisión política de cualquier estado, o
  - que constituya una operación de juego indio llevada a cabo en conformidad con la Ley Regulatoria del Juego Indio en lugar de constituir una operación limitada al juego clase I (según se define en la sección 4(6) de dicha ley).
- Cualquier negocio o agencia que participe en cualquier actividad que el Secretario del Tesoro de Estados Unidos determine, según el reglamento, que sea una actividad similar a cualquier actividad en la que cualquier negocio descrito en este párrafo esté autorizado a participar, o esté relacionada con tales actividades, o constituya un sustituto de ellas.
- Cualquier otro negocio designado por el Secretario cuyas transacciones en efectivo tengan un alto grado de utilidad en los asuntos delictivos, impositivos o normativos.
- Cualquier comisionista del mercado de futuros financieros, consejero de negociación de bienes tangibles u operador del consorcio de bienes tangibles registrado, o que tenga obligación de registrarse, bajo la Ley de la bolsa de comercio (7 USC 1, *et seq.*).

Apéndice E: Organizaciones Internacionales

El lavado de dinero y el financiamiento del terrorismo pueden tener un impacto internacional ampliamente generalizado. Se ha comprobado que los lavadores de dinero han transferido fondos y mantenido activos a nivel global, lo que hace que el rastreo de los fondos a través de diversos países sea un proceso complejo y desafiante. La mayoría de los países respaldan la lucha contra el lavado de dinero y el financiamiento del terrorismo, sin embargo, debido a los desafíos en la creación de normativas consistentes entre los países, los grupos internacionales han desarrollado recomendaciones modelo para gobiernos e instituciones financieras. A continuación, se analizan dos organismos internacionales clave en esta área:

- **El Grupo de Acción Financiera en Contra del Lavado de Dinero (FATF)** es una organización intergubernamental establecida para el desarrollo y la divulgación de políticas para combatir el lavado de dinero y el financiamiento del terrorismo. El FATF ha desarrollado recomendaciones sobre diversos asuntos de lavado de dinero y financiamiento del terrorismo publicadas en *FATF Forty Recommendations* (Cuarenta recomendaciones del FATF) y *Special Recommendations on Terrorist Financing* (Recomendaciones especiales sobre el financiamiento del terrorismo).[267]

- **El Comité de Supervisión Bancaria de Basilea** es un comité de bancos centrales y supervisores y reguladores bancarios de numerosos países que se reúne en el Banco de Pagos Internacionales (BIS) en Basilea, Suiza, para abordar asuntos relacionados con la supervisión bancaria prudente. El Comité de Basilea formula normas y pautas amplias y da recomendaciones sobre prácticas responsables, incluidas aquellas sobre debida diligencia de los clientes.

Además, otras organizaciones globales están comenzando a involucrarse cada vez más en la batalla contra el lavado de dinero. El Fondo Monetario Internacional (IMF, por sus siglas en inglés) y el Banco Mundial han incluido AML y actividades de lucha contra la financiación de terroristas en sus análisis, vigilancia y actividades de diagnóstico de sectores financieros. Además, existen diversas entidades regionales similares al FATF. Estos grupos participan como observadores en las reuniones del FATF; analizan a sus miembros según las normas del FATF, y, al igual que los miembros del FATF, con frecuencia contribuyen al programa de análisis del IMF y el Banco Mundial.

[267] Otra iniciativa conocida del FATF es su ejercicio sobre países y territorios no cooperantes (NCCT), donde se han identificado jurisdicciones como NCCT. En este momento, no hay países en la lista. Sin embargo, el 18 de Febrero de 2010, el FATF publicó una lista de jurisdicciones que están sujetas a medidas correctivas, presentan deficiencias de AML que no se han abordado o deficiencias que se abordarán en breve. Dicha lista se encuentra en el sitio Web del FATF: www.fatf-gafi.org/dataoecd/34/29/44636171.pdf.

Apéndice F: "Señales de Advertencia" de Lavado de Dinero y Financiamiento del Terrorismo

Los siguientes son ejemplos de actividades potencialmente sospechosas, o "señales de advertencia" del lavado de dinero y el financiamiento del terrorismo. Aunque estas listas no sean exhaustivas, pueden ayudar a que los bancos e inspectores reconozcan las posibles estratagemas de lavado de dinero y financiamiento del terrorismo. El enfoque principal de la gerencia debe centrarse en la elaboración de informes de actividades sospechosas, y no en determinar si las transacciones de hecho están vinculadas con el lavado de dinero, el financiamiento del terrorismo o un delito en particular.

Los ejemplos siguientes son señales de advertencia que, al detectarse, pueden requerir un escrutinio adicional. La mera presencia de una señal de advertencia no constituye una evidencia de actividad delictiva por sí misma. Un escrutinio más detallado debe ayudar a determinar si la actividad es sospechosa o si parece no existir un propósito legal o comercial razonable para su realización.

Actividad potencialmente sospechosa que puede indicar la existencia de lavado de dinero

Clientes que proporcionan información insuficiente o sospechosa

- Un cliente utiliza documentos de identificación sospechosos o poco habituales que no pueden verificarse fácilmente.
- Un cliente proporciona un número de identificación fiscal individual luego de haber utilizado previamente un número de Seguro Social.
- Un cliente utiliza números de identificación fiscal diferentes con variaciones de su nombre.
- Un negocio se rehúsa, al establecer una nueva cuenta, a proporcionar información completa sobre el carácter y propósito de su negocio, la actividad prevista de la cuenta, las relaciones bancarias anteriores, los nombres de sus funcionarios y directores o información sobre la ubicación del negocio.
- El teléfono particular o laboral de un cliente está desconectado.
- Los antecedentes del cliente difieren de lo que se esperaría en función de su actividad comercial.
- Un cliente efectúa transacciones frecuentes o de grandes volúmenes y no tiene ningún registro de experiencias laborales pasadas o presentes.

- El cliente es una compañía fiduciaria o fantasma, o una Compañía de Inversión Privada que se rehúsa a proporcionar información sobre las partes controlantes y los beneficiarios subyacentes. Los usufructuarios pueden contratar servicios de constitución de compañías nominadas para establecer compañías fantasmas y abrir cuentas bancarias para dichas compañías a la vez que protegen la identidad del propietario.

Esfuerzos para eludir las exigencias en cuanto a la presentación de informes y la gestión de registros

- Un cliente o grupo trata de persuadir a un empleado del banco de no presentar los informes o mantener los registros exigidos.

- Un cliente se rehúsa a proporcionar la información necesaria para presentar un informe obligatorio, a solicitar que se presente un informe, o a proceder con una transacción luego de haber sido notificado de la exigencia de presentar el informe.

- Un cliente se rehúsa a proveer una identificación al comprar instrumentos negociables en cantidades registrables.

- Un negocio o cliente solicita que se lo exente de las exigencias en cuanto a la presentación de informes o la gestión de registros.

- Una persona normalmente utiliza el cajero automático para efectuar varios depósitos bancarios por debajo del umbral especificado.

- Un cliente deposita fondos en varias cuentas, generalmente en cantidades menores a USD 3.000, que posteriormente se consolidan en una cuenta principal y se transfieren fuera del país, particularmente con destino a una ubicación que despierta una preocupación específica o a través de ella (p. ej., países designados por las autoridades nacionales y el Grupo de Acción Financiera en Contra del Lavado de Dinero (FATF) como países y territorios no cooperantes).

- Un cliente ingresa a una caja de seguridad luego de efectuar una transacción que involucró un retiro de grandes volúmenes de dinero, o ingresa a una caja de seguridad antes de realizar depósitos en dinero en efectivo fraccionados justo por debajo de los USD 10.000, para eludir las exigencias en cuanto a la presentación de Informes de Transacciones en Efectivo (CTR).

Transferencias de fondos

- Muchas transferencias de fondos se transmiten en sumas de grandes volúmenes, redondeadas y en cientos o miles de dólares.

- La actividad de transferencia de fondos ocurre desde o hacia un refugio en cuanto al secreto financiero, o desde o hacia una ubicación geográfica de alto riesgo sin motivo comercial aparente o cuando la actividad no es coherente con los antecedentes o el negocio del cliente.

- Se reciben muchas transferencias de fondos entrantes de poco volumen o se realizan depósitos utilizando cheques o giros postales. Casi inmediatamente, todas o la mayoría de las transferencias o depósitos se transfieren a otra ciudad o país de una manera que no es coherente con los antecedentes o el negocio del cliente.

- Se reciben transferencias de fondos entrantes de grandes volúmenes en nombre de un cliente extranjero, con pocos o sin motivos explícitos.

- La actividad de transferencias de fondos no se explica, es repetitiva o muestra patrones poco habituales.

- Se reciben pagos o recibos sin vínculo aparente a contratos, bienes o servicios legítimos.

- Se emiten o reciben transferencias de fondos de la misma persona desde o hacia diferentes cuentas.

- Las transferencias de fondos poseen contenido limitado y carecen de información sobre las partes relacionadas.

Transacciones de compensación automatizada

- Las transacciones de cámaras de compensación automáticas (ACH) de mucho valor con frecuencia se inician a través de prestadores de servicios externos (TPSP) por parte de remitentes que no son clientes del banco y para los cuales éste ha aplicado debida diligencia insuficiente o nula.

- Los TPSP tienen antecedentes de violaciones a las normas de la red de ACH o de generación de transacciones ilegales, o de procesamiento de transacciones adulteradas o fraudulentas en nombre de sus clientes.

- Múltiples niveles de TPSP que parecen estar involucrados en las transacciones de manera innecesaria.

- Nivel extraordinariamente alto de transacciones iniciadas en Internet o por teléfono.

- Las solicitudes de información de la Asociación Nacional de Cámaras de Compensación Electrónica (NACHA) indican riesgos potenciales con respecto al uso que hace el banco del sistema de ACH.

Actividad incoherente con el negocio del cliente

- Los patrones de transacciones en efectivo de un negocio muestran un cambio repentino que es incoherente con las actividades normales.

- Un gran volumen de cheques de caja, giros postales o transferencias de fondos se depositan en una cuenta o se compran a través de una cuenta pese a que el carácter del negocio del titular de la cuenta no parece justificar dicha actividad.

- Un negocio al por menor muestra patrones radicalmente diferentes de depósitos en efectivo respecto a negocios similares en la misma ubicación general.
- Transferencias de fondos poco habituales ocurren entre cuentas relacionadas o entre cuentas que involucran los mismos mandantes o mandantes relacionados.
- El propietario de un negocio al por menor y un servicio de cambio de cheques no solicita efectivo al depositar los cheques, lo que posiblemente indica la disponibilidad de otra fuente de efectivo.
- Los bienes o servicios comprados para el negocio no coinciden con el rubro de la actividad comercial declarado del cliente.
- Los pagos de bienes y servicios se efectúan mediante cheques, giros postales o giros bancarios que no se retiran de la cuenta de la entidad que realizó la compra.

Actividad de préstamo

- Préstamos garantizados con bienes prendados mantenidos por terceros que no están relacionados con el solicitante del préstamo.
- Préstamo garantizado con depósitos u otros activos negociables, como valores, particularmente cuando son de propiedad de terceros aparentemente no relacionados.
- El solicitante del préstamo no paga un préstamo garantizado con efectivo o cualquier préstamo garantizado con activos que se convierten fácilmente en efectivo.
- Los préstamos se efectúan para, o se pagan en nombre de, un tercero sin ninguna explicación razonable.
- Para garantizar un préstamo, el cliente compra un certificado de depósito utilizando una fuente de fondos desconocida, particularmente cuando los fondos se proporcionan mediante efectivo o múltiples instrumentos monetarios.
- Los préstamos que carecen de un propósito comercial legítimo, proporcionan al banco tasas significativas por asumir poco o ningún riesgo, o tienden a disimular el movimiento de los fondos (p. ej., préstamos efectuados al solicitante del préstamo que se venden inmediatamente a una entidad relacionada con éste).

Cambios en las transacciones de banco a banco

- El tamaño y la frecuencia de los depósitos en efectivo se incrementan rápidamente sin el incremento correspondiente en los depósitos que no son en efectivo.
- Un banco no puede rastrear al verdadero titular de la cuenta de transacciones de cuentas de concentración o corresponsales.
- El volumen de negocios en billetes de alta denominación es significativo y parece poco habitual, dada la ubicación del banco.

- Los cambios en los patrones de envíos de moneda entre bancos corresponsales son significativos.

Transacciones con instituciones financieras transnacionales[268]

- Los bancos estadounidenses incrementan las ventas o cambios de papel moneda estadounidense de alta denominación a instituciones financieras mexicanas.
- Grandes volúmenes de papel moneda estadounidense de baja denominación que se envían desde casas de cambio mexicanas a sus cuentas estadounidenses vía transporte blindado o que se venden directamente a bancos estadounidenses. Estas ventas o cambios podrían involucrar jurisdicciones fuera de México.
- Las casas de cambio efectúan remesas de fondos vía múltiples transferencias de fondos a jurisdicciones fuera de México que no tienen relación comercial aparente con las casas de cambio. Los receptores de transferencias de fondos pueden incluir individuos, negocios y otras entidades en áreas de libre comercio.
- Las casas de cambio depositan numerosos artículos de terceros, incluidos los instrumentos monetarios numerados secuencialmente, en sus cuentas de bancos estadounidenses.
- Las casas de cambio efectúan remesas de fondos desde sus cuentas en instituciones financieras mexicanas hacia cuentas en bancos estadounidenses. Estas transferencias de fondos son posteriores al depósito de dinero y artículos de terceros por parte de las casas de cambio en sus instituciones financieras mexicanas.

Envío de moneda en grandes cantidades

- Un incremento en la venta de papel moneda estadounidense de alta denominación a instituciones financieras extranjeras por parte de bancos estadounidenses.
- Grandes volúmenes de papel moneda estadounidense de baja denominación que se envían desde instituciones financieras no bancarias a sus cuentas estadounidenses vía transporte blindado o que se venden directamente a bancos estadounidenses.
- Transferencias bancarias múltiples iniciadas por instituciones financieras extranjeras no bancarias que dan instrucciones a bancos estadounidenses para que remitan fondos a otras jurisdicciones que no parecen tener ninguna relación comercial aparente con esa institución financiera no bancaria extranjera. Los receptores de transferencias de fondos podrían incluir individuos, negocios y otras entidades en áreas de libre comercio y otros lugares.

---

[268] Carta informativa de la FinCEN FIN-2006-A003, Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States (Guía para las instituciones financieras sobre la repatriación de moneda introducida de contrabando a México desde Estados Unidos), del 28 de Abril de 2006.

- El canje de papel moneda estadounidense de baja denominación por papel moneda estadounidense de alta denominación que podría enviarse a países extranjeros.

- Depósitos efectuados por instituciones financieras extranjeras no bancarias en sus cuentas en bancos estadounidenses que incluyen artículos de terceros, incluso instrumentos monetarios numerados en secuencia.

- Depósitos de moneda y artículos de terceros por parte de instituciones financieras extranjeras no bancarias en sus cuentas en instituciones financieras extranjeras y posteriores transferencias bancarias directas a las cuentas de las instituciones financieras extranjeras no bancarias en bancos estadounidenses.

Financiación del comercio internacional

- Envíos de artículos que no se corresponden con el carácter del negocio del cliente (p. ej., una compañía siderúrgica que comienza a comerciar productos de papel, o una compañía de tecnología de información que comienza a comerciar productos farmacéuticos en grandes cantidades).

- Clientes que realizan negocios en jurisdicciones de alto riesgo.

- Clientes que envían artículos a través de jurisdicciones de alto riesgo, incluido el tránsito por países no cooperantes.

- Clientes que participan en actividades de alto riesgo potencial, incluidas las actividades que puedan están sujetas a restricciones de importación y exportación (p. ej., equipo para organizaciones policiales o militares de gobiernos extranjeros, armas, municiones, mezclas químicas, artículos de defensa clasificados, información técnica confidencial, materiales nucleares, piedras preciosas o determinados recursos naturales tales como metales, mineral metalífero y petróleo crudo).

- Evidente fijación irregular de precios en bienes y servicios.

- Tergiversación evidente de la cantidad o el tipo de bienes importados o exportados.

- El fraccionamiento de las transacciones parece innecesariamente complejo y diseñado para disimular el verdadero carácter de la transacción.

- Los casos en los cuales los clientes solicitan el pago de lo recaudado a un tercero no relacionado.

- Ubicaciones de envío o descripciones de bienes que no son consistentes con la carta de crédito.

- Cartas de crédito significativamente enmendadas sin una justificación razonable o cambios de beneficiario o ubicación de pago. Cualquier cambio en los nombres de las partes debe promover un control adicional de la OFAC.

Cajeros automáticos de propiedad privada

- Los niveles de actividad de cajeros automáticos son altos en comparación con otros cajeros de propiedad privada o de propiedad del banco en ubicaciones geográficas o demográficas similares.

- Las fuentes de efectivo para el cajero automático no se pueden identificar o confirmar a través de los retiros de cuentas, contratos con servicios de transporte blindado, distintos tipos de préstamos u otra documentación adecuada.

Seguros

- Un cliente compra productos con servicios de terminación del seguro sin tener en cuenta el rendimiento de la inversión del producto.

- Un cliente compra productos de seguros con un pago de prima único y elevado, particularmente cuando el pago se realiza a través de métodos poco habituales como en moneda o equivalentes a la moneda.

- Un cliente compra un producto que no está incluido en su rango normal del patrimonio financiero o sus necesidades de planificación patrimonial.

- Un cliente pide prestado el valor de rescate en efectivo de las pólizas de seguro de vida permanente, en particular cuando los pagos se realizan a terceros aparentemente no relacionados.

- Se compran pólizas que permiten la transferencia de los derechos usufructo sin el conocimiento y consentimiento del emisor del seguro. Esto incluiría la póliza de seguro total de segunda mano y pólizas de seguro al portador.

- Se sabe que un cliente compra varios productos de seguros y utiliza los ingresos de una amortización anticipada de la póliza para comprar otros activos financieros.

- Un cliente utiliza múltiples equivalentes de moneda (por ej. cheques de cajero u giros postales) de diferentes bancos y negocios de servicios de dinero para llevar a cabo pagos de seguros o pagos de renta vitalicia.

Actividad de las compañías fantasmas

- Un banco no puede obtener información suficiente o la información no está disponible para identificar de un modo concluyente a los remitentes o beneficiarios de cuentas u otras actividades bancarias (utilizando Internet, búsquedas en bases de datos comerciales o consultas directas a un banco respondiente).

