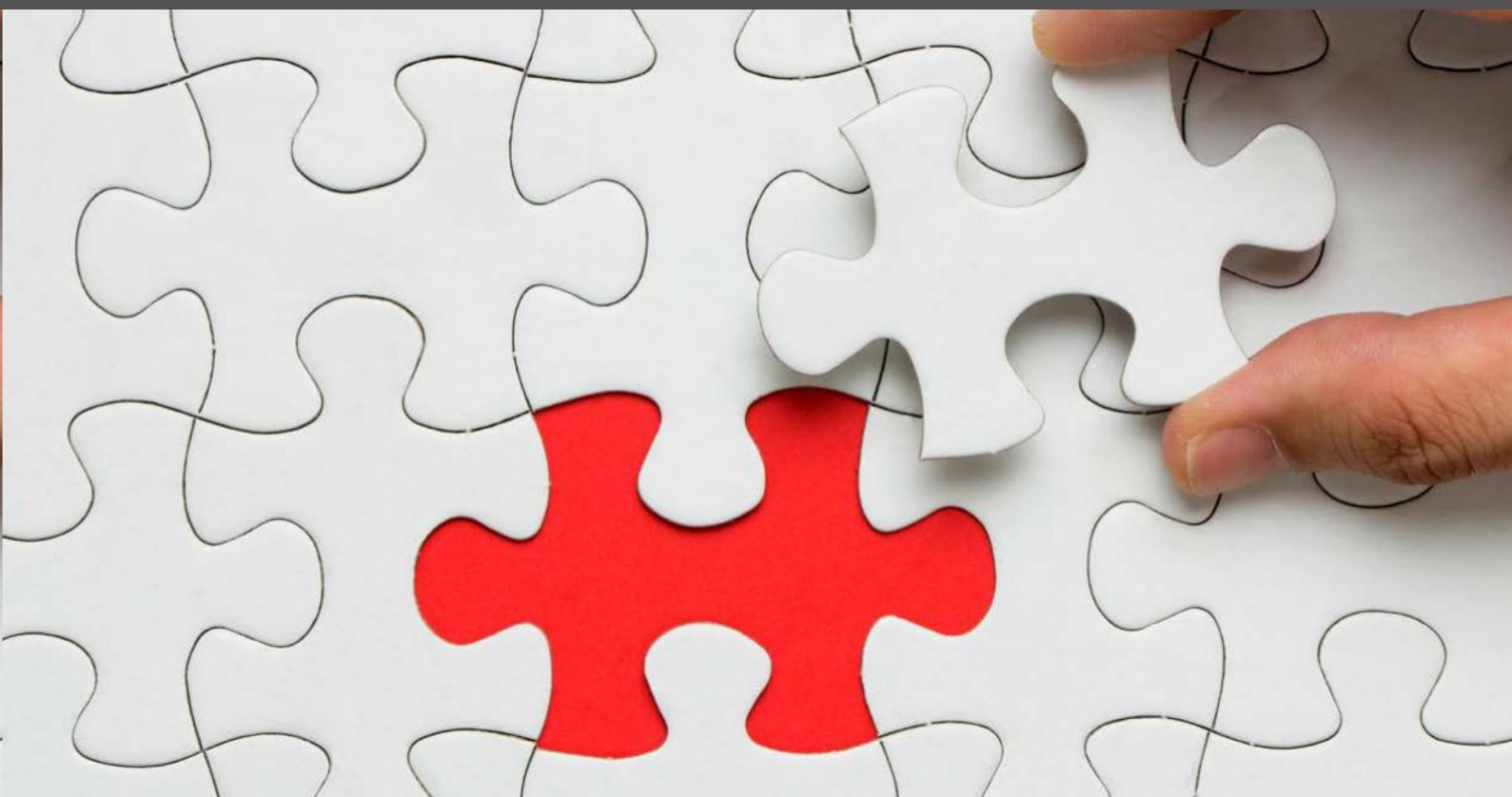
FATF

INFORME CONFIDENCIAL GAFI

Detección del financiamiento del terrorismo: *Indicadores de riesgo relevantes*

Junio de 2016



Detección del financiamiento del terrorismo: *Indicadores de riesgo relevantes*

El GAFI desarrolló los indicadores en este informe para ayudar a los organismos gubernamentales y a entidades seleccionadas del sector privado a detectar y desbaratar los flujos financieros de terroristas y organizaciones terroristas. El GAFI decidió no distribuir este informe en forma pública, para preservar la utilidad de estos indicadores y otra información relevante.

Las autoridades nacionales competentes serán responsables de comunicar este informe a las entidades relevantes del sector privado en su país. Los destinatarios de este informe deben mantener esta información en secreto y no duplicar, compartir o comunicar esta información de otra manera a terceros, sin la autorización previa de sus autoridades nacionales competentes.

Junio de 2016

INDICADORES DE RIESGO RELEVANTES

ÍNDICE DE SIGLAS

ALA/CFT	Anti-Lavado de Activos y Contra el Financiamiento del Terrorismo
ATM	Cajero automático
DDC	Debida diligencia del cliente
CIFG	Grupo contra el Financiamiento del EIIL
GAFI	Grupo de Acción Financiera Internacional
UIF	Unidad de Inteligencia Financiera
FTF	Terrorista extranjero
FTZ	Zonas de libre comercio
HOSSP	Hawala y otros proveedores de servicios similares de lavado de activos y financiamiento del terrorismo
EIIL	Estado Islámico de Irak y el Levante
KFR	Secuestro extorsivo
LA	Lavado de activos
MSB	Prestadores de servicios monetarios
MVTS	Servicios de transferencia de dinero o valores
OSFL	Organización sin fines de lucro
ROS	Reporte de operación sospechosa
FT	Financiamiento del terrorismo
TFS	Sanciones financieras específicas
TBML	Lavado de activos mediante operaciones comerciales

RESUMEN EJECUTIVO

La detección de la actividad del financiamiento del terrorismo (FT) es necesaria para identificar redes y sospechosos una vez ocurrido un ataque, pero también es fundamental para prevenir los eventos trágicos desde un principio. Desde 2001, el GAFI ha estado al frente de la asistencia al sector privado para identificar y entender mejor la naturaleza y el alcance de la actividad del FT. Este trabajo creció justificadamente durante los últimos dos años dadas las crecientes amenazas de FT que enfrentamos en todo el mundo. Los dos informes publicados en 2015 sobre *Financiamiento de la Organización Terrorista Estado Islámico de Irak y el Levante* (EIIL) y *Riesgos Emergentes de Financiamiento del Terrorismo* ayudaron a mejorar la comprensión de la comunidad global sobre el riesgo de FT. Sin embargo, dada la naturaleza dinámica de constante evolución de los riesgos y desafíos para detectar el FT, es importante que el GAFI brinde información detallada para ayudar en la detección de esta actividad.

Este informe es el resultado de una contribución importante de los sectores público y privado, y está diseñado para ser una herramienta práctica para que ambos sectores identifiquen, y en última instancia prevengan, el financiamiento del terrorismo y la actividad terrorista. La **Sección I** reconoce los diferentes roles y responsabilidades de estos sectores y la **Sección III** demuestra los beneficios mutuos que obtienen ambas partes al formar sociedades fuertes. Además, este informe sirve como herramienta a las autoridades competentes (particularmente a los organismos de seguridad) para comunicarse con las instituciones del sector privado de sus jurisdicciones. Por lo tanto, se solicita a las autoridades competentes que creen una manera efectiva de compartir esta información con el sector privado sin afectar en forma adversa las investigaciones en curso y los esfuerzos de inteligencia sobre los cuales se basan los indicadores.

