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.