- Los pagos a la compañía o de la compañía no tienen un propósito declarado, no hacen referencia a bienes o servicios, o identifican sólo un contrato o un número de factura.

- Los bienes o servicios, si se los identifica, no coinciden con el perfil de la compañía proporcionado por el banco respondiente o el carácter de la actividad financiera; una

compañía hace referencia a bienes y servicios notablemente diferentes en transferencias de fondos relacionadas; la explicación dada por el banco respondiente extranjero no es coherente con la actividad de transferencias de fondos observada.

- Los negocios involucrados en la transacción comparten la misma dirección, proporcionan sólo la dirección de un agente registrado, o presentan otras incoherencias en las direcciones.
- Grandes cantidades y variedades poco habituales de beneficiarios que reciben transferencias de fondos de una sola compañía.
- Participación frecuente de múltiples jurisdicciones o beneficiarios que se encuentran en centros financieros de alto riesgo ubicados en el exterior.
- Un banco corresponsal extranjero excede el volumen previsto en el perfil de su cliente con respecto a las transferencias de fondos, o una compañía particular exhibe un gran volumen y un patrón de transferencias de fondos que no es coherente con su actividad comercial habitual.
- Múltiples pagos o transferencias de grandes sumas entre compañías fantasma sin propósito comercial legítimo aparente.
- El propósito de la compañía fantasma es desconocido o no está claro.

Cuentas de embajadas y consulados extranjeros

- Los negocios oficiales de la embajada se realizan a través de cuentas personales.
- La actividad de la cuenta no es coherente con el propósito de la misma, como la actividad de depósitos vía maletines/bolsos o transacciones pagaderas mediante presentación de identificación apropiada.
- Las cuentas se suplen de fondos a través de transacciones en efectivo sustanciales.
- Las cuentas financian directamente los gastos personales de extranjeros sin los controles adecuados, incluidos, entre otros, los gastos de estudiantes universitarios.

Empleados

- El empleado exhibe un estilo de vida de derroche que no se condice con su salario.
- El empleado no cumple con las políticas, los procedimientos y los procesos, particularmente en la banca privada.
- El empleado se rehúsa a tomarse vacaciones.

Otras actividades sospechosas o poco habituales de los clientes

- El cliente cambia con frecuencia dólares de baja denominación por dólares de alta denominación.
- El cliente deposita con frecuencia efectivo asegurado con tiras para efectivo o efectivo asegurado con una banda elástica que está desorganizado y cuyos totales no cuadran al contarse.
- El cliente compra una cantidad de cheques de caja, giros postales o cheques de viajero en grandes volúmenes bajo un umbral especificado.
- El cliente compra una cantidad de tarjetas de valor acumulado abiertas en grandes volúmenes. Las compras de tarjetas de valor acumulado no son consistentes con las actividades comerciales habituales.
- El cliente recibe depósitos frecuentes y en grandes volúmenes de sistemas de pagos en línea pero no parece tener un negocio en línea o de subastas.
- Los instrumentos monetarios depositados por correo están numerados secuencialmente o tienen símbolos o impresiones poco habituales.
- Los movimientos sospechosos de fondos ocurren de un banco a otro y luego los fondos se transmiten nuevamente al primer banco.
- Los depósitos se fraccionan en múltiples sucursales del mismo banco o con grupos de personas que entran a una misma sucursal al mismo tiempo.
- El dinero se deposita o retira en sumas apenas debajo de los parámetros fijados para la presentación de informes.
- El cliente visita una caja de seguridad o utiliza una cuenta de custodia de depósito con una frecuencia poco habitual.
- Las cajas de seguridad y las cuentas de custodia de depósito abiertas por individuos que no residen ni trabajan en el área de servicio de la institución, a pesar de la disponibilidad de dichos servicios en una institución local.
- El cliente utiliza repetidamente y sin un propósito comercial suficiente un banco o una sucursal que se encuentra a una distancia geográfica lejana con respecto al hogar u oficina de éste.
- El cliente exhibe patrones de tráfico poco habitual en el área de la ubicación de la caja de seguridad o un uso poco habitual de las cuentas de custodia de depósito. Por ejemplo, varios individuos llegan juntos, entran con frecuencia, o llevan bolsos u otros recipientes que pueden ocultar grandes volúmenes de efectivo, instrumentos monetarios o artículos pequeños de valor.

- El cliente alquila múltiples cajas de seguridad para almacenar grandes volúmenes de efectivo, instrumentos monetarios o activos de gran valor monetario a la espera de la conversión en efectivo para la colocación en el sistema bancario. Del mismo modo, un cliente establece múltiples cuentas de custodia de depósito para colocar temporalmente grandes volúmenes de valores a la espera de la venta y conversión en efectivo, instrumentos monetarios, transferencias de fondos salientes, o una combinación de los mismos, para colocarlos en el sistema bancario.

- Uso poco habitual de fondos fiduciarios en transacciones comerciales u otra actividad financiera.

- El cliente utiliza una cuenta personal con propósitos comerciales.

- El cliente ha establecido múltiples cuentas bajo diversos nombres corporativos o individuales que carecen de propósito comercial suficiente según las complejidades de la cuenta o parecen querer ocultar el usufructo al banco.

- El cliente realiza depósitos en efectivo frecuentes y múltiples en diversas cuentas presuntamente no relacionadas.

- El cliente realiza depósitos y retiros en grandes volúmenes durante un período de tiempo corto luego de la apertura y posteriormente cierra la cuenta o ésta permanece inactiva. Por el contrario, una cuenta con poca actividad repentinamente puede experimentar una actividad de retiros y depósitos en grandes volúmenes.

- El cliente efectúa transacciones en grandes volúmenes que no son consistentes con su ingreso declarado.

Actividad potencialmente sospechosa que puede indicar la existencia de una actividad de financiamiento del terrorismo

Los siguientes ejemplos de actividades potencialmente sospechosas que pueden indicar la existencia de una actividad de financiamiento del terrorismo se basan principalmente en Guidance for Financial Institutions in Detecting Terrorist Financing (Guía de las instituciones financieras para la detección del financiamiento del terrorismo), proporcionada por el FATF.[269] El FATF es una organismo intergubernamental cuyo propósito es el desarrollo y la divulgación de políticas nacionales e internacionales para combatir el lavado de dinero y el financiamiento del terrorismo.

[269] La Guía de las instituciones financieras para la detección del financiamiento del terrorismo, del 24 Abril de 2002, está disponible en www.fatf-gafi.org.

Actividad incoherente con el negocio del cliente

- Los fondos se generan mediante un negocio que es propiedad de personas de la misma procedencia o mediante un negocio que involucra a personas procedentes de los mismos países de alto riesgo (p. ej., países designados por autoridades nacionales y el FATF como países y territorios no cooperantes).
- La ocupación declarada del cliente no es coherente con el tipo o nivel de la actividad.
- Las personas involucradas en transacciones en efectivo comparten una dirección o número de teléfono, particularmente cuando la dirección también es una ubicación comercial o no parece corresponder con la ocupación declarada (p. ej., estudiante, desempleado o trabajador independiente).
- Con respecto a las organizaciones de caridad o sin fines de lucro, se efectúan transacciones financieras que parecen no tener un propósito económico lógico o respecto a las cuales parece no haber vinculación entre la actividad declarada de la organización y las otras partes involucradas en la transacción.
- Una caja de seguridad abierta en nombre de una entidad comercial cuando la actividad comercial del cliente es desconocida o dicha actividad no parece justificar el uso de una caja de seguridad.

Transferencias de fondos

- Un gran volumen de transferencias de fondos entrantes o salientes se efectúa a través de una cuenta comercial y parece no haber un propósito comercial u otro propósito económico lógico para esas transferencias, particularmente cuando la actividad involucra lugares de alto riesgo.
- Las transferencias de fondos se organizan en pequeñas cantidades, lo que exhibe un esfuerzo aparente por evitar que se activen las exigencias en cuanto a la identificación y presentación de informes.
- Las transferencias de fondos no incluyen información sobre el remitente o la persona en cuyo nombre se efectúa la transacción, cuando se esperaría la inclusión de dicha información.
- Se utilizan múltiples cuentas comerciales y personales o las cuentas de organizaciones de caridad o sin fines de lucro para cobrar y transferir fondos a una pequeña cantidad de beneficiarios extranjeros.
- Se efectúan transacciones de cambio de moneda extranjera en nombre de un cliente por parte de un tercero, seguidas de transferencias de fondos a ubicaciones que carecen de conexión comercial aparente con el cliente, o a países de alto riesgo.

Otras transacciones que parecen poco habituales o sospechosas

- Transacciones que involucran cambios de moneda extranjera seguidas de transferencias de fondos a ubicaciones de alto riesgo dentro de un plazo muy breve.
- Se utilizan múltiples cuentas para cobrar y transferir fondos a una pequeña cantidad de beneficiarios extranjeros, tanto individuos como negocios, particularmente en ubicaciones de alto riesgo.
- Un cliente obtiene un documento de crédito o participa de transacciones financieras comerciales que involucran el movimiento de fondos desde o hacia ubicaciones de alto riesgo cuando parece no haber ningún motivo comercial lógico para hacer negocios con esas ubicaciones.
- Bancos de ubicaciones de alto riesgo que abren cuentas.
- Se envían o reciben fondos vía transferencias internacionales desde o hacia ubicaciones de alto riesgo.
- Préstamos sobre pólizas de seguros o los valores de rescate de las pólizas que están sujetos a un cargo de rescate sustancial.

Apéndice G: Fraccionamiento

El fraccionamiento de las transacciones para evadir la presentación de informes de la BSA y algunas exigencias respecto a la gestión de registros puede causar la aplicación de sanciones civiles y penales bajo la BSA. Bajo la BSA (31 USC 5324), ninguna persona debe, a los efectos de evadir el CTR o una exigencia de presentación de informes sobre una orden de fijación de ubicación geográfica objetivo, o determinadas exigencias de gestión de registros de la BSA:

- Causar o intentar causar que un banco no pueda presentar un CTR o un informe exigido bajo una orden de fijación de ubicación geográfica objetivo o mantener un registro exigido bajo los reglamentos de la BSA.

- Causar o intentar causar que un banco presente un CTR o un informe exigido bajo una orden de fijación de ubicación geográfica objetivo o mantenga un registro de la BSA que contenga una omisión material o tergiversación de los hechos.

- Fraccionar, como se define anteriormente, o intentar fraccionar o colaborar en el fraccionamiento, de cualquier transacción con uno o más bancos.

La definición de fraccionamiento, como se establece en 31 CFR 103.11(gg) (que fue implementada antes de que una disposición de la Ley PATRIOT de EE. UU. extendiera la prohibición de fraccionamiento a las órdenes de fijación de ubicación geográfica objetivo y las exigencias de gestión de registros de la BSA) determina: “una persona fracciona una transacción si esa persona, actuando sola, en complicidad con otros, o en nombre de otros, realiza o intenta realizar una o más transacciones en efectivo por cualquier monto, en una o más instituciones financieras, en uno o más días, de cualquier manera, con el propósito de evadir las [exigencias de presentación de CTR]”. “De cualquier manera” incluye, pero no se limita únicamente a, dividir un monto único en efectivo que supere los USD 10.000 en pequeños montos que se puedan realizar como una serie de transacciones de hasta USD 10.000 o inferiores a USD 10.000. Las transacciones no deben superar, en ninguno de los bancos ninguno de los días, el umbral de USD 10.000 de la presentación de CTR para constituir fraccionamiento.

Los lavadores de dinero y delincuentes han desarrollado muchas maneras de fraccionar grandes volúmenes de efectivo para evadir las exigencias de presentación de CTR. A menos que el efectivo sea sacado clandestinamente de los Estados Unidos o se combine con los depósitos de un negocio legítimo, cualquier operación de lavado de dinero que comience con la necesidad de convertir los ingresos en moneda derivados de actividades delictivas en formas de instrumentos monetarios, cuentas o inversiones de apariencia más legítima implicará probablemente algún tipo de fraccionamiento. El fraccionamiento continúa siendo una de las sospechas de delito que más comúnmente se informan en los SAR.

Los empleados del banco deben tener conocimiento de las operaciones de fraccionamiento y estar alertas a las mismas. Por ejemplo, un cliente puede fraccionar depósitos en moneda o transacciones de extracción, para que estas sean inferiores al umbral de USD 10.000 de la presentación de CTR; utilizar efectivo para comprar cheques oficiales de bancos, giros

postales o cheques de viajero en montos inferiores a los USD 10.000 (y posiblemente en montos inferiores al umbral de USD 3.000 de gestión de registros para la compra en efectivo de instrumentos monetarios con el objeto de evitar identificarse en el proceso); o cambiar papel moneda de baja denominación por aquel de alta denominación en montos inferiores a los USD 10.000.

Sin embargo, que dos transacciones levemente inferiores al umbral de USD 10.000 sean realizadas con días o semanas de diferencia no necesariamente implica que estén fraccionadas. Por ejemplo, si un cliente deposita USD 9.900 en efectivo el lunes y USD 9.900 en efectivo el miércoles, no se debe suponer que ha habido fraccionamiento. En cambio, puede llegar a ser necesario realizar controles e investigaciones adicionales para determinar el carácter de las transacciones, los antecedentes previos de la cuenta y obtener otra información relevante del cliente que sirva para analizar si la actividad es sospechosa. Aun si no ha existido fraccionamiento, el banco debe revisar las transacciones para detectar actividades sospechosas.

Además, el fraccionamiento puede ocurrir antes de que el cliente lleve los fondos al banco. En esos casos, es posible que un banco sea capaz de identificar los resultados del fraccionamiento. Los depósitos de instrumentos monetarios que pueden haber sido comprados en otro lugar podrían estar fraccionados para evadir las exigencias de presentación de CTR o las exigencias de gestión de registros relacionadas con la compra de instrumentos monetarios en efectivo. Estos instrumentos a menudo están numerados secuencialmente en grupos por un valor total inferior a los USD 10.000 o USD 3.000; están escritos con la misma letra (en su mayor parte) y a menudo tienen la misma estampilla, símbolo o iniciales; o parecen haber sido comprados en numerosos lugares en el mismo día o en días diferentes.

Apéndice H: Puntos de la Carta de Solicitud (Sección Principal y Ampliada)

Procedimientos de inspección principal

Como parte del proceso de planificación de la inspección, el inspector debe preparar una carta de solicitud. La lista que aparece a continuación incluye materiales que los inspectores *pueden* solicitar o respecto a los cuales pueden solicitar acceso a fin de realizar la inspección BSA/AML de un banco. Se debe adaptar esta lista de acuerdo al perfil específico del banco y el campo de aplicación planificado de la inspección. Se pueden solicitar materiales adicionales según sea necesario.

Programa de cumplimiento de BSA/AML

_ Nombre y cargo del funcionario de cumplimiento de BSA designado y, si es diferente, nombre y cargo de la persona responsable de supervisar el cumplimiento de BSA/AML.

- Un organigrama que muestre líneas de comunicación directas e indirectas.
- Copias de los curriculum vitae y títulos académicos de la persona o las personas que hayan comenzado a trabajar en el banco recientemente actuando en calidad de supervisores del programa de cumplimiento de BSA/AML.

_ Ponga a disposición copias del programa escrito de cumplimiento de BSA/AML más reciente aprobado por la junta directiva (o el equivalente legal de ese programa para las instituciones financieras extranjeras que operan en Estados Unidos), incluidas las exigencias del CIP, con la fecha de aprobación indicada en el acta.

_ Ponga a disposición copias de las políticas y los procedimientos relacionados con todas las exigencias de gestión de registro y presentación de informes, incluidos los informes de actividades sospechosas.

_ Correspondencia dirigida entre el banco, su personal o sus agentes y sus agencias bancarias estatales y federales, el Tesoro de Estados Unidos (Oficina del Secretario y Departamento del Tesoro, IRS, FinCEN, Centro de Cómputos Empresarial de Detroit del IRS (anteriormente conocido como el Centro de Cómputos de Detroit) y OFAC) o autoridades de aplicación de la ley desde la inspección BSA/AML previa. Por ejemplo, ponga a disposición correspondencia en poder del IRS que esté relacionada con errores u omisiones en los CTR.

Pruebas independientes

_ Ponga a disposición copias de los resultados de auditorías independientes provenientes de fuentes internas o externas o de pruebas realizadas desde la inspección BSA/AML previa, incluidos el campo de aplicación o la carta de compromiso, las respuestas de la gerencia y el acceso a los documentos.

_ Posibilite el acceso al análisis de riesgos del auditor, el plan de auditoría (cronograma) y el programa utilizado para las auditorías o pruebas.

Capacitación

_ La documentación de la capacitación (p. ej., los materiales utilizados para la capacitación desde la inspección BSA/AML previa).

_ El cronograma de la capacitación BSA/AML con fechas, asistentes y temas. Una lista de personas que ocupan puestos para los que el banco generalmente exige capacitación BSA/AML, que no hayan participado en la capacitación.

Análisis de riesgos

_ Ponga a disposición copias del análisis de riesgos BSA/AML realizado por la gerencia de los productos, servicios, clientes y ubicaciones geográficas.

_ Lista de las cuentas identificadas por el banco como de alto riesgo.

Programa de identificación de clientes

_ Lista de las cuentas que no tengan número de identificación fiscal (TIN).

_ Un archivo con la correspondencia de solicitud de TIN para los clientes del banco.

_ Una copia de cualquier formulario de apertura de cuenta (p. ej., para préstamos, depósitos u otras cuentas) utilizado para documentar la información de CIP/Debida diligencia de los clientes.

_ Una descripción escrita de los motivos del banco para las exenciones a los CIP respecto a clientes existentes que abren cuentas nuevas.

_ Una lista de las cuentas nuevas que cubra todas las líneas de productos (incluidas las cuentas abiertas por terceros) y segregue las cuentas de clientes existentes de los clientes nuevos, por _____. *(El inspector debe introducir un período de tiempo adecuado según el tamaño y la complejidad del banco).*

_ Una lista de cualquier cuenta abierta para un cliente que proporciona una solicitud para un TIN.

_ Una lista de cualquier cuenta abierta en la que la verificación no se haya realizado o de cualquier cuenta abierta con exenciones al CIP.

_ Una lista de los clientes o clientes potenciales para los que el banco haya tomado medidas desfavorables,[270] en función de sus CIP.

[270] Como se define en 12 CFR 202.2(c).