Un indicador de riesgo demuestra o sugiere la probabilidad de ocurrencia de actividad sospechosa. El informe establece cómo deben usar los sectores público y privado los indicadores de manera efectiva, ya que no son ni exhaustivos ni aplicables a todas las situaciones. Generalmente, los indicadores son solamente uno de muchos elementos que contribuyen a un panorama mayor de riesgo potencial de terrorismo o FT y es importante que los indicadores (o un indicador solo) no sean vistos en forma aislada. Deben ser contextualizados con la información obtenida a raíz de la comunicación con las autoridades relevantes. Por lo tanto, cada país debería brindarle a su sector privado los indicadores y la información más relevante para ese país (y hacerlo usando herramientas y métodos existentes para compartir información en forma segura). Las autoridades competentes también deberían evitar usar este documento como lista de verificación al supervisar a las instituciones del sector privado, ya que no todos los indicadores se aplican a todos los países o a todas las instituciones.

El financiamiento del terrorismo, debido a su naturaleza, es extremadamente difícil de detectar. No solo porque implica cantidades de dinero menores que en el lavado de activos, sino porque además implica operaciones que generalmente no se pueden distinguir entre las actividades legítimas diarias. Por lo tanto, es imposible crear una lista perfecta de indicadores o una "fórmula milagrosa" para detectar el financiamiento del terrorismo. Por lo tanto, a pesar de la información detallada y específica contenida en este informe, continuarán existiendo importante brechas de conocimiento. Se pueden reducir estas brechas mejorando el intercambio de información, tal como se describe en la Sección III, particularmente compartiendo información contextual para mejorar los indicadores de riesgo.

El proceso de consulta de este informe ha profundizado nuestra comprensión de cómo utilizan las instituciones del sector privado los indicadores y otros mecanismos para identificar actividad relacionada con el terrorismo. Este informe pretende servir como un catalizador para que los países mejoren su comunicación e interacción con los sectores privados. La interacción continua ayudará a mejorar la detección del FT y enriquecerá los esfuerzos futuros del GAFI para combatir el financiamiento del terrorismo.

I. INTRODUCCIÓN

A. PROPÓSITO, ALCANCE Y OBJETIVOS

El informe *Riesgos Emergentes de Financiamiento de Terrorismo* (GAFI, 2015b) observa la importancia de sociedades público/privado genuinas para mejorar la conciencia sobre los riesgos emergentes de financiamiento del terrorismo (FT) y sus respuestas. Brindar orientación precisa y prospectiva al sector privado mejora sus procesos de control y supervisión y el tiempo de reporte de operaciones sensibles que puedan tener relación con el FT. Esta colaboración cercana ayuda a identificar y a comunicar el riesgo de FT entre todas las partes relevantes.

Este informe es una extensión del informe *Riesgos Emergentes de Financiamiento del Terrorismo* y apunta a desarrollar indicadores de riesgo para ayudar a los sectores público y privado a identificar y mitigar los riesgos de FT. El objetivo es que este tipo de información esté disponible al sector privado a través de la autoridad competente relevante. El informe incluye una sección sobre cómo mejorar la interacción con el sector privado para promover una comunicación más regular y orientada y la comunicación de pautas sobre indicadores de riesgo.

B. METODOLOGÍA, PARTICIPANTES Y DATOS UTILIZADOS

Este informe fue elaborado bajo la co-dirección de Francia y Estados Unidos, e incorpora la colaboración de una amplia variedad de otras delegaciones dentro de la red global del GAFI. Tanto las delegaciones de los países como las entidades del sector privado presentaron más de 30 conjuntos de indicadores de financiamiento del terrorismo, contribuyendo con la Sección II de este informe. Una parte de la información brindada se basó sobre el análisis estratégico de datos disponibles a las Unidades de Inteligencia Financieras. En la mayoría de los casos, **la información se brindó con la intención de que NO fuera de alcance público y, por lo tanto, este informe es confidencial y no debe ser diseminado.** Muchos de los indicadores recibidos son específicos de jurisdicciones o áreas geográficas particulares. Sin embargo, este informe brinda indicadores más generales que podrían adaptarse a las circunstancias individuales.

Este informe, además, se construye sobre la experiencia brindada a partir de la participación de las delegaciones en varios talleres de tipologías realizados dentro de la red global de GAFI y a partir del debate en la reunión sobre financiamiento del terrorismo mantenida entre el GAFI y el sector privado en febrero de 2016. El propósito de la reunión fue hablar acerca de buenas prácticas de sociedades público-privadas para identificar indicadores de riesgo y compartir información para detectar terroristas o FT. Los aportes recibidos durante la reunión con el sector privado fueron incorporados a este documento. El GAFI también mantuvo una sesión conjunta con el Grupo contra el Financiamiento del EIIL (CIFG) para reforzar mutuamente el trabajo de lucha contra el financiamiento del EIIL y para proteger al sistema financiero internacional del abuso por parte de organizaciones terroristas. Los expertos del CIFG también contribuyeron con este documento, específicamente brindando indicadores relacionados con el Financiamiento del EIIL (por ej., Sección II (G) sobre indicadores relacionados con la industria del petróleo y el gas).

Además, el GAFI distribuyó un cuestionario acerca de cómo comparten las autoridades competentes la información sobre los riesgos de FT con el sector privado, del cual se recibieron más de 40 respuestas. Emergieron tres temas clave relacionados con (1) las respuestas a los sujetos

obligados, (2) los tipos de información compartida y (3) los mecanismos para interactuar con el sector privado. La Sección III de este informe aborda estos temas.

C. TERMINOLOGÍA

Existe una amplia experiencia a nivel internacional de producción de indicadores o índices de riesgo de lavado de activos o flujos financieros ilícitos. El GAFI buscó desarrollar indicadores de "alerta" en una cantidad de sus informes para ayudar a los sectores financiero y gubernamental a identificar instancias de lavado de activos (LA) o actividad de FT. Sin embargo, la identificación de indicadores específicos de financiamiento del terrorismo presenta un desafío diferente (y más difícil), por muchos motivos. El concepto de riesgo es amplio y complejo. Este informe no usará el término "alerta" y se limitará a usar un término general, ***indicador de riesgo***, que se podrá usar para ayudar a identificar instancias de actividad terrorista o de FT. Un indicador de riesgo demuestra o sugiere la probabilidad de ocurrencia de actividad sospechosa. Aunque una cantidad de los factores identificados pueden no parecer tener una conexión directa con el terrorismo o el financiamiento del terrorismo, sin embargo, son relevantes al intentar identificar este tipo de actividad. Un indicador, o un grupo de indicadores, puede brindar una pista que requiera más análisis. Los indicadores identificados son solo un aspecto de un panorama mayor de riesgo potencial de terrorismo o FT.

En 2002, el GAFI publicó la *Guía de Instituciones Financieras para Detectar el Financiamiento del Terrorismo.* Esa guía no distinguía entre indicadores de FT e indicadores de LA. Como se indicó más arriba, muchos indicadores de riesgo relevantes no pueden conectarse directamente con la actividad de FT o LA. Los esfuerzos recientes identificaron y comprendieron mejor métodos y técnicas más específicas y exclusivas del FT. La investigación reciente del GAFI procuró explicar operaciones o comportamientos particulares asociados en forma exclusiva, o más probablemente, a técnicas o actividades de FT. El financiamiento del terrorismo generalmente implica sumas de dinero más pequeñas, generadas a nivel local, en comparación con el lavado de productos del delito. Estas diferencias hacen que los fondos destinados al terrorismo sean más difíciles de detectar que la actividad del lavado de activos de alto valor.