_ Una lista de todos los métodos documentales y no documentales que el banco utiliza para verificar la identidad de los clientes.

_ Ponga a disposición las notificaciones del cliente y una descripción de su fecha y entrega y oportunidad, por producto.

_ Una lista de las instituciones financieras de las que el banco depende, si el banco utiliza la "disposición sobre dependencia". La lista debe tener en cuenta si las instituciones financieras de las que se depende están sujetas a una reglamentación que implementa las exigencias del programa de cumplimiento BSA/AML de 31 USC 5318(h) y están reguladas por un ente regulador funcional federal.

_ Proporcione lo siguiente:

- Copias de cualquier contrato firmado entre las partes.
- Copias del CIP o procedimientos utilizados por la otra parte.
- Cualquier certificación realizada por la otra parte.

_ Copias de los contratos con las instituciones financieras y con terceros que realicen el CIP del banco o cualquier parte del mismo.

Presentación de informes de actividades sospechosas

_ Acceso a los SAR presentados ante la FinCEN durante el período de control de la documentación respaldatoria. Incluya copias de cualquier SAR presentado que esté relacionado con las solicitudes de información de la sección 314(a) o con las solicitudes de intercambio de información de la sección 314(a).

_ Cualquier análisis o documentación de cualquier actividad respecto de la cual se haya considerado pero no se haya presentado un SAR, o el banco esté considerando activamente presentar un SAR.

_ Descripción de los procedimientos de supervisión ampliados aplicados a las cuentas de alto riesgo.

_ Determinación respecto a si el banco utiliza un sistema manual o automatizado de supervisión de cuentas o una combinación de ambos. Si se utiliza un sistema automatizado, determine si el sistema es propio o proporcionado por un proveedor. Si el sistema fue proporcionado por un proveedor externo, solicite (i) una lista que incluya al proveedor, (2) los nombres de la solicitud y (iii) las fechas de instalación de cualquier sistema automatizado de supervisión de cuentas proporcionado por un proveedor externo. Solicite una lista de las normas o algoritmos utilizados por los sistemas y copias de la validación independiente del software respecto a estas normas.

_ Ponga a disposición copias de los informes utilizados para la identificación y la supervisión de transacciones sospechosas. Esos informes incluyen, pero no se limitan únicamente a, informes de sospechas de cheques sin fondos, informes sobre actividades

en moneda, registros de instrumentos monetarios e informes de transferencias de fondos. Estos informes pueden ser generados por un software BSA/AML especializado, los sistemas generales de procesamiento de datos del banco o ambos.

_ Copias de otros informes que puedan señalar transacciones poco habituales que requieran control adicional, si dichas copias no se han proporcionado con anterioridad. Los ejemplos incluyen informes de insuficiencia de fondos (NSF), informes de análisis de cuenta sobre ingresos por honorarios e informes de artículos significativos.

_ Proporcione el nombre, el propósito, los parámetros y la frecuencia de cada informe.

_ Correspondencia recibida de autoridades federales de aplicación de la ley sobre la disposición de las cuentas respecto de las cuales se presentaron informes de actividades sospechosas.

_ Ponga a disposición copias (o un registro) de las citaciones penales recibidas por el banco desde la inspección previa.

_ Ponga a disposición copias de políticas, procedimientos y procesos utilizados para cumplir con todas las citaciones penales, incluidas las Cartas de Seguridad Nacional (NSL), relacionados con la BSA.

Informe de transacciones en efectivo

_ Acceso a Informes de transacciones en efectivo (CTR) (Formulario 104 de la FinCEN) presentados durante el período de control.

_ Acceso a informes internos utilizados para identificar transacciones en efectivo declarables durante el período de control.

_ Lista de productos o servicios que pueden implicar transacciones en efectivo.

Exenciones al informe de transacciones en efectivo

_ Acceso a los formularios de Designación de persona exenta presentados sobre exenciones actuales (Formulario 110 de la FinCEN).

_ Lista de clientes exentos de la presentación de CTR y la documentación respaldatoria de la exención (p. ej., antecedentes de transacciones en efectivo, o si corresponde, análisis sobre la base de riesgo).

_ Acceso a la documentación de los controles anuales requeridos para las exenciones a los CTR.

Intercambio de información

_ Documentación de cualquier coincidencia positiva de una solicitud de la sección 314(a).

_ Ponga a disposición la documentación que demuestre que se han realizado las búsquedas requeridas.

_ Si corresponde, ponga a disposición cualquier acuerdo de confidencialidad de proveedores respecto a los servicios de la sección 314(a).

_ Ponga a disposición copias de las políticas, los procedimientos y los procesos para el cumplimiento de 31 CFR 103.100 (Intercambio de información entre las agencias federales de aplicación de la ley y las instituciones financieras).

_ Si corresponde, una copia del formulario de notificación más reciente del banco para compartir información voluntariamente con otras instituciones financieras bajo 31 CFR 103.110 (Intercambio de información voluntario entre las instituciones financieras) o una copia de la correspondencia más reciente recibida de la FinCEN que acuse recibo por parte de la FinCEN de la notificación del banco de intercambiar información voluntariamente con otras instituciones financieras.

_ Si corresponde, ponga a disposición copias de las políticas, los procedimientos y procesos para cumplir con 31 CFR 103.110.

Compraventa de instrumentos monetarios

_ Acceso a los registros de ventas de instrumentos monetarios por montos de entre USD 3.000 y USD 10.000 (si se hicieron por medio de transacciones individuales, proporcione muestras de los registros mantenidos en relación con la venta de cada tipo de instrumento monetario).

Gestión de registros de transferencias de fondos

_ Acceso a los registros de transferencias de fondos, incluidas las transferencias de fondos salientes, entrantes y aquellas en las que el banco actúa como intermediario, de USD 3.000 o más.

Debida diligencia y gestión de registros de cuentas corresponsales extranjeras

_ Una lista de todas las cuentas bancarias corresponsales extranjeras, incluida una lista de las instituciones financieras extranjeras, a las cuales el banco preste o haya prestado servicios regulares, y la fecha en la que se recibió la información solicitada (ya sea mediante la certificación o por otros medios).

_ Si corresponde, documentación que demuestre el cumplimiento con 31 CFR 103.177 (Prohibición con respecto a cuentas corresponsales para bancos fantasmas extranjeros, registros sobre propietarios de bancos extranjeros y agentes de notificaciones de demanda) y 31 CFR 103.185 (Auto de comparecencia o citación relacionada con los registros del banco extranjero; terminación de la relación corresponsal) (para cuentas bancarias corresponsales extranjeras y bancos fantasmas).

_ Una lista de todas las relaciones asociadas con cuentas empleadas para pagos que se mantengan con instituciones financieras extranjeras según la definición de 31 CFR 103.175.

_ Acceso a contratos o acuerdos con las instituciones financieras extranjeras que tengan cuentas empleadas para pagos.

_ Una lista de las sucursales extranjeras del banco y de las medidas que ha tomado el banco para determinar si las cuentas con sus sucursales se utilizan o no para proporcionar indirectamente servicios a bancos fantasmas extranjeros.

_ Una lista de todas las cuentas bancarias corresponsales extranjeras y de las relaciones con instituciones financieras extranjeras que se hayan cerrado o hayan cesado en conformidad con las condiciones de 31 CFR 103.177 (p. ej., servicio a bancos fantasmas extranjeros, registros de propietarios y agentes).

_ Una lista de las cuentas bancarias corresponsales extranjeras que hayan sido objeto de un 31 CFR 103.100 (Intercambio de información entre las agencias federales de aplicación de la ley y las instituciones financieras) o de cualquier otra solicitud de información por parte de un oficial federal de aplicación de la ley sobre cuentas bancarias corresponsales extranjeras y demostración de cumplimiento.

_ Cualquier notificación que solicite el cierre de cuentas bancarias corresponsales extranjeras por parte del Secretario del Tesoro o el Procurador General de Estados Unidos y la demostración de cumplimiento.

_ Ponga a disposición copias de las políticas, los procedimientos y procesos para cumplir con 31 CFR 103.177.

_ Una lista de todas las cuentas de consulados o embajadas del banco u otras cuentas mantenidas por un gobierno extranjero, embajada extranjera o político extranjero de alto nivel.

_ Una lista de todos los titulares de cuenta y solicitantes de préstamos domiciliados fuera de Estados Unidos, incluidos los apoderados estadounidenses.

Actividad de envío de moneda

_ Ponga a disposición registros que reflejen el envío de moneda hacia el Banco de la Reserva Federal o los bancos corresponsales y la recepción de envíos provenientes de las mencionadas entidades, o que reflejen el envío de moneda entre sucursales y las bóvedas centrales de sus bancos durante los _____ meses previos. (*El inspector debe introducir un período de tiempo adecuado según el tamaño y la complejidad del banco*).

Otras exigencias con respecto a la gestión de registros y presentación de informes de la BSA

_ Cronograma de conservación de registros y pautas sobre procedimientos.

_ Presentación de Informes sobre el transporte internacional de moneda o instrumentos monetarios (CMIR) (Formulario 105 de la FinCEN, anteriormente conocido como Formulario de la aduana 4790).

_ Registros de Informe de cuentas de banco y financieras en un banco del extranjero (FBAR) (TD F 90-22.1).

OFAC

_ Nombre y cargo del funcionario de cumplimiento de la OFAC designado y, si es diferente, nombre y cargo de la persona responsable de supervisar el cumplimiento de la OFAC.

_ Un organigrama que muestre las líneas de comunicación directas e indirectas.

_ Copias de curriculum vitae y títulos académicos de la persona (o personas) que haya empezado a trabajar en el banco recientemente actuando en calidad de supervisor del programa de cumplimiento con la OFAC.

_ El cronograma de capacitación OFAC con fechas, asistentes y temas. Una lista de personas que ocupan puestos para los que el banco generalmente exige capacitación OFAC, que no hayan participado en la capacitación.

_ Ponga a disposición copias de los resultados de auditorías independientes provenientes de fuentes internas o externas o de pruebas realizadas desde la inspección OFAC previa, incluidos el campo de aplicación o la carta de compromiso, las respuestas de la gerencia y el acceso a los documentos.

_ Ponga a disposición copias del análisis de riesgos de la OFAC realizado por la gerencia de los productos, servicios, clientes y ubicaciones geográficas.

_ Ponga a disposición copias de las políticas y los procedimientos de la OFAC.

_ Ponga a disposición una lista de las transacciones bloqueadas o rechazadas con personas o entidades que están en la lista de la OFAC y que fueron informadas a la OFAC. *(Los bancos deben informar todos los bloqueos dentro de los diez días mediante la presentación de un Informe de transacciones bloqueadas).*

_ Si se conservan, ponga a disposición registros u otra documentación relacionada con el control de las coincidencias potenciales con las listas de la OFAC, incluido el método para revisar y borrar aquellas que son coincidencias.

_ Proporcione una lista de todas las licencias expedidas por la OFAC al banco. *Por medio de un proceso de expedición de licencias, la OFAC tiene autoridad para permitir ciertas*

transacciones que están prohibidas por sus reglamentos. Si el cliente de un banco afirma poseer una licencia específica, el banco debe verificar que la transacción cumpla con los términos de la licencia y debe obtener una copia de la licencia que la autoriza.

_ Si corresponde, proporcione una copia de los registros que verifican que se han instalado las actualizaciones más recientes en el software de la OFAC.

_ Proporcione una copia del Informe anual de propiedades bloqueadas presentado ante la OFAC (TD F 90-22.50). *(Los bancos deben informar todos los activos bloqueados a la OFAC anualmente al 30 de Septiembre).*

Procedimientos de inspección de la sección ampliada

Como parte del proceso de planificación de la inspección, el inspector debe preparar una carta de solicitud. La lista que aparece a continuación incluye materiales que *pueden* solicitarse en la inspección BSA/AML de un banco. Se debe adaptar la lista de acuerdo al perfil específico de la institución y el campo de aplicación planificado de la inspección. Se pueden solicitar materiales adicionales según sea necesario.

Cuentas corresponsales (nacionales)

_ Ponga a disposición copias de políticas, procedimientos y procesos específicos de las cuentas corresponsales del banco, incluidos los procedimientos para supervisar actividades sospechosas.

_ Ponga a disposición una lista de las cuentas corresponsales nacionales del banco.

_ Proporcione una lista de los SAR presentados con respecto a las cuentas corresponsales nacionales del banco.

Cuentas corresponsales (extranjeras)

_ Ponga a disposición copias de políticas, procedimientos y procesos específicos de las cuentas de instituciones financieras corresponsales extranjeras, incluidos los procedimientos para supervisar actividades sospechosas.

_ Ponga a disposición una lista de cuentas de instituciones financieras corresponsales extranjeras.

_ Proporcione análisis de riesgos que abarquen las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras.

_ Proporcione una lista de los SAR presentados con respecto a las cuentas de instituciones financieras corresponsales extranjeras.

Envíos de moneda en grandes cantidades

_ Ponga a disposición copias de políticas, procedimientos y procesos relacionados con la recepción de envíos de moneda en grandes cantidades. Descripción de los procedimientos de supervisión ampliados aplicados a remitentes de moneda e intermediarios.

_ Ponga a disposición una lista de remitentes de moneda, intermediarios, incluso agentes referentes y clientes extranjeros y nacionales que envían dinero en grandes cantidades al banco.

_ Proporcione una lista de todas las cuentas bancarias extranjeras y nacionales, incluso una lista de las instituciones financieras extranjeras de las cuales el banco recibe o a las cuales remite envíos de dinero en grandes cantidades.

_ Proporcione una copia del análisis de riesgos de la gerencia sobre las relaciones y transacciones de remitentes de moneda e intermediarios.

_ Ponga a disposición copias de los informes utilizados para la identificación y la supervisión de transacciones sospechosas relacionadas con remitentes de moneda e intermediarios.

_ Ponga a disposición acuerdos o contratos con remitentes de moneda e intermediarios.

_ Proporcione una relación de los informes SAR presentados de envios y transacciones relacionadas.

Giros en dólares estadounidenses

_ Ponga a disposición copias de políticas, procedimientos y procesos específicos de los giros en dólares estadounidenses, incluidos los procedimientos para supervisar actividades sospechosas.

_ Ponga a disposición una lista de cuentas corresponsales extranjeras que ofrecen giros en dólares estadounidenses. Si es posible, incluya el volumen, por cantidad y suma en dólares, de las transacciones mensuales de cada cuenta.

_ Proporcione una lista de los informes SAR presentados con respecto a los giros en dólares estadounidenses.

Cuentas empleadas para pagos

_ Poner a disposición copias de políticas, procedimientos y procesos específicos de las cuentas empleadas para pagos (PTA), incluidos los procedimientos para supervisar actividades sospechosas.

_ Ponga a disposición una lista de cuentas corresponsales extranjeras del banco con PTA. Incluya un resumen detallado (cantidad y volumen en dólares mensual) de cotitulares de cuentas PTA.

_ Proporcione una lista de los informes SAR presentados con respecto a las PTA.

Actividades de depósitos vía maletines/bolsos

_ Ponga a disposición copias de políticas, procedimientos y procesos de las actividades de depósitos vía maletines/bolsos, incluidos los procedimientos para supervisar actividades sospechosas.

_ Proporcione una lista de las cuentas de clientes a los que se les permite utilizar los servicios de depósitos vía maletines/bolsos.

_ Proporcione una lista de los informes CTR, CMIR, o SAR presentados con respecto a las actividades de depósitos vía maletines/bolsos.

_ Según sea necesario, proporcione una copia de los registros de depósitos vía maletines/bolsos.

Sucursales y oficinas en el extranjero de bancos estadounidenses

_ Ponga a disposición copias de políticas, procedimientos y procesos específicos de la sucursal u oficina extranjera, si fueran diferentes a las políticas, los procedimientos y los procesos de la compañía matriz.

_ Proporcione los informes de gestión más recientes que se recibieron sobre las sucursales y oficinas en el extranjero.

_ Ponga a disposición copias del informe de la estructura organizativa o de la estratificación del banco.

_ Proporcione informes de auditoría AML, informes de cumplimiento y documentación respaldatoria de las sucursales y oficinas en el extranjero.

_ Proporcione una lista de los tipos de productos y servicios ofrecidos por las sucursales y oficinas en el extranjero e información sobre nuevos productos o servicios ofrecidos por la sucursal en el extranjero, incluidos aquellos que la casa matriz todavía no ofrece.

_ Proporcione una descripción del método de acumulación de todas las relaciones con clientes en todas las unidades comerciales y ubicaciones geográficas en toda la organización.

_ Proporcione una copia del Código de ética de las sucursales u oficinas en el extranjero, si fuera diferente a la política estándar del banco.

_ Cuando se realicen pruebas, proporcione una lista de las cuentas originadas o revisadas en la sucursal u oficina en el extranjero. Los inspectores deben intentar limitar esta solicitud y enfocarse en las cuentas de productos o servicios específicos, sólo en las cuentas de alto riesgo, o en las cuentas que hayan generado preocupaciones relacionadas con las auditorías o en las que se hayan descubierto excepciones.

_ Proporcione una lista de ubicaciones de sucursales y oficinas en el extranjero, incluyendo, si es posible, la agencia regulatoria del país anfitrión y la información de contacto.

_ Proporcione la estructura organizativa de las sucursales y oficinas en el extranjero, incluidas las líneas de comunicación a nivel del banco estadounidense.

Banca paralela

_ Proporcione una lista de cualquier relación asociada con la banca paralela.

_ Ponga a disposición copias de políticas, procedimientos y procesos específicos de las relaciones asociadas con la banca paralela, incluidos los procedimientos relacionados con las actividades de alto riesgo de lavado de dinero. Dichos procedimientos y políticas deben incluir aquellos que son específicos de la relación con la entidad paralela.

_ Proporcione una lista de los informes SAR presentados con respecto a las relaciones asociadas con la banca paralela.

_ Ponga a disposición documentos que especifiquen restricciones o procedimientos que deban cumplirse al tratar con la entidad paralela.

_ Proporcione una lista de directores o funcionarios del banco que también estén asociados con el banco paralelo extranjero.

Banca electrónica

_ Ponga a disposición copias de cualquier política y procedimiento relacionados de manera directa con la banca electrónica (*e-banking* o sistemas de transacciones bancarias a través de Internet) que todavía no estén incluidos en las políticas BSA/AML.

_ Proporcione informes de gestión que indiquen el volumen mensual de la actividad de banca electrónica.