D. PÚBLICO

Los indicadores en este informe son relevantes tanto para el sector privado como público. En el sector privado, no se observarán todos los indicadores sin información contextual adicional de las autoridades competentes (ver Sección III). Dentro del sector privado, estos indicadores deben ser usados por el personal responsable del cumplimiento, el control de operaciones, el análisis de investigación y otras operaciones tipo UIF dentro de las instituciones financieras y Prestadores de servicios monetarios (MSB). Los indicadores son más relevantes para la industria bancaria pero podrían aplicarse a remesadoras de fondos y casas de cambio. La mayoría de los indicadores, particularmente aquellos relacionados con el comportamiento, se aplican a la banca minorista pero hay algunos indicadores que son más relevantes a la banca corporativa, por ej., Sección II.G. Los indicadores deben aplicarse a un rango diverso de clientes, desde personas con medios modestos a personas con un patrimonio elevado, y cubren ampliamente varios aspectos de la relación con un cliente. Los indicadores también son aplicables a pequeñas y medianas empresas y a conglomerados grandes.

Los indicadores también son relevantes a autoridades competentes, particularmente unidades de inteligencia financiera, servicios de aplicación de la ley o seguridad, que son responsables de conducir un análisis operativo y estratégico de las tendencias de FT. Los indicadores también pueden ayudar a las autoridades a detectar comportamientos de FT desde su perspectiva. Este informe estará disponible para autoridades competentes con la intención de que

lo compartan, o compartan su contenido, con entidades del sector privado (ver Sección III sobre Compartir información contextual para mejorar los indicadores de riesgo). Las autoridades competentes también pueden usar la información en este informe para elaborar sus propias advertencias a los sujetos obligados relevantes. Sin embargo, NO debe utilizarse este informe como una herramienta regulatoria con fines de cumplimiento y verificación. Hacerlo podría conducir, sin querer, a un abordaje basado en reglas para determinar el riesgo. El GAFI controlará la difusión y el uso de este informe para garantizar su máxima utilidad.

E. USO DE INDICADORES

Los indicadores identificados son globales, incluyendo actividades y situaciones específicas, pero lo suficientemente generales para permitir una aplicación adaptada. Las categorías son genéricas y apuntan a llamar la atención para que se puedan realizar investigaciones y análisis adicionales para evaluar si hay sospechas suficientes de actividades de FT detrás de ciertas operaciones, comportamientos y actividades. Este informe no tiene como fin ser utilizado como base para involucrarse en prácticas de eliminación de riesgo al por mayor o indiscriminadas o cualquier otra actividad que podría resultar en consecuencias indeseadas significativas fuera del propósito de prevenir el financiamiento del terrorismo.

Los indicadores provistos están derivados de un muestreo de los datos recibidos y de ninguna manera es una lista exhaustiva. Un solo indicador no puede garantizar por sí mismo la sospecha de financiamiento del terrorismo o brindar una indicación clara de dicha actividad. Además, la presencia de un solo indicador no necesariamente puede estar al nivel de sospecha, pero podría impulsar controles y análisis adicionales, según corresponda. De manera similar, la existencia de varios indicadores en relación con un cliente u operación también podrían garantizar el análisis. La observación de uno o más de los indicadores depende de las líneas de negocios, productos o servicios que ofrece una institución y cómo interactúa con sus clientes, y de los recursos humanos y tecnológicos de la institución.

Muchos de los indicadores en este borrador son demasiado generales y requieren de control, estudio o información contextual adicionales sobre el cliente o la operación para establecer sospechas. Muchos de los indicadores describen actividades cotidianas normales. Este informe pone énfasis en que el sector privado necesitará información contextual de las autoridades garantes del cumplimiento de la ley y de las unidades de inteligencia financiera para usar de la mejor manera los indicadores provistos. Dado que los riesgos de FT están en constante evolución, los indicadores en sí mismos son dinámicos. Al usar estos indicadores, las entidades deben tener en cuenta la totalidad del perfil del cliente, incluyendo la información obtenida en el proceso de debida diligencia del cliente (DDC), como así también otros factores de riesgo contextuales relevantes. Los sujetos obligados no siempre podrán establecer una conexión entre una actividad sospechosa de un cliente y actividades relacionadas con el terrorismo. Sin embargo, cualquier asunto sospechoso informado a las unidades de inteligencia financiera puede constituir una pequeña pero importante pieza de un rompecabezas mayor y puede ser crucial para el éxito de las investigaciones de FT y actividades asociadas al terrorismo realizadas por autoridades competentes.

Los indicadores deben brindar apoyo a los sistemas de control y reporte de actividad sospechosa e informar los análisis de inteligencia usando un abordaje basado en el riesgo. Los sistemas de monitoreo generalmente incluyen identificación o derivación de empleados, sistemas basados en operaciones (manuales), sistemas de vigilancia (automatizados) o una combinación de ellos. Algunos de los indicadores de este informe se pueden observar durante un control general de operaciones mientras que otros solamente se pueden presentar al realizar un análisis profundo o revisiones de casos.

Por ejemplo, algunos bancos han usado la minería de datos proactiva para identificar a terroristas extranjeros (FTF) y redes asociadas mediante la observación de la actividad de pago y el uso de las cuentas de sus clientes (incluyendo uso de tarjetas de débito/crédito). Esto incluye examinar datos de clientes sospechosos como la dirección y la información de pagos. Generalmente, esto se informa mediante alertas emitidas por indicadores trazados por las UIF. Este abordaje proactivo generalmente ayuda en el desarrollo del foco de investigaciones adicionales o controles intensivos. El sector privado también brindó un ejemplo de un gráfico que indica el estadio del proceso de monitoreo del cliente donde podrían verse estos indicadores. El ejemplo demuestra que algunos indicadores pueden identificarse durante los procesos iniciales de DDC o de vigilancia automatizada pero muchos de ellos requerirán de herramientas especializadas, investigaciones adicionales o información de los organismos de aplicación de la ley para poder ser identificados.

El mayor número de indicadores provistos puede resultar en dificultades para administrar esta información, particularmente para las instituciones más pequeñas. Algunas instituciones pueden elegir integrar los indicadores en sus sistemas automatizados (por ej., usando criterios o reglas de filtración) que podrían reducir la discreción del personal pero que podrían aumentar la capacidad de detección de anomalías. Los criterios de filtración del sistema, incluyendo perfiles y reglas específicos, deben basare sobre lo que es razonable y esperable de cada tipo de cuenta. Sin embargo, algunos indicadores, como aquellos relacionados con las actividades de gastos, no pueden ser automatizados, lo cual podría dificultar el control. Aquellos indicadores que pueden detectarse en forma automatizada, pueden requerir que las entidades intensifiquen la capacidad de sus sistemas de TI o gestión de la información (por ej., geoubicación de las conexiones de Internet y extracciones en el área de la frontera, la naturaleza de la actividad de gastos).

II. INDICADORES DE RIESGO PARA IDENTIFICAR ACTIVIDAD DE FT

Las Normas GAFI brindan un marco para ayudar a los sectores público y privado a identificar actividades de FT. Las normas fueron revisadas en 2012 para fortalecer los requerimientos en situaciones de mayor riesgo y permitir que estos sectores adopten un abordaje más focalizado en áreas donde persiste un alto riesgo, en particular en el contexto del financiamiento del terrorismo. La evaluación precisa de los riesgos de FT requiere de un análisis multifacético de los clientes, sus actividades y los riesgos conocidos asociados con un producto, país o tipo de operación.