_ Proporcione una lista de los clientes comerciales que habitualmente efectúan transacciones de banca electrónica, incluidos la cantidad y el volumen en dólares de las transacciones.

_ Ponga a disposición una lista de prestadores de servicios relacionados con actividades de captura de depósitos remotos (RDC).

_ Ponga a disposición copias de contratos relacionados con actividades de captura de depósitos remotos (RDC).

Transferencias de fondos

_ Proporcione registros de transferencias de fondos, incluso transferencias de fondos que involucren pagos de cobertura y transferencias que salen del banco y se reciben en éste. Incluya la cantidad y volumen en dólares de la actividad de transferencias de fondos del mes.

_ Proporcione una lista de transferencias de fondos adquiridas con dinero en efectivo durante un período de tiempo específico.

_ Proporcione una lista de transacciones de individuos que no son clientes durante un período de tiempo específico.

_ Si todavía no están incluidas en las políticas BSA/AML, ponga a disposición copias de cualquier política, procedimiento y proceso relacionados con transferencias de fondos, inclusive transferencias que involucren pagos de cobertura o transacciones pagaderas mediante presentación de identificación apropiada (PUPID).

_ Proporcione una lista de cuentas puente o de tránsito utilizadas para ingresos de PUPID.

_ Proporcione una lista de transacciones PUPID efectuadas por el banco, ya sea actuando como banco beneficiario o como banco remitente.

Transacciones de compensación automatizada

_ Ponga a disposición copias de políticas y procedimientos relacionados de manera directa con las transacciones de compensación automatizadas (ACH) y las transacciones de ACH internacionales (IAT) que todavía no estén incluidos en las políticas BSA/AML.

_ Ponga a disposición copias de informes de gestión que indiquen el volumen mensual de actividad de ACH, incluidas las IAT.

_ Ponga a disposición una lista de transacciones frecuentes o de grandes volúmenes de ACH o IAT.

_ Ponga a disposición una lista de IAT (tanto de aquellas originadas por el banco como de las recibidas por éste).

_ Ponga a disposición una lista de quejas de clientes con respecto a transacciones de ACH y de IAT.

Efectivo electrónico

_ Ponga a disposición copias de políticas y procedimientos relacionados de manera directa con el efectivo electrónico (*e-cash*), incluidas las tarjetas prepagadas, que todavía no estén incluidos en las políticas BSA/AML.

_ Proporcione informes de gestión que indiquen el volumen mensual de la actividad de efectivo electrónico, incluidas las tarjetas prepagadas.

_ Proporcione una lista de los clientes comerciales que habitualmente efectúan transacciones de efectivo electrónico, incluidas las tarjetas prepagadas, con la cantidad y el volumen en dólares de las transacciones.

Procesadores de pagos externos

_ Si todavía no están incluidas en las políticas BSA/AML, ponga a disposición copias de cualquier política, procedimiento y proceso relacionados con procesadores de pagos externos.

_ Proporcione una lista de las relaciones asociadas con procesadores de pagos externos. Incluya la cantidad y volumen en dólares de los pagos procesados por cada relación.

_ Proporcione una lista de los SAR presentados acerca de las relaciones asociadas con procesadores de pagos externos.

Compraventa de instrumentos monetarios

_ Si todavía no están incluidas en las políticas BSA/AML, ponga a disposición copias de cualquier política, procedimiento y proceso relacionados con la venta de instrumentos monetarios a cambio de dinero. Particularmente, incluya políticas, procedimientos y procesos relacionados con la supervisión de las ventas de instrumentos monetarios para detectar actividades poco habituales.

_ Proporcione registros de los instrumentos monetarios u otros informes MIS utilizados para la supervisión y detección de actividades sospechosas relacionadas con las ventas de instrumentos monetarios.

_ Proporcione una lista de transacciones de individuos que no son clientes durante un período de tiempo específico.

_ Proporcione una lista de instrumentos monetarios adquiridos con dinero en efectivo durante un período de tiempo específico.

_ Proporcione una lista de los SAR presentados relacionados con la compraventa de instrumentos monetarios.

Depósitos mediante agentes

_ Poner a disposición copias de políticas, procedimientos y procesos específicos relativos a depósitos mediante agentes, incluidos los procedimientos para supervisar actividades sospechosas.

_ Proporcione análisis de riesgos que abarquen los depósitos mediante agentes.

_ Proporcione auditorías internas que abarquen los depósitos mediante agentes.

_ Proporcione una lista de los agentes de depósito autorizados.

_ Proporcione informes de gestión que abarquen los programas de financiamiento que no estén basados en relaciones (incluidos los informes sobre saldos, concentraciones, rendimiento o cargos pagados).

_ Proporcione SAR y citaciones con respecto a las relaciones asociadas con depósitos mediante agentes.

_ Proporcione una copia de la documentación de la cuenta o acuerdos relacionados con los convenios con agentes de depósito.

Cajeros automáticos de propiedad privada

_ Proporcione análisis de riesgos que abarquen los cajeros automáticos de propiedad privada y las Organizaciones de Ventas Independientes (ISO), incluso una lista de las relaciones asociadas con los cajeros automáticos de propiedad privada de alto riesgo.

_ Ponga a disposición copias de políticas, procedimientos y procesos aplicables a los cajeros automáticos de propiedad privada y la aceptación de cuentas de ISO, la debida diligencia y la supervisión continua.

_ Proporcione una lista de los clientes y los saldos de las ISO.

_ Proporcione SAR y citaciones relacionados con los cajeros automáticos de propiedad privada y las ISO.

Productos de inversión que no son para depositar

_ Ponga a disposición copias de políticas, procedimientos y procesos relacionados con los productos de inversión que no son para depositar (NDIP) y las relaciones con cualquier proveedor independiente de NDIP.

_ Proporcione auditorías internas que abarquen las ventas de NDIP y las relaciones asociadas con los proveedores de esos productos.

_ Proporcione análisis de riesgos que abarquen los clientes y las transacciones de NDIP.

_ Si está disponible, proporcione una lista de clientes y saldos de NDIP.

_ Proporcione una lista de cuentas puente o de tránsito, de concentración u ómnibus utilizadas para los NDIP. Describa el propósito y los controles en torno a cada cuenta.

_ Proporcione informes de gestión que abarquen de 25 a 50 de los clientes de NDIP más importantes, más activos y con más ganancias.

_ Proporcione SAR y citaciones relacionados con clientes de NDIP.

_ Ponga a disposición una copia de la documentación o los acuerdos de apertura de cuentas para los NDIP.

_ Ponga a disposición una copia de los contratos o acuerdos entre el banco y los proveedores externos de NDIP para la aplicación del CIP, la debida diligencia y la supervisión continua de clientes de NDIP.

Seguros

_ Ponga a disposición copias de políticas y procedimientos BSA/AML relacionados con la venta de seguros.

_ Proporcione análisis de riesgos que abarquen los productos de seguros.

_ Ponga a disposición informes de MIS relacionados con las ventas de productos de seguros. Los informes pueden incluir aquellos que traten sobre transacciones de grandes volúmenes, cancelación anticipada, sobrepagos de la prima y cesiones de derecho a un pago.

_ Ponga a disposición una copia de los contratos o acuerdos entre el banco y los proveedores de seguros para la aplicación del CIP, la debida diligencia y la supervisión continua de clientes de seguros.

_ Proporcione una lista de productos de seguros autorizados para la venta en el banco.

_ Proporcione informes de gestión que abarquen productos de seguros (incluidas las transacciones de grandes volúmenes, las transferencias de fondos, los pagos únicos de la prima y las cancelaciones anticipadas).

_ Proporcione informes SAR o citaciones relacionados con los clientes de seguros.

_ Proporcione una copia de las exigencias y aplicaciones relacionadas con la documentación de la cuenta para los productos de seguros.

Cuentas de concentración

_ Ponga a disposición copias de políticas, procedimientos y procesos BSA/AML específicos de las cuentas de concentración (también conocidas como cuentas especiales, cuentas ómnibus, cuentas puente o de tránsito, de liquidación, intradía, de barrido o de cobro).

_ Proporcione una lista de todas las cuentas de concentración y la conciliación más reciente de cada cuenta.

_ Proporcione informes de actividad de la cuenta sobre las cuentas de concentración durante _____. (*El inspector debe introducir un período de tiempo adecuado según el tamaño y la complejidad del banco*).

Actividades de préstamo

_ Ponga a disposición copias de políticas y procedimientos BSA/AML que se apliquen específicamente a los préstamos.

_ Proporcione análisis de riesgos relacionados con la función de préstamo, incluida una lista de cualquier relación asociada con préstamos de alto riesgo identificada por el banco.

_ Respecto a los préstamos garantizados con efectivo, valores negociables o valor de rescate en efectivo de los productos de seguros de vida:

- Proporcione una lista de todos los préstamos que no se hayan pagado desde la inspección BSA/AML anterior, incluidos aquellos cuyos cargos hayan sido anulados.
- Proporcione una lista de todos los préstamos que han sido otorgados desde la anterior inspección BSA/AML.

Actividades de financiación del comercio internacional

_ Ponga a disposición copias de políticas y procedimientos BSA/AML que se apliquen específicamente a las actividades de financiación del comercio internacional.

_ Proporcione análisis de riesgos relacionados con las actividades de financiación del comercio internacional, incluida una lista de cualquier transacción, cuenta o relación de financiación del comercio internacional de alto riesgo identificada por el banco.

_ Proporcione una lista de clientes involucrados en transacciones con ubicaciones geográficas de alto riesgo o para los cuales el banco facilita actividades de financiación del comercio internacional con ubicaciones geográficas de alto riesgo.

Banca privada

_ Ponga a disposición copias de políticas, procedimientos y controles utilizados para gestionar riesgos BSA/AML en el departamento de banca privada.

_ Ponga a disposición planes estratégicos o de negocios para el departamento de banca privada.

_ Proporcione la versión más reciente de los informes de gestión sobre la actividad de la banca privada, tales como los informes sobre acumulación de clientes, informes sobre excepciones a las políticas, cuentas de concentración de clientes, informes de clasificación de riesgos de clientes y sobre actividad poco habitual de la cuenta.

_ Proporcione informes sobre la banca privada recientes elaborados a partir de información sobre cumplimiento, auditoría interna, gestión de riesgos, y por parte de auditores o consultores externos que abarcan BSA/AML.

_ Proporcione una lista de productos y servicios ofrecidos a los clientes de la banca privada. Información sobre nuevos productos y servicios ofrecidos a los clientes de la banca privada y sobre el proceso del banco para aprobar nuevas actividades.

_ Proporcione una descripción del método de acumulación de la participación y las actividades de los clientes en las unidades comerciales de toda la organización.

_ Proporcione una descripción de los puestos de gerentes y oficiales de cuenta y los programas de compensación, contratación y capacitación para estos puestos.

_ Ponga a disposición la política del código de ética para los funcionarios de la banca privada.

_ Proporcione análisis de riesgos que abarquen los clientes y las transacciones de la banca privada.

_ Proporcione una lista de cuentas puente o de tránsito, de concentración u ómnibus utilizadas para las transacciones de la banca privada. Describa el propósito de cada cuenta y los controles que la rigen.

_ Proporcione informes de gestión que abarquen de 25 a 50 de los clientes de la banca privada más importantes, más activos o con más ganancias.

_ Proporcione una lista de los titulares de las cuentas de la banca privada que cumplen con los siguientes criterios:

- Personalidades sujetas a exposición política (PEP), propietarios de negocios de importación o exportación, transmisores de dinero, Compañías de Inversión Privada (PIC), asesores financieros, entidades instaladas en el exterior o administradores financieros (cuando actúa un intermediario en nombre de los clientes).
- Clientes que comenzaron a operar con el banco por recomendación de individuos que eran empleados de otras instituciones financieras.
- Clientes que comenzaron a operar con el banco por recomendación de un asesor de inversiones externo.

- Los clientes que utilizan una razón social genérica.
- Clientes que provienen de una ubicación geográfica de alto riesgo o que realizan negocios con tal ubicación geográfica.
- Clientes que participan en negocios intensivos en efectivo.
- Clientes a quienes se les concedieron excepciones respecto a políticas, procedimientos y controles.
- Clientes que con frecuencia aparecen en informes de supervisión de actividades poco habituales.

_ Proporcione SAR y citaciones relacionados con clientes de la banca privada.

_ Ponga a disposición una copia de la documentación o los acuerdos de apertura de la cuenta para los clientes de la banca privada.

Servicios de gestión de fideicomisos y de activos

_ Ponga a disposición copias de políticas, procedimientos y procesos BSA/AML que se apliquen a los servicios de gestión de fideicomisos y de activos.

_ Ponga a disposición procedimientos y pautas de gestión de fideicomisos y de activos utilizados para determinar cuando es adecuado aplicar debida diligencia especial a las cuentas y las partes de alto riesgo de la relación. Estos deben incluir métodos para identificar quienes son las partes interesadas de la cuenta (es decir, otorgantes particulares, coadministradores de bienes o administradores de inversiones externos).

_ Proporcione una lista de los titulares de cuentas de gestión de fideicomisos y de activos que cumplen con los siguientes criterios:

_ Proporcione una lista de personalidades sujetas a exposición política (PEP), propietarios de negocios de importación o exportación, transmisores de dinero, Compañías de Inversión Privada (PIC), asesores financieros, entidades instaladas en el exterior o administradores financieros (cuando actúa un intermediario en nombre de los clientes).

- Clientes que comenzaron a operar con el banco por recomendación de individuos que eran empleados de otras instituciones financieras.
- Clientes que comenzaron a operar con el banco por recomendación de un asesor de inversiones externo.
- Los clientes que utilizan una razón social genérica.
- Clientes que provienen de una ubicación geográfica de alto riesgo o que realizan negocios con tal ubicación geográfica.
- Clientes que participan en negocios intensivos en efectivo.

- Clientes a quienes se les concedieron excepciones respecto a políticas, procedimientos y controles.
- Clientes que con frecuencia aparecen en informes de supervisión de actividades poco habituales.

_ Ponga a disposición informes y actas enviados a la junta directiva o a su comité designado relacionados con asuntos de BSA/AML sobre rubros de la actividad comercial y actividades de gestión de fideicomisos y de activos.

_ Proporcione un organigrama de la función de cumplimiento BSA/AML en relación con los servicios de gestión de fideicomisos y de activos.

_ Proporcione un análisis de riesgos de los servicios de gestión de fideicomisos y de activos que identifique aquellos clientes, clientes probables o productos que el banco haya determinado que son de alto riesgo.

_ Proporcione informes de gestión que abarquen de 25 a 50 de los clientes de los servicios de gestión de fideicomisos y de activos más importantes, más activos o con más ganancias.

_ Proporcione un control o auditoría independiente BSA/AML de los servicios de gestión de fideicomisos y de activos. Ponga a disposición documentos a solicitud.

_ Ponga a disposición copias de los materiales de capacitación BSA/AML de la gerencia y los empleados involucrados en las actividades de gestión de fideicomisos y de activos.

_ Identifique los sistemas de contabilidad utilizados en los fideicomisos. Explique brevemente cómo se adaptan y asisten en el cumplimiento de las pautas y los reglamentos BSA/AML.

_ Proporcione una lista de cuentas de gestión de fideicomisos y de activos abiertas recientemente desde _____. *(El inspector debe introducir un período de tiempo adecuado según el tamaño y la complejidad del banco).*

_ Proporcione procedimientos para verificar las solicitudes según la sección 314(a) relacionadas con los servicios de gestión de fideicomisos y de activos.

_ Proporcione una lista de todas las cuentas de gestión de fideicomisos y de activos designadas como de alto riesgo y una lista de todas las cuentas cuyos activos consisten en PIC y fideicomisos de protección patrimonial.

_ Proporcione copias de los SAR asociados con servicios de gestión de fideicomisos y de activos.

_ Proporcione una lista de citaciones, particularmente relacionadas con la ley de secreto bancario y el lavado de dinero, con respecto a actividades de gestión de fideicomisos y de activos.

Extranjeros no residentes y ciudadanos extranjeros

_ Ponga a disposición copias de políticas, procedimientos y procesos que se apliquen específicamente a las cuentas de extranjeros no residentes (NRA), incluidas las pautas y los sistemas para establecer y actualizar la condición de exento según el formulario W-8.

_ Proporcione una lista de cuentas de NRA y ciudadanos extranjeros mantenidas por el banco, particularmente aquellas que el banco haya designado como de alto riesgo.

_ Proporcione una lista de cuentas de NRA y ciudadanos extranjeros sin un TIN, número de pasaporte u otro número de identificación adecuado.

_ Proporcione una lista de SAR y citaciones relacionados con cuentas de NRA y ciudadanos extranjeros.

Personalidades sujetas a exposición política

_ Ponga a disposición copias de políticas, procedimientos y procesos que se apliquen específicamente a las personalidades sujetas a exposición política (PEP). Las políticas deben incluir la definición del banco de una PEP y también los procedimientos para abrir cuentas de PEP y el papel de la alta gerencia en el proceso de aprobación de la apertura de cuentas de PEP.

_ Proporcione una lista de cuentas a nombre de una PEP o en su beneficio. La lista debe incluir el país de residencia de la PEP, los saldos de la cuenta y la cantidad y el volumen en dólares promedio de las transacciones mensuales.

_ Proporcione una lista de los sistemas de información u otros métodos utilizados para identificar cuentas de PEP.

_ Ponga a disposición informes de gestión utilizados para supervisar las cuentas de PEP, incluidos los informes para identificar actividades sospechosas y poco habituales.

Cuentas de embajadas y consulados extranjeros

_ Ponga a disposición copias de políticas, procedimientos y procesos aplicables específicamente a las relaciones asociadas con cuentas de embajadas y consulados extranjeros.

_ Proporcione una lista de cuentas de embajadas y consulados extranjeros mantenidas por el banco, incluidos los saldos de cuentas y la cantidad y el volumen en dólares promedio de las transacciones mensuales.

_ Proporcione una lista de cuentas que estén a nombre de individuos que trabajan para la embajada o el consulado extranjero.

Instituciones financieras no bancarias

_ Ponga a disposición copias de políticas, procedimientos y procesos relacionados con instituciones financieras no bancarias.

_ Proporcione una lista de las cuentas de instituciones financieras no bancarias, incluidas todas las cuentas relacionadas.

_ Proporcione un análisis de riesgos de las cuentas de instituciones financieras no bancarias, identificando aquellas que el banco haya designado como de alto riesgo. Esta lista debe incluir productos y servicios ofrecidos por la institución financiera no bancaria; el saldo promedio de la cuenta; y la cantidad, el tipo y el volumen en dólares promedio de las transacciones mensuales.