Riesgos de clientes, productos y geográficos son tres categorías generales consideradas al realizar las DDC y pueden mostrar indicadores específicos de riesgo más alto que requieren medidas intensificadas. Dada la naturaleza única del financiamiento del terrorismo, este informe creó categorías de riesgo de FT específicas sobre la base de:

A. Comportamiento del cliente

B. Perfil económico

C. Riesgo geográfico

D. Actividad de gasto

E. Productos/servicios

F. Organizaciones Sin Fines de Lucro (OSFL) y

G. Comercio y entidades comerciales.

Esta es una categorización flexible y, en muchos casos, los indicadores pueden pertenecer a categorías múltiples.

A. INDICADORES RELEVANTES PARA EL COMPORTAMIENTO DEL CLIENTE

El conocimiento de un cliente representa un papel vital en la comprensión del comportamiento financiero del cliente en relación con sus actividades no financieras y con la relación general del cliente. Al desarrollar indicadores, el sector privado debería considerar la información de una cantidad de fuentes, incluyendo a título meramente enunciativo, el análisis de datos de operaciones internas, la revisión de los datos del Protocolo de Internet (PI), el análisis de datos sospechosos específicamente relacionados con eventos de FT potenciales, como así también la información provista por organismos de aplicación de la ley. Las instituciones generalmente realizan el monitoreo de las operaciones, el control de los nombres y las DDC intensificadas de clientes con conexiones financieras o subjetivas a personas/agrupaciones, entidades (por ej., industrias, OSFL) o jurisdicciones de alto riesgo.

El GAFI siempre fue explícito en relación con que el terrorismo y aquellos que apoyan al terrorismo nunca pueden estar asociados a ninguna religión, nacionalidad, civilización o grupo étnico. Sin embargo, cuando los terroristas, grupos terroristas o aquellos que apoyan al terrorismo reclaman estar asociados con bagajes particulares, dicho comportamiento puede ser tomado en cuenta para los fines de la debida diligencia basada en el riesgo. Este comportamiento incluye la adhesión a nociones radicales, extremistas o violentas que supuestamente surjan de la religión, el nacionalismo o la etnia. En este aspecto, se deben realizar esfuerzos para comprender qué puede constituir comportamientos radicalizados o extremistas que impliquen un riesgo de terror potencial comparado con el comportamiento que está dentro del rango más típico de las prácticas y creencias dentro del país o región.

Establecimiento de una relación comercial

Al establecer una relación comercial con un cliente, el nombre del cliente potencial debe ser contrastado con las personas o entidades designadas en las listas de sanciones financieras específicas (TFS) desarrolladas de conformidad con la ley y los procedimientos nacionales o internacionales aplicables.[1] Los sujetos obligados y las autoridades competentes deberían verificar además las listas de designación de personas o entidades de otros países. Naciones Unidas recientemente consolidó todas sus listas de sanciones (incluyendo las sanciones por FT) en una lista de sanciones de NU para facilitar el cumplimiento.[2] La Lista de Sanciones Consolidada incluye a todas las personas y entidades sujetas a medidas de sanciones del Consejo de Seguridad. Mientras que claramente no debería tratarse con las personas designadas, también debería considerarse a las personas vinculadas con las personas designadas para la aplicación de medidas de debida diligencia intensificadas, incluyendo a los representantes, beneficiarios finales, concubinos, parientes cercanos u otras personas que se conoce que están vinculadas con una persona designada. Esto incluye el monitoreo de operaciones solicitadas por una persona que se conoce que es cercana a una persona designada. La información a tener en cuenta al realizar controles de las listas de TFS incluye lo siguiente:

- Nombres, alias, fechas de nacimiento y otros identificadores personales de personas involucradas en terrorismo en listas de TFS nacionales o internacionales pueden estar vinculados con clientes actuales, beneficiarios y entidades comerciales en el archivo.
- Cuando se brindan, los domicilios de personas involucradas en terrorismo en listas de TFS nacionales o internacionales pueden estar vinculados con clientes actuales, beneficiarios y entidades comerciales en el archivo.
- El dinero u otros valores asociados a personas involucradas en terrorismo en listas de TFS nacionales o internacionales pueden estar vinculados con otras entidades o clientes.

El seguimiento de medios extranjeros y nacionales de fuente abierta puede asistir en la detección de clientes nuevos de alto riesgo. Las herramientas de investigación externas también pueden asistir en el desarrollo de una comprensión razonable de las personas asociadas a una operación. Las entidades deben tener en cuenta la prensa negativa o los medios adversos relacionados con la criminalidad asociada al financiamiento del terrorismo, las finanzas ilícitas u otras noticias negativas sobre los clientes de alto riesgo, sus titulares, operaciones comerciales, relaciones personales o industriales. Es probable que la información contenida en sitios de medios sociales por parte de organizaciones terroristas o personas radicalizadas sea beneficiosa al evaluar la actividad sospechosa potencial e identificar indicadores de financiamiento del terrorismo.

En la mayoría de las circunstancias, es difícil identificar la actividad relacionada con el FT sin información adicional de las autoridades competentes. La información de autoridades competentes generalmente incluirá tipologías o estudios de caso. Aunque las autoridades competentes generalmente no pueden intercambiar información contextual con las instituciones financieras sobre las personas asociadas con una investigación de FT hasta después de su conclusión, en algunas instancias, las autoridades compartirán la información para evitar la actividad terrorista (ver también la Sección III). Los asuntos a considerar incluyen:

- Personas previamente acusadas de terrorismo o delitos relacionados con el terrorismo.

1 Ver *Mejores prácticas internacionales sobre sanciones financieras específicas para el financiamiento del terrorismo* (GAFI, 2013a).

2 *Lista de sanciones consolidada del Consejo de Seguridad de Naciones Unidas* (UNSC, nd)

- Personas sobre las que se conoce o sospecha (por ej. bajo investigación) que están involucradas en actividad terrorista o como terroristas extranjeros.
- Publicaciones de medios sociales que apoyan o promueven la radicalización o el extremismo violento.
- Números de teléfonos móviles sobre los que se conoce o se sospecha su utilización por terroristas o sospechosos.
- Cualquier detalle de partidarios, simpatizantes o facilitadores clandestinos.

Debajo hay una muestra de indicadores de riesgo adicionales relevantes para el comportamiento del cliente al momento de establecer una relación comercial, que podrían ser tenidos en cuenta como indicadores de riesgo de FT relevantes:

- La resistencia a normas culturales del país donde el cliente conduce las operaciones, como esfuerzos manifiestos realizados por el cliente para evitar el contacto personal con los empleados bancarios (por ej., rechazo a interactuar con empleadas mujeres).
- El comportamiento que indica adhesión a nociones radicales o extremistas o que exhiban tendencias violentas (por ej., perfiles de medios sociales que exhiban publicaciones múltiples de noticias relacionadas o simpatizantes con organizaciones terroristas).
- Presentación de documentos de identidad notoriamente nuevos o falsificados (por ej., sello o foto falsificados, foto pegada sobre el sello, fecha de emisión que no coincide con la condición del documento en relación con el desgaste y deterioro).
- Nuevos clientes que hacen preguntas excesivas a los empleados bancarios en relación con las divulgaciones, requerimientos de informes, umbrales o requerimientos de mantenimiento de registros.
- Nuevos clientes reticentes a brindar información.
- Clientes que puedan estar realizando operaciones o actuando en nombre de otras personas.
- Cuentas abiertas en nombre de una persona jurídica con el mismo domicilio que otra persona física que no está asociada a la cuenta.
- Cuenta conjunta o usada por una gran cantidad de personas que no están relacionadas en forma profesional o personal y que no son relevantes al dueño de la cuenta.
- Persona física que abre varias cuentas (por ej., cuentas bancarias, tarjetas prepagas, billeteras electrónicas, etc.) para los fines de recibir y/o enviar transferencias de baja denominación.
- Persona física que abre una cuenta con el único fin de recibir una o más transferencias y de retirar o transferir dinero a otras personas.
- Establecimiento de una residencia permanente y/o cambio frecuente de domicilio y/o no estar relacionado aparentemente con la ocupación declarada.