_ Proporcione una lista de cuentas de instituciones financieras no bancarias, incluidos los productos y servicios ofrecidos; el saldo promedio de la cuenta; y el promedio, la cantidad, el tipo y el volumen en dólares de transacciones mensuales.

_ Proporcione una muestra de la documentación de apertura de la cuenta para las instituciones financieras no bancarias de alto riesgo.

_ Proporcione una lista de SAR y citaciones relacionados con instituciones financieras no bancarias.

Prestadores de servicios profesionales

_ Ponga a disposición copias de políticas, procedimientos y procesos relacionados con cuentas de prestadores de servicios profesionales.

_ Proporcione una lista de las cuentas de prestadores de servicios profesionales, incluidas todas las cuentas relacionadas (como las cuentas fiduciarias de abogados con rendimiento de interés [IOLTA] que deben incluir el nombre del apoderado de cada cuenta).

_ Proporcione una lista de cuentas de prestadores de servicios profesionales que el banco haya designado como de alto riesgo.

Organizaciones no gubernamentales y entidades de beneficencia

_ Ponga a disposición copias de políticas, procedimientos y procesos relacionados con organizaciones no gubernamentales y entidades de beneficencia.

_ Una lista de organizaciones no gubernamentales y entidades de beneficencia, particularmente aquellas que el banco haya designado como de alto riesgo. Esta lista debe incluir los saldos de la cuenta y la cantidad y el volumen en dólares promedio de las transacciones.

_ Una lista de organizaciones no gubernamentales involucradas en ubicaciones geográficas de alto riesgo.

Entidades comerciales (nacionales y extranjeras)

_ Ponga a disposición copias de políticas, procedimientos y procesos aplicables específicamente a entidades comerciales nacionales y extranjeras.

_ Proporcione una lista de cuentas abiertas por entidades comerciales. Si esta lista es demasiado extensa, enmiende la solicitud para tener en cuenta aquellas entidades constituidas en jurisdicciones de alto riesgo o aquellas que el banco haya designado como de alto riesgo.

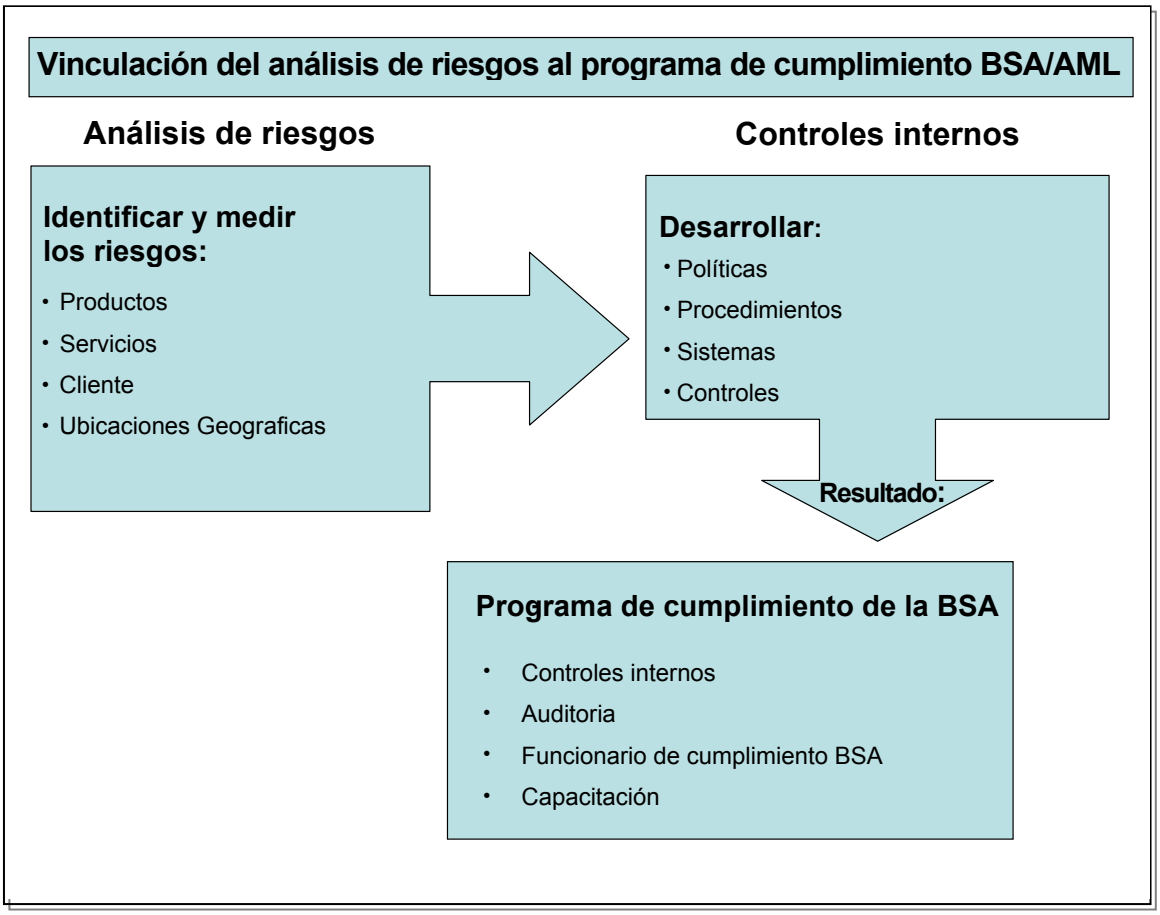
_ Proporcione una lista de préstamos a entidades comerciales respaldadas con acciones al portador.

Negocios intensivos en efectivo

_ Ponga a disposición copias de políticas, procedimientos y procesos relacionados con otros negocios y entidades.

_ Proporcione análisis de riesgos de otros negocios y entidades, enumere otros negocios y entidades que el banco haya designado como de alto riesgo. La lista debe incluir los saldos de la cuenta y la cantidad y el volumen en dólares promedio de las transacciones.

Apéndice I: Vinculación del análisis de riesgos al programa de cumplimiento BSA/AML



Apéndice J: Cuadro de Cantidad de Riesgos

Los bancos y los inspectores podrán utilizar el siguiente cuadro para formular un resumen de conclusiones: Antes de utilizar este cuadro, se deberán completar los pasos de identificación y cuantificación detallados en la sección de esquema general de Análisis de Riesgos BSA/AML en las páginas 23 a 33 de este manual.

Bajo	Moderado	Alto
Clientela estable, conocida.	La clientela aumenta debido a sucursales, fusiones o adquisiciones.	Una gran clientela en crecimiento en un área geográfica muy amplia y diversa.
No hay banca electrónica (*e-banking*) o el sitio Web es informativo o no transaccional.	El banco recién implementa la banca electrónica y ofrece una cantidad limitada de productos y servicios.	El banco ofrece una gran variedad de productos y servicios de banca electrónica (por ej. transferencias entre cuentas, pagos de facturas por banca electrónica o apertura de cuentas por Internet).
Sobre la base de información recibida del banco de datos de informes de BSA, hay pocas transacciones fraccionadas o de grandes volúmenes de dinero o directamente no hay.	Sobre la base de información recibida del banco de datos de informes de BSA, hay una cantidad moderada de transacciones fraccionadas o de grandes volúmenes de dinero.	Sobre la base de información recibida del banco de datos de informes de BSA, hay una cantidad considerable de transacciones fraccionadas o de grandes volúmenes de dinero.
Se identificaron pocos clientes y negocios de alto riesgo.	Se identificó una moderada cantidad de clientes y negocios de alto riesgo.	Se identificó una gran cantidad de clientes y negocios de alto riesgo.

Bajo	Moderado	Alto
No hay cuentas de instituciones financieras extranjeras corresponsales. El banco no se dedica a actividades de depósito vía maletines/bolsos, ni ofrece cuentas para uso especial, ni cuentas empleadas para pagos (PTA), ni ofrece servicios de giros denominados en dólares estadounidenses.	El banco tiene pocas cuentas de instituciones financieras corresponsales extranjeras, pero por lo general con instituciones financieras con políticas y procedimientos de AML adecuados de países de bajo riesgo, y pocas actividades de depósitos vía maletines/bolsos, cuentas para uso especial, cuentas empleadas para pagos (PTA) o servicios de giros denominados en dólares estadounidenses.	El banco tiene una gran cantidad de cuentas de instituciones financieras corresponsales extranjeras con políticas y procedimientos de AML poco adecuados, especialmente aquellos ubicados en jurisdicciones de alto riesgo, u ofrece bastantes actividades de depósitos vía maletines/bolsos, cuentas para uso especial, cuentas empleadas para pagos (PTA), o servicios de giros denominados en dólares estadounidenses.
El banco no ofrece servicios de banca privada ni de gestión de fideicomisos y de activos o los ofrece en forma limitada.	El banco ofrece una cantidad limitada de servicios de banca privada nacional o productos y servicios de gestión de fideicomisos y de activos sobre los cuales tiene discreción para invertir. El plan estratégico podría ser incrementar el negocio del fideicomiso.	El banco ofrece muchos servicios de banca privada nacional e internacional o productos o servicios de gestión de fideicomisos y de activos. Los servicios de banca privada o de gestión de fideicomisos y de activos están creciendo. Los productos ofrecidos incluyen servicios de administración de inversiones, y las cuentas de fideicomiso son primordialmente no discrecionales, excepto donde el banco tiene plena discreción para invertir.
Pocas cuentas internacionales o bajo volumen de actividad en moneda en las cuentas.	Moderado nivel de cuentas internacionales con actividades en moneda no explicadas.	Gran cantidad de cuentas internacionales con actividades en moneda no explicadas.

Bajo	Moderado	Alto
Limitada cantidad de transferencias de fondos de clientes, no clientes, limitada cantidad de transacciones de partes externas; sin transferencias de fondos del exterior.	Una moderada cantidad de transferencias de fondos. Pocas transferencias de fondos internacionales desde cuentas personales o comerciales por lo general con países de bajo riesgo.	Una gran cantidad de transacciones de transferencias de fondos de individuos que no son clientes y transacciones pagaderas mediante presentación de identificación apropiada (PUPID). Fondos frecuentes desde o hacia cuentas personales o comerciales de jurisdicciones de alto riesgo y refugios o jurisdicciones con secreto bancario.
El banco no está ubicado en Zonas de alta densidad de narcotráfico (HIDTA)[271] o Zonas de alta densidad de delitos financieros (HIFCA). No hay transferencias de fondos ni relaciones de cuentas que involucren HIDTA o HIFCA.	El banco está ubicado en una HIDTA o una HIFCA. El banco tiene algunas transferencias de fondos o relaciones de cuentas que involucran HIDTA o HIFCA.	El banco está ubicado en una HIDTA o en una HIFCA. Una gran cantidad de transferencias de fondos o relaciones de cuentas involucran HIDTA o HIFCA.
No hay transacciones con ubicaciones geográficas de alto riesgo.	Cantidad mínima de transacciones con ubicaciones geográficas de alto riesgo.	Importante volumen de transacciones con ubicaciones geográficas de alto riesgo.
Baja rotación de personal clave o de contacto directo con clientes (por ej. representantes de atención a clientes, cajeros, u otro tipo de personal de la sucursal).	Baja rotación de personal clave, pero el personal de contacto directo con clientes podría haber cambiado.	Mucha rotación, especialmente en los puestos del personal clave.

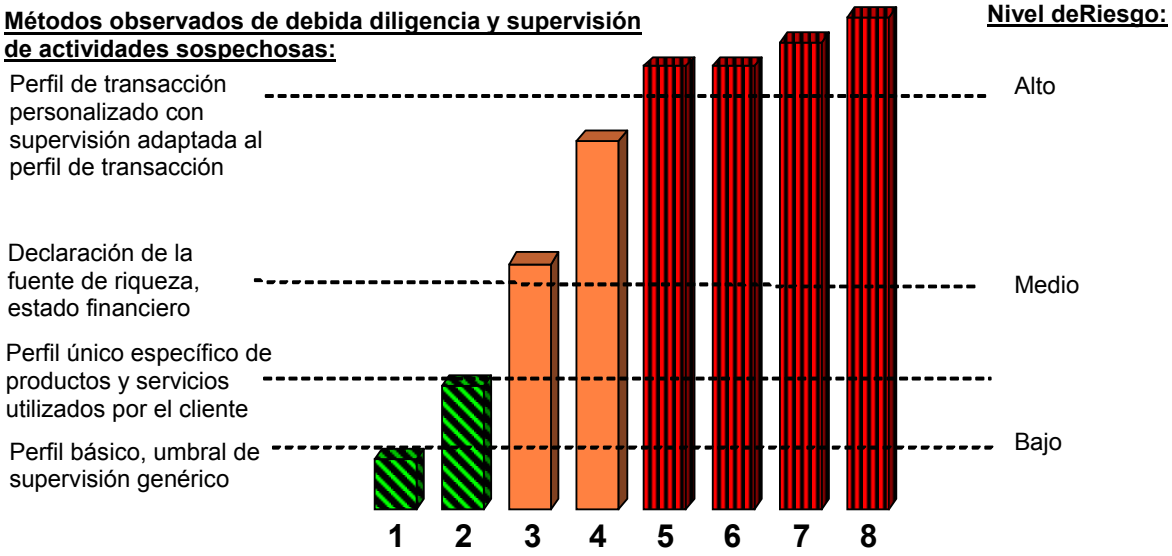
[271] El sitio www.whitehousedrugpolicy.gov/index.html dispone de una lista de HIDTA.

Apéndice K: Riesgos del Cliente Frente a la Debida Diligencia y la Supervisión de Actividades Sospechosas

A modo de ejemplo

Riesgos del cliente frente a la debida diligencia y la supervisión de actividades sospechosas

Algunas relaciones con los clientes pueden plantear más riesgos que otras. Este cuadro proporciona un ejemplo de la manera en que el banco puede estratificar el perfil de riesgo de sus clientes (vea la leyenda y los niveles de riesgo). Debido a que el carácter del cliente es solamente una variable en el análisis de riesgos, este cuadro simplificado es tan sólo a modo de ejemplo. El cuadro también ejemplifica los métodos progresivos de debida diligencia y sistemas de supervisión de actividades sospechosas que los bancos podrían utilizar a medida que los niveles de riesgos aumenten. (Vea Métodos observados, abajo).



Leyenda: Tipos de clientes / Cuentas

1 Cuenta de cliente residente (DDA, ahorro, tiempo, CD)
2 Cuenta de cliente extranjero no residente (DDA, ahorro, tiempo, CD)
3 Negocios comerciales y franquicias pequeños
4 Creación de riqueza de consumidor (en el umbral correspondiente de acuerdo con el interés de riesgo del banco)
5 Inversionista extranjero no residente
6 Personas de alto valor neto (Banca privada)
7 Cuentas de varios niveles (administradores financieros, consejeros financieros, cuentas “empleadas para pagos”)
8 Compañías fantasmas y extraterritoriales

Apéndice L: Guía Sobre Calidad del SAR

La siguiente información se suministra a modo de guía. Consulte el manual *Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative* (Guía sobre la preparación de una descripción completa y suficiente en el informe de actividades sospechosas, Noviembre de 2003) de FinCEN. El texto original se puede encontrar en www.fincen.gov. Los bancos también deben consultar *Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting* (Sugerencias para analizar errores comunes encontrados en los informes de actividades sospechosas, 10 de Octubre de 2007), disponible en www.fincen.gov.

Con frecuencia los informes SAR han resultado decisivos para permitir a las autoridades de aplicación de la ley que inicien o profundicen importantes investigaciones de lavado de dinero o financiamiento del terrorismo y otros casos delictivos. La información proporcionada en los formularios SAR también permite que la FinCEN y las agencias bancarias federales identifiquen nuevos patrones y tendencias asociadas con delitos financieros. La información sobre estos patrones y tendencias es vital para las agencias de aplicación de la ley y proporciona valiosos aportes a las instituciones financieras.

Los bancos deben presentar informes SAR completos, suficientes y oportunos. Desafortunadamente, algunos bancos presentan formularios SAR con descripciones incompletas, incorrectas o desorganizadas que dificultan o directamente imposibilitan análisis más profundos. Algunos informes SAR se entregan con las descripciones en blanco. Debido a que la descripción del formulario SAR es la única parte con texto libre para resumir las actividades sospechosas, la sección de descripción es "fundamental". El detalle con el cual se redacte la descripción puede determinar si las autoridades de aplicación de la ley comprenderán cabalmente la conducta descripta y su posible carácter delictivo. Por lo tanto, la falta de una descripción adecuada de los factores que hacen que una transacción o actividad sea sospechosa menoscaba el propósito del SAR.

El formulario SAR deberá incluir toda información que esté a dispoción del banco que presenta el informe mediante el proceso de apertura de cuenta y las actividades de debida diligencia. En general, una descripción en el formulario SAR debe identificar los cinco elementos esenciales de información (quién, qué, cuándo, dónde y por qué) con respecto a la actividad sospechosa que se está informando. El método de operación (o cómo) también es importante y deberá incluirse en la descripción.

¿Quién está llevando a cabo la actividad sospechosa?

A pesar de que una sección del formulario SAR pide información específica sobre los sospechosos, se debe usar la descripción para dar mayores detalles sobre los sospechosos, incluso la profesión, el cargo o el puesto dentro del negocio, el carácter de su negocio (o sus negocios) y toda otra información y números de identificación relacionados con los sospechosos.

¿Qué instrumentos o mecanismos se utilizan para facilitar las transacciones sospechosas?

Una lista de instrumentos o mecanismos que podrían utilizarse en actividades sospechosas, incluye, entre otros, transferencias de fondos, cartas de crédito y otros instrumentos de

comercio internacional, cuentas corresponsales, casinos, fraccionamiento, compañías fantasma, bonos o pagarés, acciones, fondos mutuos, pólizas de seguro, cheques de viajero, giros bancarios, giros postales, tarjetas de crédito o de débito, tarjetas prepagadas y servicios comerciales de dinero digital. La descripción SAR debe enumerar los instrumentos o mecanismos utilizados en la actividad sospechosa que se informa. Si una descripción SAR resume el flujo de fondos, siempre debe incluir la fuente de los fondos (origen) y el uso, destino o beneficiario de los fondos.

¿Cuándo se llevó a cabo la actividad sospechosa?

Si la actividad se ha estado llevando a cabo a lo largo de un período de tiempo, indique la fecha en que se detectó por primera vez esa actividad sospechosa y la duración de esa actividad. Cuando sea posible, y a los efectos de hacer un mejor seguimiento del flujo de fondos, se deberán incluir fechas y montos específicos de las transacciones en la descripción, en lugar de indicar sólo un importe global.

¿Dónde se llevó a cabo la actividad sospechosa?

La descripción debe indicar si están involucradas en la actividad sospechosa varias oficinas de un mismo banco y debe consignar las direcciones correspondientes. La descripción también debe especificar si la actividad o las transacciones sospechosas involucran una jurisdicción extranjera.

¿Por qué el banco responsable de la presentación considera que la actividad es sospechosa?

En el formulario SAR se debe describir, con los mayores detalles posibles, por qué la actividad o transacción es poco habitual para el cliente, tomando en cuenta los tipos de productos y servicios que ofrece el sector del banco que presenta el informe, y hacer la correspondiente comparación con el carácter y las actividades previstas de clientes similares.

¿Cómo se llevó a cabo esa actividad sospechosa?

En la descripción se debe incluir el "modus operandi" o el método de operación del sujeto que está llevando a cabo la actividad sospechosa. Se debe describir de manera concisa, precisa y lógica de qué manera se ha llevado a cabo la transacción o el patrón de transacciones. Por ejemplo, si lo que aparenta ser un fraccionamiento de depósitos de moneda coincide con transferencias salientes de fondos de las cuentas, la descripción en el formulario SAR debe incluir información tanto sobre el fraccionamiento y las transferencias salientes (inclusive las fechas, los destinos, los importes, las cuentas, la frecuencia y los beneficiarios de las transferencias de fondos).

Los bancos no deben incluir ninguna documentación respaldatoria al presentar un formulario SAR ni tampoco utilizar los términos "ver adjunto" en el texto del SAR.

En el Centro de Cómputo de Instituciones de Detroit del IRS (anteriormente el Centro de Cómputos de Detroit), solamente se procesarán los formularios SAR recibidos que contengan información explícita y texto; por lo tanto, las tablas, hojas de cálculo u otro tipo de adjuntos no se incorporarán en el banco de datos de informes de BSA. Los bancos deben guardar la información respaldatoria en sus archivos durante cinco años para que la información esté disponible para las autoridades de aplicación de la ley cuando la soliciten.

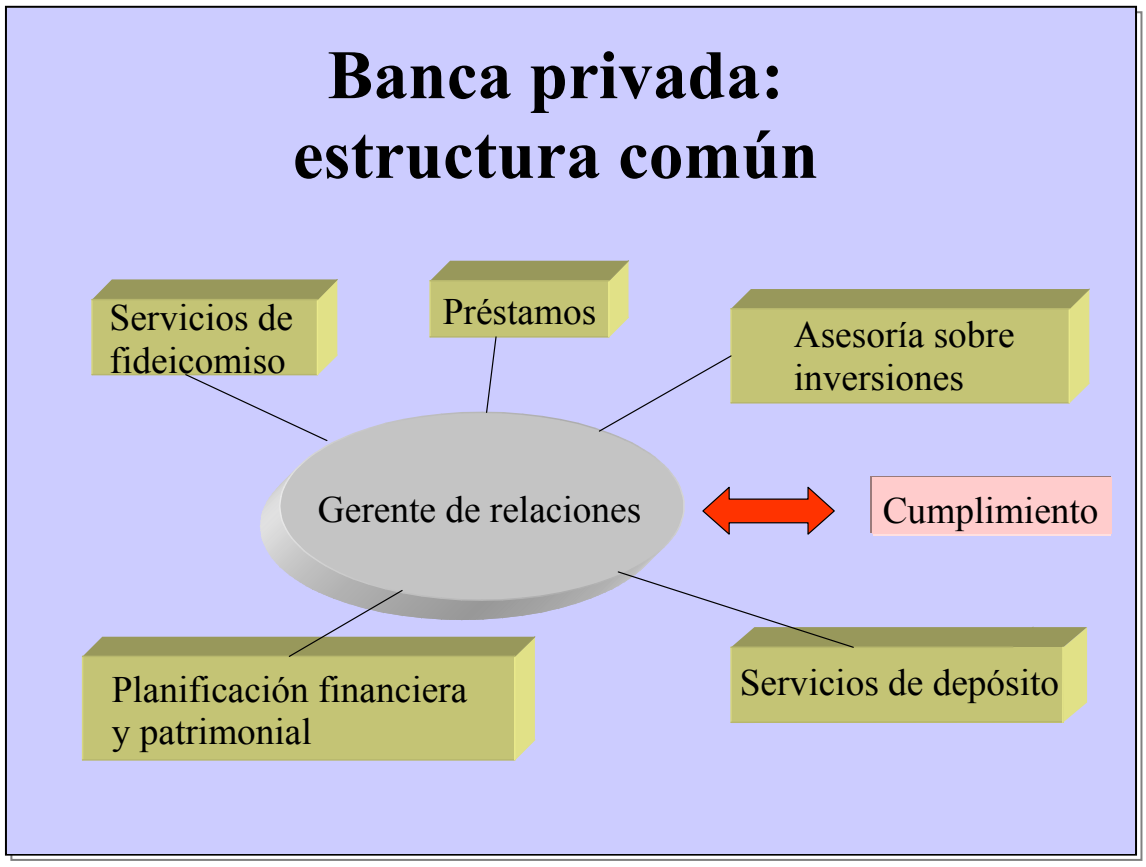
Apéndice M: Cuadro de Cantidad de Riesgos: Procedimientos de la OFAC

Los inspectores deberán usar el siguiente cuadro, cuando corresponda, al analizar el riesgo del banco de encontrar un problema relacionado con la OFAC.

Bajo	Moderado	Alto
Base de clientes estables y conocidos en un entorno localizado.	El tipo de clientela está cambiando debido a la apertura de nuevas sucursales, fusiones o adquisiciones en el mercado local.	Una importante base de clientes fluctuante, en un entorno internacional.
Pocos clientes de alto riesgo, que podrían incluir extranjeros no residentes (incluso cuentas con apoderados estadounidenses) y clientes comerciales extranjeros.	Una cantidad moderada de clientes de alto riesgo.	Una gran cantidad de clientes de alto riesgo.
No existen sucursales en el extranjero ni cuentas corresponsales con bancos extranjeros.	Sucursales en el extranjero o cuentas corresponsales con bancos extranjeros.	Sucursales en el extranjero o varias cuentas corresponsales con bancos extranjeros.
No se ofrecen servicios de banca electrónica (*e-banking*) o los productos disponibles son sólo a efectos informativos o no transaccionales.	El banco ofrece una limitada cantidad de productos y servicios de banca electrónica.	El banco ofrece una gran variedad de productos y servicios de banca electrónica (por ej. transferencias entre cuentas, pagos de facturas por banca electrónica o apertura de cuentas por Internet).
Limitada cantidad de transferencias de fondos de clientes, no clientes, limitada cantidad de transacciones de partes externas; sin transferencias de fondos del exterior.	Una moderada cantidad de transferencias de fondos, la mayoría de ellos para clientes. Posiblemente una pocas transferencias de fondos internacionales desde cuentas personales o comerciales.	Una gran cantidad de transferencias de fondos de clientes y no clientes, incluso transferencias de fondos internacionales.

Bajo	Moderado	Alto
No existen otros tipos de transacciones internacionales, tales como financiación de comercio internacional, transacciones ACH transnacionales y administración de deuda soberana.	Limitada cantidad de transacciones internacionales de otro tipo.	Una gran cantidad de otros tipos de transacciones internacionales.
No hay antecedentes de medidas tomadas por la OFAC. No hay evidencia de aparentes violaciones o circunstancias que podrían generar violaciones a las normas.	Una pequeña cantidad de medidas recientes (por ej., medidas de los últimos cinco años) por parte de la OFAC, incluso cartas de notificación, o sanciones monetarias civiles, con evidencia de que el banco se ocupó de estos temas y no existe el riesgo de que ocurran violaciones similares en el futuro.	Varias medidas recientes por parte de la OFAC, en las que el banco no se ocupó de estos temas, lo que indica que existe un riesgo mayor de que cometa violaciones similares en el futuro.

Apéndice N: Banca Privada: Estructura Común



Apéndice O: Herramientas del Inspector para las Pruebas de Transacciones

Informes de transacciones en efectivo e informes de actividades sospechosas

Si el banco no cuenta con informes de filtrado preestablecidos para la presentación de informes de transacciones en efectivo y la identificación de transacciones en efectivo sospechosas, el inspector deberá tener en cuenta la posibilidad de solicitar un informe personalizado. Por ejemplo, un informe puede generarse con los siguientes criterios: transacciones en efectivo de USD 7.000 o más (entrantes y salientes) durante el período precedente *(a ser determinado por el inspector)* antes de la fecha de la inspección. Según lo determine el inspector, se puede modificar el período de tiempo cubierto y las sumas de las transacciones. El informe también debe incluir:

- El número de archivo de información (CIF), si está disponible, o el número de Seguro Social (SSN)/número de identificación fiscal (TIN) del cliente.
- La fecha, la suma y el número de cuenta de cada transacción.
- El cajero y la sucursal u otra información de identificación correspondiente.

Estos datos se deben preparar en una hoja de cálculo electrónica o en un formato de base de datos para ordenar los datos con facilidad. Los datos se pueden ordenar siguiendo diferentes criterios (p. ej., por sucursal, cajero, número de SSN/TIN o CIF, si están disponibles). El análisis de esta información debe permitir que el inspector determine si los CTR y los SAR se han presentado de manera adecuada.

Supervisión de las transferencias de fondos

Si el banco no cuenta con informes de filtrado preestablecidos para la gestión de registros de transferencias de fondos y la identificación de transacciones sospechosas, el inspector deberá tener en cuenta la posibilidad de solicitar un informe personalizado. El inspector puede considerar la posibilidad de solicitar que el banco proporcione un informe generado por sus sistemas de transferencias de fondos que identifique todas las transferencias de fondos (entrantes y salientes) durante un período de tiempo determinado por el inspector. El informe también debe incluir:

- El nombre completo, el país de residencia, el SSN/TIN y la valoración de riesgos BSA/AML del cliente, si corresponde.
- La fecha, la suma, el tipo de transacción y el número de cuenta de cada transacción.
- El nombre, el país, la institución financiera y el número de cuenta del remitente.
- El nombre, el país, la institución financiera y el número de cuenta del beneficiario.

El banco debe proporcionar una lista de sus códigos internos para identificar en su totalidad el tipo de cuenta, la valoración de riesgos BSA/AML, el país, el tipo de transacción, el número del banco, el número de cuenta y cualquier otro código de los informes electrónicos. La lista se debe ordenar para identificar aquellas cuentas que no contienen suficiente información sobre el remitente o el beneficiario. La información faltante puede indicar deficiencias en la supervisión de las transferencias de fondos. Un gran volumen de transferencias o aquellas de mayor valor en dólares desde y hacia jurisdicciones de alto riesgo o que involucren partes que no acostumbran participar en esas transacciones pueden indicar la necesidad de un mayor escrutinio.

Aptitud de la información sobre cuentas de depósito y sobre cuentas de gestión de fideicomisos y activos

Esta prueba está diseñada para garantizar que el banco cumpla con las exigencias normativas del CIP y para comprobar la aptitud de las políticas, procedimientos y procesos de CDD del banco.

El inspector debe solicitar una lista electrónica (hoja de cálculo o base de datos) de todas las cuentas de depósito y cuentas de gestión de fideicomisos y de activos a partir de la fecha de la inspección. Los saldos deben ser conciliados con el libro mayor. El informe también debe incluir:

- El nombre completo, la fecha de nacimiento, la dirección, el país de residencia, el SSN/TIN y la valoración de riesgos BSA/AML del cliente, si corresponde.
- La fecha de apertura de cuenta.
- El saldo diario promedio (durante el período de control) y el saldo de la cuenta a partir de la fecha de la inspección.

El banco debe proporcionar una lista de sus códigos internos para identificar en su totalidad el tipo de cuenta, la valoración de riesgos BSA/AML, el país, el tipo de transacción, el número de sucursal, el número de cajero y cualquier otro código de los informes electrónicos. La lista se debe ordenar para identificar aquellas cuentas que no contienen suficiente información.

Pruebas de registros de envíos de moneda para detectar actividades poco habituales

Revise todos los registros de envíos de moneda del banco o una muestra de ellos para detectar anormalidades significativas o patrones poco habituales de actividades de envío de moneda. Los inspectores también deben tener en cuenta el control de los datos del Resumen de Depósitos (SOD, por sus siglas en inglés) de la FDIC para detectar tendencias poco habituales en el crecimiento de los depósitos de la sucursal.

Analice si los niveles de envío y la frecuencia de envío son adecuados en relación con los niveles de actividad prevista de la sucursal y el banco. Este análisis debe incluir las transacciones desde y hacia la bóveda central y las sucursales. La actividad poco habitual que requiere más

investigación puede incluir cambios significativos de billetes de baja denominación por billetes de alta denominación y solicitudes significativas de billetes de mayor denominación.

Extranjeros no residentes y ciudadanos extranjeros

Un método eficaz para identificar y revisar el nivel de extranjeros no residentes (NRA), ciudadanos extranjeros y corporaciones instaladas en el exterior que operan con el banco es obtener informes de MIS que no proporcionen TIN ni titulares de cuentas con números de identificación fiscal individual (ITIN). El informe debe incluir:

- El nombre completo, la fecha de nacimiento, la dirección, el país de residencia y el SSN/TIN del cliente.
- La fecha de apertura de cuenta.
- El saldo diario promedio y el saldo de la cuenta a partir de la fecha de la inspección.

Estos datos se deben preparar en una hoja de cálculo electrónica o en un formato de base de datos para ordenar los datos con facilidad. El banco debe proporcionar una lista de sus códigos internos para identificar en su totalidad la información de la hoja de cálculo. Esta información se puede utilizar para analizar si la cantidad de NRA y ciudadanos extranjeros plantea un mayor riesgo al banco determinando el saldo diario promedio acumulado, los tipos de cuentas y los países en los que el banco está expuesto.

Informes de flujo de fondos

Los inspectores pueden revisar esta información para identificar a los clientes con alta velocidad de flujo de fondos y aquellos cuya actividad es poco habitual. Un informe de velocidad de fondos refleja los débitos y créditos totales que fluyen a través de una cuenta en particular durante un período de tiempo específico (p. ej., 30 días). Los informes electrónicos deben incluir:

- Nombre del cliente.
- Número de cuenta.
- Fecha de la transacción.
- Suma de los pagos en dólares (débitos).
- Suma de los recibos en dólares (créditos).
- El saldo promedio de la cuenta.
- Tipo de cuenta.

Estos datos se deben preparar en una hoja de cálculo electrónica o en un formato de base de datos para ordenar los datos con facilidad. Este informe se puede utilizar para identificar las cuentas de clientes con flujo de fondos sustancial en relación con otras cuentas.

Apéndice P: Exigencias Respecto a la Conservación de Registros de la BSA

Este apéndice se proporciona en formato de lista resumen. Consulte los reglamentos de la FinCEN/Tesoro de Estados Unidos que se encuentran en 31 CFR 103 para conocer las exigencias sobre requisitos detallados y actuales respecto de la conservación de los registros. Estas exigencias de retención de registros BSA son independientes y adicionales a los requisitos de retención de registros conforme a otras leyes.

Conservación durante cinco años de los registros según se especifica a continuación

La BSA establece las exigencias en cuanto a la gestión de registros relacionadas con diversos tipos de registros, incluidos: las cuentas de clientes (p. ej., de préstamos, de depósito o fiduciarias), las exigencias en cuanto a la presentación de informes de la BSA y los registros que documentan el cumplimiento de un banco con la BSA. En general, la BSA exige que un banco conserve la mayoría de los registros durante al menos cinco años. Estos registros se pueden mantener en el formato original, copia o reproducción, o en microfilm o medios electrónicos, entre otros. No es obligatorio que un banco cuente con un sistema de registros diferente para cada una de las exigencias de la BSA; sin embargo, debe conservar todos los registros en un formato que permita acceder a ellos en un período de tiempo prudente.

Un banco debe conservar los registros relacionados con las transacciones abordadas a continuación durante cinco años. Sin embargo, como se indica más adelante, los registros relacionados con la identidad de un cliente del banco se deben mantener durante cinco años luego del cierre de la cuenta (p. ej., de préstamos, de depósito o fiduciaria). Además, según el caso (p. ej., debido a una Orden del Departamento del Tesoro de Estados Unidos o una investigación de las autoridades de aplicación de la ley), se le puede exigir o solicitar a un banco que mantenga algunos de estos registros durante períodos más prolongados.

Concesión de crédito que supera los USD 10.000 (sin estar garantizado con bienes inmuebles)

Este registro debe incluir:

- Nombre del solicitante del préstamo.
- Dirección del solicitante del préstamo.
- Suma del crédito concedido.
- Carácter o propósito del préstamo.
- Fecha del préstamo.

Transacciones internacionales que superan los USD 10.000

Un registro de cualquier solicitud realizada o instrucciones recibidas o dadas con respecto a una transferencia de efectivo u otros instrumentos monetarios, cheques, fondos, inversiones en valores o crédito mayor a USD 10.000 desde o hacia cualquier persona, cuenta o lugar fuera de Estados Unidos.

Tarjetas de firma

Un registro de cada concesión de autoridad de firma sobre cada cuenta de depósito.

Estados de cuenta

Un estado, una tarjeta de mayor u otro registro de cada cuenta de depósito que muestre cada transacción hecha en dicha cuenta o con respecto a la misma.

Cheques que superan los USD 100

Cada cheque, giro o giro postal librado contra el banco o emitido y pagadero por éste que supere los USD 100.

Depósitos que superan los USD 100

Cada comprobante de depósito o ticket de crédito que refleje una transacción que supere los USD 100 o el registro equivalente para depósito directo u otras transacciones de depósito de transferencias de fondos. El comprobante o ticket debe registrar la suma de cualquier moneda involucrada.

Registros para reconstruir cuentas corrientes

Los registros preparados o recibidos por el banco en el transcurso normal de los negocios, que se necesitarían para reconstruir una cuenta de transacciones y para rastrear un cheque que supere los USD 100 depositado en una cuenta corriente a través de su sistema de procesamiento nacional o para proporcionar una descripción de un cheque depositado que supere los USD 100.