- El uso recurrente de las mismas direcciones, los mismos números de teléfono y las mismas referencias (por ej., empleo) en varias cuentas aparentemente no relacionadas abiertas bajo diferentes nombres.
- Apertura de cuentas en regiones fuera de donde vive o trabaja el cliente y sin un propósito razonable.

B. INDICADORES RELEVANTES PARA EL PERFIL ECONÓMICO DEL CLIENTE

La debida diligencia del cliente comienza antes del establecimiento de una relación comercial y continúa mediante el monitoreo de cualquier cambio que ocurra en el comportamiento del cliente y en su perfil económico (incluyendo un cambio en el origen de los fondos y en los gastos). Los indicadores de comportamiento de FT también pueden verificarse en el curso de la relación comercial. De la misma manera, los indicadores detectados durante el monitoreo continuo deberían extenderse a aquellos que deben verificarse después del establecimiento de la relación comercial. El conocimiento del cliente, incluyendo el historial establecido de las operaciones financieras del cliente, puede ser importante para formar la sospecha de financiamiento del terrorismo. Los indicadores de las operaciones que no están en línea con las actividades usuales del cliente pueden incluir:

- La persona realiza varias operaciones en una oficina o en sucursales múltiples con la intención obvia de usar diferentes cajeros/cajeros automáticos.
- El cliente usa instrumentos financieros marcados (por ej., cheques) con notas informales, iniciales o símbolos, como un número de seguimiento que actúa como medio de identificación.
- La cancelación de la relación comercial o contrato sin explicación (por ej., cuentas que devengan intereses).
- Los depósitos, transferencias o pagos inesperados que se relacionan con la venta de activos personales, cuentas de jubilación y propiedad personal.
- La cuenta del cliente muestra signos de aumento inexplicable en los depósitos y flujos de dinero.
- Las cuentas individuales reciben múltiples transferencias de gran valor de personas no relacionadas o de fuentes desconocidas (por ej., el propósito declarado es "alimento").
- Varias personas físicas autorizadas a usar la cuenta que no son familiares de su titular.
- Clientes que son reticentes o se rehúsan a la presentación de información de identificación o a actualizar sus datos respectivos.
- Clientes que presentan diferentes documentos de identificación cada vez que la institución los requiere.
- Clientes que, en el transcurso de sus negocios, usan alias, sobrenombres u otras expresiones alternativas o simplificadas en vez de su propio nombre (completo). Esto podría incluir la transposición del orden de los nombres.

- Clientes cuya dirección o información de contacto (teléfono, fax, correo electrónico u otro) cambia a menudo, es incorrecta o continuamente no funciona, especialmente cuando los intentos de contacto por parte de la institución financiera ocurren poco después del establecimiento de una relación comercial.
- Transferencias solicitadas por diferentes personas o entidades que comparten uno o más detalles personales (por ej., apellido, domicilio, empleador, número de teléfono, etc.) el mismo día o en fechas cercanas.
- La frecuencia o el volumen de la operación es inconsistente con la ocupación, los ingresos, la edad, etc. del cliente.
- Retiro repentino importante (generalmente en efectivo) de pagos de beneficios que se devengan durante un período de meses.

Caso de estudio: **Cambios en el perfil económico de un cliente**

Una persona solicitó a la institución financiera cancelar sus cuentas que devengan intereses, sin brindar explicación. El contenido total de las cuentas de depósito se retiró en efectivo.

El cajero informó que esta persona se rehusó a interactuar con empleadas mujeres del banco y parecieron haber cambiado su vestimenta y apariencia física, lo cual podría ser indicador de adhesión a nociones radicales. Se observó un largo período de silencio en esta cuenta.

Fuente: Francia

C. INDICADORES RELEVANTES PARA LOS RIESGOS GEOGRÁFICOS

Al evaluar los riesgos de FT, los riesgos geográficos asociados con los países de origen, destino y tránsito deberían ser siempre tomados en cuenta. Esto incluye riesgos asociados con el originante de una operación y el beneficiario de fondos que puedan estar relacionados con una jurisdicción o región de alto riesgo. El riesgo geográfico también puede aplicarse a la nacionalidad, residencia o lugar de negocios de una persona. Este informe no busca identificar una lista de jurisdicciones como de alto riesgo de financiamiento del terrorismo. Las autoridades competentes pueden determinar su propia lista de países y regiones de alto riesgo (incluyendo áreas nacionales dentro de sus propias jurisdicciones) sobre la base de estos factores.

Jurisdicciones/regiones de alto riesgo

Los términos "jurisdicción/región de alto riesgo" no pueden definirse o explicarse fácilmente porque pueden aplicarse a una cantidad de situaciones e incluir riesgos asociados con varios tipos de delitos (por ej., narcotráfico, lavado de activos, corrupción), u otros riesgos relacionados con la situación política o económica. Desde la perspectiva del financiamiento del terrorismo, estos términos pueden incluir aquellas jurisdicciones/regiones en las que ocurren actividades terroristas (incluyendo, a título meramente enunciativo, ataques y planificación de ataques) o en las que residen las organizaciones terroristas, reclutan u obtienen soporte logístico para la perpetración de actos terroristas. Debajo hay ejemplos adicionales que podrían significar una jurisdicción/región de alto riesgo.

- Una zona de conflicto. Este es un término sinónimo para aquellas jurisdicciones/regiones de alto riesgo que no son estables, que están en guerra, donde la hostilidad armada está presente o donde las organizaciones terroristas están activas.

- Provincias/regiones con vínculos conocidos con organizaciones terroristas o que comparten fronteras con territorios controlados por organizaciones terroristas.
- Países donde se generan los fondos y otros activos (por ej., originante de las transferencias de fondos) para actos de terrorismo u organizaciones terroristas independientemente de dónde se realizan aquellos actos o dónde residen las organizaciones.
- Jurisdicciones/regiones que son puntos de tránsito o que han tenido flujos de dinero hacia/desde terroristas extranjeros (FTF) conocidos (ver caso de estudio a continuación).
- Jurisdicciones con deficiencias ALA/CFT estratégicas, marcos institucionales deficientes, aquellos que no cumplen con las Normas del GAFI (incluyendo aquellos identificados públicamente por el GAFI) o que generalmente no son cooperadores en materia de CFT.

Caso de estudio: **Uso de transferencias de fondos cerca de territorios donde opera el EIIL**

De acuerdo con información financiera confidencial, se descubrieron riesgos de financiamiento del terrorismo con respecto al uso de Transferencias Electrónicas de Fondos (TEF) vía canales bancarios y otras transferencias vía Sistemas de Transferencia de Valores Monetarios (MVTS) a áreas ubicadas cerca de territorios donde opera el EIIL o personas designadas. La ubicación de recepción de estas transferencias generalmente era en áreas conocidas por ser centros de financiamiento, logística y contrabando de terroristas extranjeros y organizaciones terroristas. En algunos casos, los medios sociales sugirieron que los beneficiarios de las transferencias de fondos pueden tener vínculos con grupos terroristas o radicales. En otros casos, se realizaron depósitos en efectivo excesivos en EE. UU. con posteriores transferencias electrónicas a beneficiarios en áreas ubicadas cerca de territorios donde opera el EIIL. Los riesgos identificados también incluyeron falta de información sobre el propósito de las transferencias, la relación de los receptores o la razón por la que las transferencias de fondos se realizaron en operaciones múltiples en períodos de tiempo cortos.

Fuente: Estados Unidos

Factores transfronterizos

Dentro de esta categoría se encuentran las operaciones y las actividades asociadas con el viaje, especialmente relacionadas con FTF. En esta área ya se ha realizado mucho trabajo, en particular por parte del Grupo Egmont de Unidades de Inteligencia Financieras, que trabajó en perfiles de FTF específicos. El Grupo Egmont desarrolló un boletín interno sobre FTF que está disponible a las autoridades competentes relevantes para su emisión a su sector privado. Este informe no busca duplicar el trabajo extenso de Egmont. Sin embargo, la Sección II.D de este informe incluye una cantidad de factores relevantes a FTF.

Además, el riesgo geográfico puede incluir el uso de servicios de transferencia de dinero brindados por una institución financiera, en paralelo con los pagos comunes, como así también las empresas familiares que brindan servicios de transferencias electrónicas a través de redes informales. Este informe busca explorar algunos de los indicadores de riesgo relevantes asociados con los servicios de transferencia de valores monetarios (MVTS) (además ver el informe sobre El rol de *Hawala y otros proveedores de servicios similares en el lavado de activos y el financiamiento del terrorismo* (GAFI, 2013b)). Otros indicadores relacionados con el riesgo geográfico están ubicados en las categorías asociadas con las actividades de gastos y productos y servicios. Debajo hay una muestra de los indicadores relevantes al riesgo geográfico:

- Varias personas que envían fondos al mismo beneficiario en una jurisdicción de alto riesgo.
- El mismo cliente que envía fondos a múltiples beneficiarios en una jurisdicción de alto riesgo.
- Transferencias transfronterizas de valores bajos enviadas/recibidas con alta frecuencia hacia/desde personas no conectadas o no relacionadas.
- Enviar/recibir fondos hacia/desde las mismas contrapartes por parte de personas que parecen actuar en forma separada. (Es decir, también conocido como una "red de consumidores" que representa a una cantidad de personas conectadas por contrapartes comunes).
- Un pago del exterior, con la descripción de la operación como donación, ayuda, préstamo, etc. y su inmediato retiro de efectivo, o inmediata transferencia a una cuenta diferente.
- Fondos excesivos pagados a una cuenta de un estudiante en un país extranjero por parte de un miembro de la familia o de una organización no relacionada.
- Clientes con residencia en una jurisdicción de alto riesgo, o con conexión a ella.
- Clientes que acceden a las instalaciones bancarias por Internet (en línea) desde una dirección de IP dentro de una zona de conflicto o una dirección no asociada con los registros de DDC.
- El cliente muestra gastos significativos en el extranjero en una cuenta recientemente abierta.
- Estadías en el extranjero más prolongadas (más de 6 semanas) por parte de personas sin empleo que continúan recibiendo beneficios por desempleo del gobierno.
- Indicaciones de que el cliente ha viajado (o viaja regularmente) a áreas en o alrededor de la zona de conflicto con efectivo encima.

Caso de estudio: **Ejemplo de red europea con facilitadores**

Cuatro personas trasladaron 28 remesas de fondos a través de siete entidades diferentes ubicadas en Alemania y Francia. Estas operaciones tuvieron 17 beneficiarios diferentes que retiraron los fondos en 16 entidades comerciales distintas, ubicadas en Egipto, Alemania, Grecia, Marruecos, Portugal y Túnez.

De acuerdo con el análisis, las operaciones vinculadas a este grupo ocurrieron entre 2006 y 2013, la mayoría de las cuales fueron en 2008. El beneficiario en Portugal retiró los fondos en enero de 2009 en tres entidades diferentes ubicadas en Oporto. No tenía ingresos o propiedades en Portugal. De acuerdo con la inteligencia recopilada a través de cooperación internacional, en 2014, el beneficiario en Portugal supuestamente viajó a Siria, vía Turquía, y es sospechado de haberse unido al EIIL. Posteriormente fue arrestado al regresar a Europa.

Fuente: Portugal

Secuestro extorsivo

El secuestro extorsivo (KFR) es una fuente de ingresos para los grupos terroristas, incluyendo el EIIL.[3] Las organizaciones terroristas usan las redes de facilitadores para mover los productos del KFR a través del sistema financiero global, incluyendo sistemas de remesas alternativos, casas de cambio, bancos y otras instituciones financieras.[4] El efectivo generalmente tiene un papel importante en el KFR. Es improbable que los bancos puedan determinar si un pago fue derivado de un pago de rescate en ausencia de información específica. Algunos indicadores recientemente identificados incluyen:

- Familiares (en nombre de la víctima) que adquieren dinero a través de la venta de activos o préstamos.
- Establecimiento de un fideicomiso (u otra estructura jurídica) para recolectar/almacenar donaciones de pagos de rescates.
- Establecimiento de un sitio de micromecenazgo (*crowdfunding)* para aceptar donaciones en nombre de la víctima.
- Envíos de efectivo en bultos grandes enviados a través de MVTS (incluyendo remesadores y hawalas) a jurisdicciones distintas a aquella donde ocurrió el secuestro.
- Transferencias de fondos internacionales en nombre de grupos o entidades religiosas. Personas (por ej. tesoreros) que controlan cuentas bancarias en nombre de organizaciones religiosas que, cuando son interrogadas por el banco, indican que el verdadero fin de las operaciones fue, de hecho, el pago de rescates.
- Extracción de dinero en efectivo de cuentas disimuladas para uso como pagos de ayuda.
- Fondos recibidos de un asegurador que comercializa productos de Seguro de Secuestro y Rescate (K&R).
- Cooperación con empresas o compañías de seguro que tratan en negociaciones para la liberación de rehenes.

D. INDICADORES RELEVANTES PARA LA ACTIVIDAD DE GASTOS

La actividad de gastos podría detectarse de muchas maneras diferentes, teniendo en cuenta la información provista por el cliente, el propósito de las transferencias de crédito y el sector comercial de las contrapartes. Como se observó en la sección sobre el riesgo geográfico, una cantidad de indicadores de gasto se relacionan específicamente a FTF. Estas personas realizarán una cantidad de arreglos financieros y logísticos antes de su viaje y mientras se encuentran en ruta a la zona de conflicto. Un indicador involucra la compra de una "visa electrónica" fuera del país de residencia del viajante o una inconsistencia con el primer destino declarado del viajante. Para evitar la detección, los FTF generalmente escalonan sus viajes a las regiones de conflicto viajando a través de destinos intermedios. Para legitimar estos viajes intermedios, los FTF obtendrán visas para sus destinos intermedios. Examinar el origen de los fondos y la edad del viajante (por ej., un adolescente) también puede ayudar a determinar si las compras serían consideradas anormales en relación con los gastos de planificación de la mayoría de los tipos de vacaciones.

[3] *Financiamiento de la Organización Terrorista del Estado Islámico de Irak y el Levante (EIIL)* (GAFI, 2015a).

[4] *Piratería Marítima Organizada y Secuestro Extorsivo Relacionado* (GAFI, 2011).