Certificados de depósito presentados o comprados

Este registro debe incluir:

- Nombre del cliente (comprador o presentante).
- Dirección del cliente.
- Número de identificación fiscal (TIN) del cliente.
- Descripción del certificado de depósito.
- Anotación que indique el método de pago en caso de compra.
- Fecha de la transacción.

Compra de instrumentos monetarios de USD 3.000 o más

Un banco debe mantener un registro de cada cheque o giro bancario, cheque de caja, giro postal o cheque de viajero de USD 3.000 o más en efectivo.

Si el comprador es titular de una cuenta de depósito en el banco, este registro debe incluir:

- Nombre del comprador.
- Fecha de la compra
- Tipo o tipos de instrumentos comprados.
- Monto en dólares de cada instrumento o los instrumentos comprados.
- Número o números de serie del instrumento o los instrumentos comprados.

Si el comprador no es titular de una cuenta de depósito en el banco, este registro debe incluir:

- Nombre del comprador.
- Direcciones de los compradores.
- Número de seguro social del comprador o número de identificación de extranjero.
- Fecha de nacimiento del comprador.
- Fecha de la compra
- Tipo o tipos de instrumentos comprados.
- Monto en dólares de cada instrumento o los instrumentos comprados.
- Número o números de serie del instrumento o los instrumentos comprados.
- Descripción del documento o método utilizado para verificar el nombre y la dirección del comprador (p. ej., estado que expidió la licencia de conducir y número de la licencia).

Transferencias de fondos de USD 3.000 o más

Las exigencias de la BSA en cuanto a la gestión de registros del banco con respecto a las transferencias de fondos varían según el papel del banco en relación con las transferencias de fondos.

Banco que actúa como banco del remitente. Por cada orden de pago que un banco acepta como banco del remitente, el banco debe obtener y conservar un registro de la siguiente información:

- Nombre y dirección del remitente.
- Monto de la orden de pago.

- Fecha de otorgamiento de la orden de pago.
- Cualquier instrucción de pago que se reciba del remitente con la orden de pago.
- Identificación del banco del beneficiario.
- De los siguientes elementos, los que se reciban con la orden de pago:
  - Nombre y dirección del beneficiario.
  - Número de cuenta del beneficiario.
  - Cualquier otra identificación específica del beneficiario.
- Por cada orden de pago que un banco acepta para un remitente que no es un cliente reconocido del banco, además de la información enumerada anteriormente, el banco debe obtener información adicional según lo exige 31 CFR 103.33(e)(2).

Banco que actúa como banco intermediario o banco del beneficiario. El banco debe conservar un registro de cada orden de pago en la que acepte participar como banco intermediario o banco del beneficiario.

- Por cada orden de pago que un banco acepta para un beneficiario que no es un cliente reconocido del banco, éste debe obtener información adicional según lo exige 31 CFR 103.33(e)(3).

Excepciones. La BSA no exige que un banco mantenga registros para los siguientes tipos de transferencias de fondos: (1) transferencias de fondos en las que el remitente y el beneficiario sean la misma persona y en las que el banco del remitente y el banco del beneficiario sean la misma entidad; y (2) transferencias de fondos en las que el remitente y el beneficiario sean cualquiera de los siguientes:

- Un banco.
- Una subsidiaria nacional de entera propiedad de un banco constituido en Estados Unidos.
- Un agente o comisionista de valores.
- Una subsidiaria nacional de entera propiedad de un agente o comisionista de valores.
- Estados Unidos.
- Un gobierno local o estatal.
- Una agencia o dependencia del gobierno federal, estatal o local.

Número de identificación fiscal

Un registro del TIN de *cualquier* cliente que abra una cuenta. En el caso de las cuentas conjuntas, se debe mantener información sobre una persona con interés financiero. (Si la persona es un extranjero no residente (NRA), registre el número de pasaporte o una

descripción de algún documento expedido por el otro gobierno utilizado para verificar la identidad). Esta información se debe registrar dentro de los 30 días a partir de la fecha en la que se efectúa la transacción. En caso de que un banco no pueda obtener la información, debe mantener una lista que incluya los nombres, las direcciones y los números de cuenta de aquellos miembros respecto de los cuales no haya podido obtener la información.

Excepciones. No es necesario que un banco mantenga un TIN para las cuentas o transacciones con los siguientes:

- Agencias o dependencias de gobiernos federales, estatales, locales o extranjeros.
- Jueces, funcionarios públicos o actuarios de tribunales de registro como custodios de fondos en disputa o bajo el control del tribunal.
- Ciertos extranjeros según se especifica en 31 CFR 103.34(a)(3)(iii-vi).
- Ciertas organizaciones exentas de impuestos y unidades de organizaciones exentas de impuestos (31 CFR 103.34(a)(3)(vii)).
- Una persona menor de 18 años con respecto a una cuenta abierta como parte de un programa de ahorro para la universidad, siempre que el dividendo anual sea menor a USD 10.
- Una persona que abra una cuenta de ahorro especial para financiar los gastos navideños (en inglés, *Christmas club*) o las vacaciones (en inglés, *vacation club*) y programas de ahorro equivalentes con pagos periódicos, siempre que el dividendo anual sea menor a USD 10.
- NRA que no participen en un comercio o negocio en Estados Unidos.

Informe de actividades sospechosas y documentación respaldatoria

Un banco debe mantener un registro de cualquier SAR presentado y el registro original o comercial equivalente de cualquier documentación respaldatoria durante un período de cinco años a partir de la fecha de presentación.

Informe de transacciones en efectivo

Un banco debe conservar un registro de todos los Informes de transacciones en efectivo (CTR) durante un período de cinco años a partir de la fecha de presentación.

Designación de persona exenta

Un banco debe mantener un registro de todas las designaciones de personas exentas de la presentación de CTR en el Tesoro (es decir, el Formulario 110 de la FinCEN) durante un período de cinco años a partir de la fecha de designación.

Programa de identificación de clientes

Un banco debe mantener un registro de toda la información que obtiene bajo los procedimientos de implementación de su CIP. Como mínimo, estos registros deben incluir lo siguiente:

- Toda la información de identificación del cliente (p. ej., nombre, fecha de nacimiento, dirección y TIN).
- Una descripción del documento del que el banco se valió para verificar la identidad del cliente.
- Una descripción de los métodos no documentales y los resultados de cualquier medida que el banco haya tomado para verificar la identidad del cliente.
- Una descripción de la resolución del banco sobre cualquier discrepancia sustantiva que se haya descubierto al verificar la información de identificación obtenida.

Un banco debe conservar la información de identificación del cliente durante un período de cinco años luego de la fecha en que se cerró la cuenta, o en el caso de las cuentas de tarjetas de crédito, cinco años luego de que la cuenta se haya cerrado o haya permanecido inactiva.

Un banco debe conservar la información de la que se valió, los métodos utilizados para verificar la identidad y la resolución de las discrepancias durante un período de cinco años luego de que se haya asentado el registro.

Tal como se indicó, las exigencias de gestión de registros son independientes y adicionales a los requisitos para presentar y conservar informes impuestos por otras leyes. Para conocer el significado de los términos de la BSA, consulte 31 CFR 103.11.

Apéndice Q: Siglas

Sigla o abreviatura	Nombre complete
ACH	Automated Clearing House (Compensación automática)
AML	Anti-Money Laundering (Antilavado de dinero)
APO	Army Post Office (Apartado postal del Ejército)
ATM	Automated Teller Machine (Cajero automático)
APT	Asset Protection Trust (Plan de protección patrimonial en el extranjero)
BCBS	Basel Committee on Banking Supervision (Comité de Supervisión Bancaria de Basilea)
BHC	Bank Holding Company (Sociedad de control de bancos)
BIS	Bank for International Settlements (Banco de Pagos Internacionales)
BSA	Bank Secrecy Act (Ley de Secreto Bancario)
CDD	Customer Due Dilligence (Debida diligencia de los clientes)
CFR	Code of Federal Regulations (Código de Reglamentos Federales)
CHIPS	Clearing House Interbank Payments System (Sistema de Pagos Interbancarios por Cámara de Compensación)
CIF	Customer Information File (Archivo de información del cliente)
CIP	Customer Identification Program (Programa de identificación de clientes)
CMIR	Reporto f International Transportation of Currency or Monetary Instruments (Informe sobre el transporte internacional de moneda o instrumentos monetarios)
CTR	Currency Transaction Report (Informe de transacciones en efectivo)
DCN	Document Control Number (Número de control del documento)

E-banking	Electronic Banking (Banca electrónica)
E-cash	Electronic Cash (Efectivo electrónico)
EDD	Enhanced Due Diligence (Debida diligencia especial)
EFT	Electronic Funds Transfer (Transferencia electrónica de fondos)
EIC	Examiner in charge (Inspector a cargo).
EIN	Employer Identification Number (Número de identificación del empleador)
EPN	Electronic Payments Network (Red de pago electrónico)
ERISA	Employee Retirement Income Security Act (Ley de Seguridad de los Ingresos para el Retiro de los Empleados) de 1974
FAQ	Frequently Asked Questions (Preguntas frecuentes)
FATF	Financial Action Task Force on Money Laundering (Grupo de Acción Financiera en Contra del Lavado de Dinero)
FBAR	Report of Foreign Bank and Financial Accounts (Informe de cuentas bancarias y financieras extranjeras)
FBI	Federal Bureau of Investigation (Oficina Federal de Investigaciones)
Ley FDI	Federal Deposit Insurance Act (Ley Federal de Seguro de Depósitos)
FDIC	Federal Deposit Insurance Corporation (Corporación Federal de Seguro de Depósitos)
Fedwire	Fedwire Funds Service (Servicios de Fondos Fedwire)
FFIEC	Federal Financial Institutions Examination Council (Consejo Federal de Inspección de Instituciones Financieras)
FGO	Foreign Gateway Operator (Operador de puerta de enlace extranjera)
FIL	Financial Institution Letters (Cartas de instituciones financieras)
FinCEN	Financial Crimes Enforcement Network (Red de Lucha contra Delitos Financieros)
FPO	Fleet Post Office (Apartado postal de la Marina)

GAO	U.S. Government Accountability Office (Oficina de Contabilidad del Gobierno de los Estados Unidos)
GO	Gateway Operator (Operador de puerta de enlace)
HIDTA	High Intensity Drug Trafficking Area (Zona de alta densidad de narcotráfico)
HIFCA	High Intensity Financial Crime Area (Zona de alta densidad de delitos financieros)
IAIS	International Association of Insurance Supervisors (Asociación Internacional de Supervisores de Seguros)
IAT	International Automated Clearing House Transaction (Transacciones internacionales de compensación automatizada)
IBC	International Business Corporation (Corporación comercial internacional)
IMF	International Monetary Fund (Fondo Monetario Internacional)
INCSR	International Narcotics Control Strategy Report (Informe Estratégico para el Control Internacional de Narcóticos)
IOLTA	Interest on Lawyers' Trust Accounts (Cuentas fiduciarias de abogados con rendimiento de interés)
IP	Internet Protocol (Protocolo de Internet)
IRA	Individual Retirement Account (Cuenta individual de retiro)
IRS	Internal Revenue Service (Servicio de Impuestos Internos)
ISO	Independent Sales Organization (Organización de ventas independiente)
ITIN	Individual Taxpayer Identification Number (Número de identificación fiscal individual)
IVTS	Informal Value Transfer System (Sistema informal de transferencia de valor)
KYC	Know Your Customer (Conozca a su cliente)
LCU	Letters to Credit Unions (Cartas a las Cooperativas de Crédito)

MIS	Management Information Systems (Sistemas para la información de gestión)
MLSA	Money Laundering Suppression Act (Ley de Supresión del Lavado de Dinero) de 1994
MLTA	U.S. Money Laundering Threat Assessment (El lavado de dinero y la evaluación de amenazas en Estados Unidos)
MSB	Money Services Business (Negocios de servicios monetarios)
NACHA	The Electronic Payments Association (Asociación de Pagos Electrónicos)
NAICS	North American Industry Classification System (Sistema de clasificación industrial de Norteamérica)
NASD	National Association of Securities Dealers (Asociación Nacional de Operadores de Valores o Bolsa)
NASDAQ	National Association of Securities Dealers Automated Quotation Systems (Sistemas de cotización automática de la Asociación Nacional de Operadores de Valores o Bolsa)
NBFI	Nonbank Financial Institutions (Instituciones financieras no bancarias)
NCCT	Noncooperative Countries and Territories (Países o territorios que no cooperan)
NCUA	National Credit Union Administration (Administración Nacional de Cooperativas de Crédito)
NDIP	Nondeposit Investment Products (Productos de inversión que no son para depositar)
NGO	Nongovernmental Organization (Organización no gubernamental)
NIS	Nominee Incorporation Services (Servicios de constitución de compañías nominadas)
NRA	Nonresident Alien (Extranjeros no residentes)
NSF	Nonsufficient Funds (Fondos insuficientes)
NSL	National Security Letter (Carta de Seguridad Nacional)

NYCH	New York Clearing House Association, L.L.C. (Asociación de Cámaras de Compensación de Nueva York, L.L.C.)
OCC	Office of the Comptroller of the Currency (Oficina del Interventor Monetario)
ONDCP	The Office of National Drug Control Policy (El Gabinete de Política Nacional de Control de las Drogas)
ODFI	Originating Depository Financial Institution (Institución Financiera de Depósito de Origen)
OFAC	Office of Foreign Assets Control (Oficina de Control de Activos Extranjeros)
OFC	Offshore Financial Center (Centro financiero instalado en el exterior)
OTS	Office of Thrift Supervision (Oficina de Supervisión de Instituciones de Ahorro)
PEP	Politically Exposed Person (Personalidades sujetas a exposición política)
PIC	Private Investment Company (Compañía de inversión privada)
POS	Point-of-Sale (Punto de venta)
PTA	Payable Through Account (Cuenta empleada para pagos)
PUPID	Payable Upon Proper Identification (Transacciones pagaderas mediante presentación de identificación apropiada)
RA	Regulatory Alerts (Alertas normativas)
RCC	Remotely Created Check (Cheque creado remotamente)
RDC	Remote Deposit Capture (Captura de depósitos remotos)
RDFI	Receiving Depository Financial Institution (Institución Financiera de Depósito Receptora)
ROE	Report of Examination (Informe de inspección)
SAR	Suspicious Activity Report (Informe de actividades sospechosas)

SDN	Specially Designated Nationals or Blocked Persons (Ciudadanos especialmente designados o personas bloqueadas)
SEC	U.S. Securities and Exchange Commission (Comisión de Valores y Bolsa de EE. UU.)
SOD	Summary of Deposits (Resumen de depósitos)
SSN	Social Security Number (Número de Seguro Social)
SWIFT	Society for Worldwide Interbank Financial Telecommunication (Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales)
TD F	Treasury Department Form (Formulario del Departamento del Tesoro)
TIN	Taxpayer Identification Number (Número de identificación fiscal)
TPSP	Third-Party Service Provider (Prestador de servicios externos)
UBPR	Uniform Bank Performance Report (Informe uniforme de desempeño bancario)
U.S. Treasury	U.S. Department of the Treasury (Departamento del Tesoro de Estados Unidos)
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Ley para unir y fortalecer a Norteamérica mediante la provisión de herramientas adecuadas rqueridas para interceptar y obstruir el terrorismo de 2001)
USC	United States Code (Código de Estados Unidos)
Web CBRS	Web Currency and Banking Retrieval System (Sistema en línea de recuperación de información de moneda y banca)

Apéndice R: Guía sobre Cumplimiento

Informe Entre Agencias sobre el Cumplimiento de las Exigencias BSA/ AML[272]

Esta declaración conjunta entre agencias, que emite la Junta de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguro de Depósitos, la Oficina del Interventor Monetario, la Oficina de Supervisión de Instituciones de Ahorro y la Administración Nacional de Cooperativas de Crédito[273] enuncia la política de las agencias con respecto a las circunstancias en las cuales una agencia emitirá una orden de cese de determinadas prácticas comerciales para ocuparse de la falta de cumplimiento de ciertos requisitos de la Ley de Secreto Bancario (BSA)/ Contra Lavado de Dinero ("BSA/AML"),[274] en especial en vista de disposiciones específicas de cumplimiento de BSA/AML de la sección 8(s) de la Ley Federal de Seguro de Depósitos ("Ley FDI") y la sección 206(q) de la Ley Federal de Cooperativas de Crédito ("FCUA").

Las exigencias del programa de cumplimiento BSA/AML

Conforme a la sección 8(s) de la FDIA y la sección 206(q) de la FCUA, se exige que las agencias emitan reglamentos que insten a las instituciones de depósito aseguradas a establecer y mantener procedimientos razonablemente diseñados para garantizar y supervisar el cumplimiento de las exigencias de la BSA ("Programa de Cumplimiento BSA"). Las secciones 8(s) y 206(q) también exigen que las inspecciones que realice cada agencia de una institución de depósito asegurada revisen el Programa de Cumplimiento BSA y que sus informes de inspección describan cualquier problema con dicho programa. Por último, las secciones 8(s) y 206(q) determinan que si una institución de depósito asegurada no ha establecido ni mantenido un Programa deC cumplimiento BSA o no ha corregido los problemas con el Programa de Cumplimiento BSA que fueron informados a la institución por la agencia correspondiente, esta última emitirá una orden que exija el cese de la actividad a la institución. Tal como lo requieren las secciones 8(s) y 206(q), cada una de las agencias ha emitido normativas que requieren que toda institución que supervisan o aseguran establezca y mantenga un Programa de Cumplimiento BSA. Cada una de estas

[272] La intención de esta declaración es dar lineamientos generales de la política. La intención no es forzar o evitar una acción de aplicación de la ley u otro tipo de acciones de supervisión que fueran necesarias en una situación fáctica específica.

[273] En forma colectiva, "las agencias" y en forma individual, "la agencia".

[274] Esta declaración no se ocupa de la evaluación de penalidades civiles en dinero por violaciones a la BSA o los reglamentos que la implementan La FinCen tiene autoridad para analizar sanciones conforme a la BSA. De la misma manera, las agencias también tiene la misma autoridad conforme a las leyes de supervisión general. 12 USC 1818(i)(2), 1786(k)(2).

[275] 12 USC 1818(s) y 12 USC 1786 (q).

normativas impone en gran medida las mismas exigencias.[276] Particularmente, conforme a las reglamentaciones de cada agencia, un Programa de Cumplimiento BSA debe contar con los siguientes elementos como mínimo:

- Un sistema de controles internos para garantizar el constante cumplimiento con la BSA.
- Pruebas independientes de cumplimiento de BSA/AML.
- Un individuo o individuos designados que estén a cargo de la coordinación y supervisión del cumplimiento de BSA/AML.
- Capacitación del personal correspondiente.

Además, el Programa de Cumplimiento BSA debe incluir un CIP con procedimientos basados en riesgos que permitan que la institución tenga una convicción razonable de que conoce la verdadera identidad del cliente.[277]

Comunicación de preocupaciones de supervisión sobre los Programas de Cumplimiento BSA.

Cuando una agencia identifica preocupaciones de supervisión relacionadas con el Programa de Cumplimento BSA de una organización bancaria o cooperativa de crédito durante una inspección o de otra manera, puede comunicar estas preocupaciones de diferentes formas. El método particular de comunicación utilizado generalmente depende de la gravedad de las preocupaciones. Estos métodos incluyen:

- Diálogos informales de los inspectorescon la gerencia de la institución durante el proceso de inspección.
- Diálogos formales de los inspectores con la junta directiva como parte del proceso de inspección o con posterioridad a éste.
- Cartas de supervisión y otras comunicaciones escritas de los inspectores o de la agencia a la gerencia de una institución.

---

[276] 12 CFR 21.21 (OCC); 208.63 (Junta de Gobernadores); 326.8(c) (FDIC); 563.177 (OTS); 748.2 (NCUA). Las disposiciones de la sección 8(s) también se aplican a ciertas organizaciones bancarias que no son instituciones de depósito aseguradas. 12 USC 1818(b)(3), (b)(4). Las reglamentaciones de la OCC también se aplican a las sucursales federales y agencias de bancos extranjeros. 12 USC 3102(b); 12 CFR 28.13. Las reglamentaciones de la Reserva Federal también se aplican a corporaciones que se rigen por la Ley de Organizaciones Bancarias Extranjeras (Edge Act) y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal y a sucursales, agencias y otras oficinas de organizaciones bancarias extranjeras. 12 CFR 211.5, 211.24. También se considera que los Programas de Cumplimiento BSA que cumplen con estas reglamentaciones de las agencias cumplen con las reglamentaciones del Tesoro emitidas conforme a la BSA, que exige por separado que las instituciones financieras establezcan programas AML. Consulte 31 CFR 103.120(b); 31 USC 5318(h).

[277] 12 CFR 21.21(b)(2) (OCC); 208.63(b)(2), 211.5(m)(2), 211.24(j)(2), (Junta de Gobernadores); 326.8(b)(2) (FDIC); 563.177(b)(2) (OTS); 748.2(b)(2) (NCUA); 31 CFR 103.121.

- Un resultado que está incluido en el informe de inspección o en otra comunicación formal de una agencia a la junta directiva de una institución para indicar deficiencias o puntos débiles en el Programa de Cumplimiento BSA.

- Un resultado que está incluido en el informe de inspección o en otra comunicación formal de una agencia a la junta directiva de una institución con respecto a una violación de una exigencia normativa de implementación y mantenimiento de un Programa de Cumplimiento BSA razonablemente diseñado.

Tal como se explica seguidamente, para que se trate de un "problema" con el Programa de Cumplimiento BSA que pueda redundar en una orden de que se desista de esa práctica conforme a las secciones 8(s) o 206(q) si no fuera corregido por la institución, se deben identificar las deficiencias en el Programa de Cumplimiento BSA en un informe de inspección o en otro tipo de de documento por escrito ya que se requiere una comunicación a la junta directiva o a la alta gerencia de la institución con respecto a los temas que deben corregirse. Sin embargo, otros problemas o sugerencias para mejorar pueden comunicarse a través de otros medios.

Medidas coercitivas por incumplimiento del Programa de Cumplimiento BSA.

De conformidad con las secciones 8(s)(3) y 206(q)(3), la agencia correspondiente emitirá una orden para que la organización bancaria o la cooperativa de crédito desista de esa práctica de incumplimiento de las normativas del Programa de Cumplimiento BSA en las siguientes circunstancias, a partir de una cuidadosa revisión de los hechos y circunstancias relevantes.

No establecer ni mantener un Programa de Cumplimiento BSA razonablemente diseñado. La agencia correspondiente emitirá una orden para que se desista de una práctica que constituye una violación a las exigencias de las secciones 8(s) y 206(q) de establecer y mantener un Programa BSA razonablemente diseñado donde la institución:

- no cumpla con la exigencia de contar con un Programa de Cumplimiento BSA por escrito, incluso un CIP que abarque de manera adecuada los elementos requeridos en el programa (o sea, controles internos, pruebas independientes, personal de cumplimiento designado y capacitación), o bien

- no cumpla con la implementación de un Programa de Cumplimiento BSA que abarque de manera adecuada los elementos requeridos del Programa (las declaraciones de políticas emitidas por la institución por sí solas no son suficientes; el programa implementado debe ser coherente con las políticas, los procedimientos, y los procesos escritos de la organización bancaria), o bien

- presente defectos en uno o más de los elementos del Programa de Cumplimiento BSA que indiquen que el Programa de Cumplimiento escrito o su implementación no son efectivos, por ejemplo, si las deficiencias están asociadas con otros factores agravantes tales como (i) una actividad altamente sospechosa que crea un importante potencial de riesgos de lavado de dinero o financiamiento del terrorismo, (ii) patrones de fraccionamiento para evadir exigencias de informe, (iii) importante complicidad interna

o (iv) repetidos incumplimientos en la presentación de informes CTR, SAR, o de otros informes requeridos por BSA.[278]

Por ejemplo, una institución que cuenta con procedimientos para brindar capacitación BSA/AML al personal correspondiente, pruebas independientes y un funcionario de cumplimiento de la BSA/AML designado estará sujeta, de todas maneras, a una orden de que se desista de ciertas prácticas si su sistema de controles internos (por ej., debida diligencia de los clientes, procedimientos de supervisión de actividades sospechosas o una evaluación de riesgos adecuada) falla con respecto a un área de mayores riesgos o a varios rubros de actividad comercial que afectan considerablemente el cumplimiento general de la BSA de la institución. Asimismo, se requeriría una orden de desistir de una actividad si, por ejemplo, la institución presentara deficiencias en el elemento obligatorio de pruebas independientes del Programa y dichas deficiencias estuvieran acompañadas de evidencia de una actividad muy sospechosa que creara una importante posibilidad de que existiera lavado de dinero o financiación del terrorismo no informados en la institución. Sin embargo, otros tipos de deficiencias en el Programa de Cumplimiento BSA de una institución o en la implementación de uno o más de los elementos requeridos del Programa no necesariamente redundarán en una orden de desistir de una práctica, excepto en el caso de que las deficiencias fueran tan graves que hicieran que el Programa resulte ineficiente al observarlo en su totalidad. Por ejemplo, una institución que tiene deficiencias en sus procedimientos de capacitación en BSA/AML del personal adecuado, pero cuenta con controles eficientes, pruebas independientes y un funcionario de cumplimiento de BSA/AML designado, podrá estar sujeta a las críticas del inspector y/o a medidas de supervisión que no sean una orden de que se desista de una práctica, a menos que las deficiencias del programa de capacitación, en vista de todas las circunstancias relevantes, fueran tan graves que se descubriera que el Programa de la organización, tomado en su totalidad, fuera ineficiente.

Para determinar si una organización no ha implementado un Programa de Cumplimiento BSA, una agencia también considerará la aplicación del Programa en todos los rubros comerciales y actividades de esa organización. En el caso de instituciones con varios rubros de actividad comercial, se deberán evaluar las deficiencias que afectan solamente a algunos rubros o actividades para determinar si son tan graves o significativas en su alcance que podrían generar la conclusión de que la institución no ha implementado un programa general eficiente.

Falta de corrección de un problema informado anteriormente con el Programa de Cumplimiento BSA. La existencia de antecedentes de deficiencias en el Programa de Cumplimiento BSA de una institución en una diversidad de áreas diferentes, o en las mismas áreas generales, podría redundar en una orden de que se desista de esa práctica. De conformidad con las secciones 8(s) y 206(q), y sobre la base de una cuidadosa revisión de los hechos y circunstancias relevantes, la agencia emitirá una orden de que se desista de la práctica cuando una institución no corrija un problema con el cumplimiento de BSA/AML

[278] De ninguna manera estos ejemplos limitan la capacidad de la agencia de iniciar acciones de aplicación de la ley cuando la falta de un Programa de Cumplimiento BSA o de su implementación se vean demostradas por otras deficiencias.

que se haya identificado en el proceso de supervisión. Sin embargo, a los efectos de que se considere un "problema" dentro del significado de las secciones 8(s)(3)(B) y 206(q)(3)(B), una deficiencia informada a la institución, por lo general, debe involucrar un defecto grave en uno o más de los componentes exigidos del Programa de Cumplimiento BSA de la institución o su respectiva implementación que haya sido identificado en un informe de inspección u otro tipo de comunicación de supervisión por escrito y que requiera ser informado a la junta directiva o a la alta gerencia de una institución como un problema que debe ser corregido. Por ejemplo, la falta de medidas en respuesta a una crítica expresa en un informe de inspección con respecto a la falta de nombramiento de un funcionario de cumplimiento idóneo se consideraría un problema no corregido que podría redundar en una orden de desistir de esa práctica.

Por lo general, una agencia no emitirá una orden de que se cese una práctica conforme a las secciones 8(s) o 206(q) por no corregir un problema con el Programa de Cumplimiento BSA, excepto en el caso de que las deficiencias que haya detectado posteriormente la Agencia sean esencialmente las mismas que se hayan informado anteriormente a la institución. Por ejemplo, si una agencia nota en un informe de inspección que el programa de capacitación de una institución no era adecuado por estar desactualizado (por ejemplo, porque no reflejaba las modificaciones de la ley) y la próxima inspección del programa de capacitación detecta que el programa está debidamente actualizado, pero se descubren fallas en los controles internos del Programa BSA/AML, la agencia podría determinar que no emitirá una orden de que se desista de esa práctica conforme a las secciones 8(s) o 206(q) debido a la falta de corrección de los problemas informados anteriormente y se considerará toda la gama de respuestas potenciales de supervisión. Asimismo, si una institución se cita en el informe de inspección descripto anteriormente por no designar a un funcionario de cumplimiento BSA idóneo, y para la próxima inspección la institución ha designado a una persona idónea para que asuma esa responsabilidad, pero los inspectores recomiendan capacitación adicional para esa persona, una agencia podrá determinar que no se emitirá una orden de que se desista de esa práctica conforme a las secciones 8(s) o 206(q) únicamente debido a esa deficiencia. Las declaraciones de un informe de inspección por escrito o de otro tipo de comunicación de supervisión donde se identifiquen problemas de poca gravedad, o donde se sugieran aspectos para mejorar que el informe de inspección no identifique como algo que deba ser comunicado a la junta directiva o a la alta gerencia como temas que deben ser corregidos, no se considerarán "problemas" a los efectos de las secciones 8(s) y 206(q).

Las agencias reconocen que hay ciertos tipos de problemas con el Programa de Cumplimiento BSA de una institución que no es posible corregir totalmente antes de la próxima inspección, por ejemplo, medidas correctivas que involucran adoptar o actualizar sistemas de computación. En estos tipos de situaciones, no es necesaria una orden de que se desista de esa práctica, siempre y cuando la agencia determine que la institución ha hecho un progreso sustancial para corregir el problema en el momento de la inspección inmediatamente posterior a la inspección en la que se identificó el problema inicialmente y se informó a la institución.

Otras medidas de aplicación de la ley respecto a deficiencias del Programa de Cumplimiento BSA. Tal como se enunció anteriormente, además de las situaciones que se

describen en esta declaración en las que la agencia emitirá una orden de que se desista de esa práctica por una violación de las normas del Programa de Cumplimiento BSA o por la falta de corrección de un "problema" que había sido informado anteriormente con respecto al Programa, una agencia también podrá emitir una orden de que se desista de una práctica o podrá firmar un acuerdo formal por escrito o tomar una medida informal de aplicación de la ley contra una institución por otros tipos de preocupaciones con respecto al Programa BSA/AML. En estas situaciones, y según los hechos particulares involucrados, una agencia podrá implementar medidas de aplicación de la ley sobre la base de prácticas inseguras o cuestionables o violaciones de la ley, incluso de la BSA. El formato de la medida de aplicación de la ley en un caso en particular dependerá de la gravedad de la falta de cumplimiento, la debilidad, o las deficiencias, la capacidad y la cooperación de la gerencia de la institución y de la confianza que pueda tener la agencia en que la institución tomará medidas correctivas apropiadas y oportunas.

Las exigencias con respecto a la conservación y presentación de informes de la BSA.

Exigencias para los informes de actividades sospechosas. Conforme a las normas de las agencias y del Departamento del Tesoro, las organizaciones sujetas a la supervisión de las agencias deben presentar un informe SAR cuando detecten ciertas violaciones penales o transacciones sospechosas de las que se sospeche o tenga conocimiento.[279] Los informes sobre actividades sospechosas constituyen la base del sistema de informes de BSA y son críticos para la capacidad de Estados Unidos de utilizar la información financiera para combatir el lavado de dinero, el financiamiento del terrorismo y otros delitos financieros. Las normas requieren que las organizaciones bancarias y las cooperativas de crédito presenten informes SAR con respecto a los siguientes tipos de actividades generales:

- Violaciones penales de las que se sospeche o tenga conocimiento que involucren actividad interna con cualquier importe.
- Violaciones penales de las que se sospeche o tenga conocimiento por un monto acumulado de USD 5.000 o más, cuando sea posible identificar a un sospechoso.
- Violaciones penales de las que se sospeche o tenga conocimiento por un total de USD 25.000 o más, independientemente de los posibles sospechosos.
- Transacciones sospechosas de USD 5.000 o más que involucren posible lavado de dinero o violaciones de BSA.

El informe SAR debe presentarse dentro de los 30 días de haber detectado los hechos que podrían constituir un fundamento para la presentación de un SAR (o dentro de los 60 días si no hay ningún sospechoso).

---

[279] 12 CFR 21.11 (OCC); 208.62, 211.5(k), 211.24(f), 225.4(f) (Junta de Gobernadores); Parte 353 (FDIC); 563.180(d) (OTS); 748.1(c) (NCUA); 31 CFR 103.18 (Tesoro).

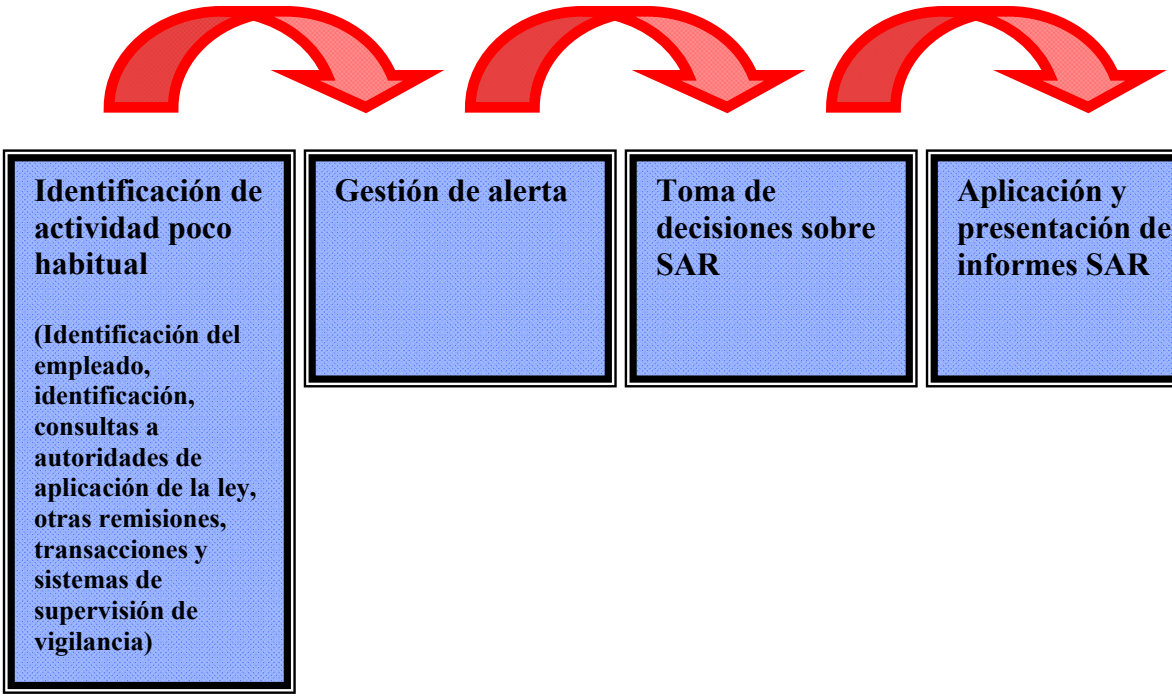
Las agencias citarán una violación de las normas de SAR y tomarán las medidas de supervisión correspondientes en caso de que la falta de presentación del SAR por parte de la organización evidencie una violación sistemática de sus políticas, procedimientos o procesos para identificar e investigar actividades sospechosas, involucre un patrón o práctica de incumplimiento del requisito de presentación de informes, o represente una situación importante o flagrante.

Otras exigencias con respecto a la conservación y presentación de informes de la BSA. Las organizaciones bancarias y cooperativas de crédito también están sujetas a otras exigencias de presentación de informes y gestión de registros BSA que se establecen en las normas emitidas por el Departamento del Tesoro.[280] Estas exigencias se analizan en forma detallada en el Manual de Inspección BSA/AML del FFIEC e incluyen, entre otros, requisitos aplicables a transacciones en efectivo e instrumentos monetarios y transferencias de fondos, presentaciones de Informes de transacciones en efectivo ("CTR") y sus normas de exención y debida diligencia, certificación y otras exigencias para las cuentas de bancos corresponsales y de banca privada.

Medidas de aplicación de la ley para exigencias BSA/AML que no pertenecen al programa. En las circunstancias que corresponda, una agencia podrá tomar medidas de aplicación de la ley formales o informales para abordar violaciones a las exigencias de BSA/AML que no sean las exigencias del Programa de Cumplimiento BSA. Estas otras exigencias incluyen, por ejemplo, las obligaciones normativas de SAR y CTR que se explicaron anteriormente.

[280] 31 CFR Parte 103.

Apéndice S: Componentes Clave de la Supervisión de Actividades Sospechosas



Índice Alfabético

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V