Aplicar estos indicadores puede presentar una cantidad de desafíos para el sector privado. Por ejemplo, las instituciones pueden recibir información insuficiente acerca del producto, servicio o incluso tipo de negocio que procesó la operación de crédito/débito. Además, muchos de los indicadores en esta sección son benignos en su naturaleza y no son indicadores inmediatos de financiamiento del terrorismo. Los indicadores pueden ser particularmente relevantes al identificar un cambio en la actividad operativa usual de una persona que se prepara para viajar a una zona de conflicto para convertirse en un terrorista extranjero (ver el caso de estudio a continuación), que muestra una desproporción entre los ingresos y los gastos. Esta sección abordará escenarios relacionados con los viajes, personas/grupos que gastan con fines diferentes a los viajes y la identificación de redes.

Actividad de gastos relacionados con los viajes

- Los pagos a tiendas de actividades al aire libre (donde pueden comprar botas, bolsas de dormir, ropa, ropa interior térmica, carpas y equipos).
- Pagos que indican citas en clínicas médicas antes de viajar.
- Compras de billetes aéreos, billetes de autobús, alquiler de autos, reserva de servicios de transporte.
- Reserva de vuelos de ida al exterior mediante tarjeta de crédito (generalmente para personas sin conexión directa identificable).
- Compra de numerosos billetes aéreos o de autobús, después de recibir varias transferencias electrónicas o de efectivo.
- Pago de visas, en particular pagos bancarios por Internet para visas electrónicas a regiones de conflicto.
- Viajeros que hacen preguntas con respecto a la confirmación de que los beneficiarios nominados de pólizas de seguro de vida recibirán el pago en caso de circunstancias que sugieran la participación en el terrorismo, y no ser víctima del terrorismo. (Estos casos involucran a FTF potenciales que no declaran su viaje a zonas de conflicto antes de la salida).
- Personas jóvenes que compran pólizas de seguro de funeral o vida, o que cobran una póliza para pagar los billetes aéreos.
- Compra de autos para exportarlos a países fronterizos con zonas de conflicto.
- Compra de teléfonos prepagos o tarjetas SIM.

Caso de estudio: **Actividades operativas de un FTF que se prepara para viajar a una zona de conflicto**

Una persona, sin ingresos regulares, registra numerosos pagos en pequeños montos por viajes (en tren, transporte público) realizados dentro de Francia. Esta actividad tiende a indicar la existencia de personas radicalizadas que podrían ser FTF potenciales.

Las cuentas bancarias mantenidas por las personas que se describieron anteriormente también están marcadas por un aumento en los gastos telefónicos en los meses anteriores a su partida. Se registra al menos una compra (por unos pocos cientos de euros) de "artículos deportivos" en la cuenta de la persona. La compra de "artículos deportivos" se realiza en línea o en tiendas de artículos deportivos, o en tiendas especializadas en la venta de artículos para climas extremos. Dichas compras pueden contribuir a obtener equipamiento militar básico (por ej., bolsa de dormir, botas de montaña, parkas, etc.)

Finalmente, las cuentas observaron compras en línea relacionadas con gastos de viaje (por ej., pagos a agencias de viaje, aerolíneas y compañías de ferris) fuera del territorio nacional.

Fuente: Francia

Caso de estudio: Facilitador de una red de terroristas extranjeros potenciales

Una persona que tiene varias cuentas bancarias recibió numerosas transferencias electrónicas de una gran cantidad de personas. Los fondos recibidos luego se transfieren a la cuenta bancaria de otra persona, que compra billetes de avión y seguro en forma habitual. Sin embargo, el uso de su tarjeta de crédito no muestra viajes al exterior.

Fuente: Turquía

Actividad de gastos no relacionados con los viajes

- Compra de dispositivos de comunicación y tecnología de la información caros y sofisticados (por ejemplo, teléfonos satelitales).
- Compra de juegos de disparo o participación en actividades de tipo de capacitación de combate.
- Compra de armas o productos de doble uso que pueden usarse para ataques terroristas o en un contexto de guerra (por ej., municiones, materiales explosivos, suministros militares, equipos ópticos o electrónicos) a través de cuentas de pago electrónico.
- Pagos a medios o librerías asociados con la propaganda del radicalismo, extremismo o violencia.
- Donación a OSFL o sitios web religiosos asociados con la propaganda del radicalismo, extremismo o violencia.
- Compra de múltiples tarjetas prepagas (por ej., teléfono, fines generales).

Identificación de redes

La minería proactiva generalmente identificará las relaciones que puedan mostrar redes más amplias alrededor de FTF sospechosos. Las redes generalmente pueden ser identificadas examinando las relaciones de los sospechosos principales a través de los datos del cliente, como dirección y datos de pago. Podrían usarse los siguientes factores para establecer redes.

- Direcciones compartidas.
- Uso compartido de computadoras y direcciones de IP.
- Depósitos de las mismas fuentes.
- Personas dentro de una red que distribuyen fondos a otras partes.
- Flujos de dinero del extranjero para financiar actividades nacionales.

E. INDICADORES RELEVANTES PARA PRODUCTOS O SERVICIOS

Como otras categorías de indicadores de riesgo, esta área es amplia, diversa y de difícil organización. Un tema a considerar es cómo se usan los productos y servicios ofrecidos por el sector financiero para mover fondos. Un punto de referencia útil es la Sección III (B) del informe de 2015 *Riesgos Emergentes de Financiamiento del Terrorismo* (ver páginas 20-23). Esta sección provee una descripción general de los métodos y técnicas de FT tradicionales que todavía se utilizan para trasladar fondos. Los indicadores de muestra que se brindaron, generalmente cubren aquellos productos identificados en el informe al que se hace referencia arriba. De manera alternativa, la Sección IV (B y C) del informe *Riesgos Emergentes de Financiamiento del Terrorismo* observó las vulnerabilidades relevantes a los medios sociales y una cantidad de productos y servicios nuevos.

Sistemas de transferencia de valores monetarios y servicios de remesas

El GAFI define MVTS como servicios financieros que implican la aceptación de efectivo, cheques, otros instrumentos monetarios u otras reservas de valor y el pago de una suma correspondiente de efectivo u otra forma a un beneficiario mediante una comunicación, mensaje, transferencia o a través de una red de compensación a la cual pertenece el prestador de MVTS. Las operaciones realizadas por dichos servicios pueden involucrar uno o más intermediarios y un pago final a un tercero, y pueden incluir métodos de pago nuevos. Una cantidad de los indicadores identificados bajo la sección de riesgo geográfico se relacionan con MVTS.

Los cambistas de dinero y las compañías de transferencia continúan siendo uno de los medios más grandes mediante los cuales el EIIL traslada los recursos financieros. Estos tipos de compañías son prominentes en Irak y en Siria, donde solamente una minoría de la población tiene cuentas bancarias. Los negocios de la región dependen de estas compañías para enviar y recibir pagos a y de homólogas extranjeras, aun así son particularmente vulnerables a la explotación por parte del EIIL. Por ejemplo, Irak tiene más de 1900 cambistas de dinero registrados y 34 transmisores de dinero registrados. En enero de 2016, el Banco Central de Irak (CBI) identificó de manera pública casi 150 cambistas y transmisores de dinero conocidos por realizar operaciones en nombre del EIIL o que se encuentran ubicados físicamente en territorio controlado por EIIL[5]. El CBI emitió una directiva prohibiendo su participación en la ventana de cambio de moneda extranjera.

Riesgos geográficos

- Operaciones con/en/desde regiones de alto riesgo hacia/desde aparentemente personas no relacionadas sin conexión familiar aparente.
- Transferencias a jurisdicciones/regiones de alto riesgo que no son consistentes con las operaciones comerciales extranjeras habituales del cliente.

[5] La lista del Banco Central de Irak de cambistas y transmisores de dinero prohibidos se encuentra en:http://www.cbi.iq/documents/public%20Blacklist%2016%20March%202016%205th%20april.xlsx

- El remitente y el beneficiario no tienen relación con el país donde envían/reciben el dinero y no pueden explicar suficientemente por qué se envía/recibe el dinero allí (especialmente cuando el receptor es un ciudadano extranjero).
- El remitente específicamente pide que el dinero sea dado en una moneda extranjera y no en la moneda local.
- Enrutamiento de operaciones en múltiples países, a través de corredores o regiones de alto riesgo.
- Clientes que usan sistemas web identificados con distancias significativas entre la ciudad de residencia y la ubicación de la dirección IP.
- El beneficiario constantemente brinda la dirección de un hotel en un área turística como su domicilio personal.

Problemas de identificación

- Documentos de identificación múltiples provistos por la misma persona, que contienen información inconsistente, o diferentes personas que usan los mismos documentos de identificación.
- Clientes que presentan datos biográficos inconsistentes (por ej., una creciente cantidad de terroristas extranjeros de países occidentales son conversos musulmanes que cambiaron sus nombres a un apodo árabe. Las operaciones también pueden ser realizadas con su nombre anglosajón). Al establecer una relación comercial, debe verificarse el nombre de los clientes en las listas de sanciones financieras específicas (TFS) (ver la sección anterior sobre *Establecimiento de una* relación comercial).
- Números de teléfono reales reemplazados con números de teléfono generados en forma aleatoria o secuencias lógicas de números que podrían parecer un número de teléfono nacional (por ej., 0123456789).

Volumen y frecuencia de las operaciones

- Alto volumen de operaciones realizadas por una sola persona, en diferentes ubicaciones.
- El aumento repentino del volumen de las operaciones por parte de múltiples personas en una ubicación de agente única, durante un período de tiempo corto.
- Aumento en el volumen de las operaciones no relacionadas con un patrón habitual conocido localmente (por ej., remesa de salario o celebración cultural).
- Operaciones a/de ciudades identificadas como receptoras de un número creciente de transferencias de fondos y/o fondos entre períodos pre-crisis y conflictos en curso.

Redes de consumidores "muchos a uno" y "uno a muchos"

- Personas que realizan operaciones de volúmenes grandes con múltiples países.
- El mismo cliente que envía fondos a múltiples beneficiarios en una jurisdicción de alto riesgo.
- Transferencias transfronterizas de valores bajos enviadas/recibidas con alta frecuencia hacia/desde personas no conectadas.
- Remitentes múltiples que transfieren fondos a una única persona, que actúa como receptor "tercero".
- La misma persona recibe dinero de diferentes compañías remesadoras de fondos o ubicaciones de agentes MVTS.

Otros elementos

- El cliente parece conocer el monto que se transfiere una vez que el empleado del MVTS cuenta el dinero.
- El cliente no muestra interés por los costos de la transferencia.
- La operación enviada nunca fue recibida por el beneficiario, que supuestamente está fallecido.

Caso de estudio: **Red de cobradores mediante MVTS**

Varios miembros A, B y C de una familia recibieron una gran cantidad de transferencias de efectivo a través de MVTS, cada uno de ellos de distintas personas aparentemente no relacionadas (diferentes nombres y varias ubicaciones en todo el país). Aquellas personas A, B y C siempre brindaron números de teléfono consistentes en una secuencia de números. Enviaban regularmente transferencias de efectivo a personas D, E y F ubicadas en un país vecino a una zona de conflicto. Los receptores de esas transferencias siempre brindaron un hotel en una zona turística como su domicilio personal. Los receptores D, E y F nunca recibieron dinero al mismo tiempo y parecían operar en forma sucesiva. Las personas A, B y C enviaban su dinero a las únicas personas activas, presuntamente conscientes del cambio de nombre del cobrador de D a E y luego de E a F. Una persona con varias cuentas bancarias recibió numerosas transferencias electrónicas de una gran cantidad de personas. Los fondos recibidos luego se transfieren a la cuenta bancaria de otra persona, que compra billetes de avión y seguro en forma habitual. Sin embargo, el uso de su tarjeta de crédito no muestra viajes al exterior.

Fuente: Francia

Hawala y otros proveedores de servicios similares

Los hawalas se consideran un subconjunto de MVTS y se definen como transmisores de dinero[6], particularmente con vínculos a regiones geográficas o comunidades étnicas específicas, que organizan la transferencia y la recepción de los fondos o el valor equivalente y lo liquidan a través del comercio, efectivo y liquidación neta durante un período de tiempo. Mientras que generalmente usan canales bancarios para liquidar entre dos agentes de recepción y pago, lo que los distingue de otros transmisores de dinero es su uso de métodos de liquidación no bancarios, incluyendo la liquidación a través del comercio y el efectivo, como así también un tiempo de liquidación prolongado. Esta descripción se basa sobre los servicios que brindaron y no su estado legal. Estas NO son redes de transferencia de dinero globales (incluyendo a los agentes) operadas por transmisores de dinero y transferencias de dinero multinacionales grandes.

El informe de 2013 del GAFI sobre *El rol de Hawalas y otros prestadores de servicios similares en el lavado de activos* y financiamiento del terrorismo (HOOP) identifica las vulnerabilidades de FT y brinda orientación sobre los patrones de las operaciones que generalmente se asocian con prestadores de transferencia de dinero ilegal/no regulado, incluyendo HOSSP. Debajo, se hace una breve referencia sobre algunos de estos indicadores de riesgo para identificar proveedores sospechosos (además ver *Indicadores relevantes a riesgos geográficos*).

- Uso extensivo de cuentas de cobro (en las que se depositan o agregan pequeñas sumas y luego se transfieren al extranjero en intervalos regulares).
- Transferencias electrónicas enviadas frecuentemente por comerciantes a países extranjeros que no parecen tener conexión comercial con los países de destino.
- Cuentas comerciales usadas para recibir o desembolsar grandes sumas de dinero pero que virtualmente no muestran actividades normales relacionadas con el negocio como el pago de sueldos, facturas, etc.
- Depósitos frecuentes de cheques de terceros y giros postales a cuentas comerciales o personales.

El informe *El rol de Hawalas y otros prestadores de servicios similares en el lavado de activos y financiamiento* del terrorismo (HOSSP) también subraya el uso de redes hawala delictivas y el rol de diferentes personas como los controladores. El controlador (también llamado corredor de cambio en algunas jurisdicciones) ofrece servicios globales especializados en lavado de dinero y brinda a los delincuentes un punto central de contacto y coordinación para sus requisitos. El cliente delincuente le dice al controlador quién entregará el dinero y dónde debe pagarse el valor. El informe identificó una cantidad de métodos que podrían considerarse indicadores de riesgo relevantes, como:

- Usar MVTS locales cómplices para bancarizar y transmitir el dinero a terceros o en cuentas administradas por el controlador.
- Pagar el dinero en cuentas bancarias en nombre del controlador para completar remesas futuras separadas.
- El movimiento físico del efectivo (contrabando de efectivo) por correo, flete o cargo.

[6] *El rol de Hawalas y otros prestadores de servicios similares en el lavado de activos y financiamiento del terrorismo* (GAFI, 2013b)

Efectivo y cajeros automáticos

Mientras que el uso de efectivo está cubierto en la categoría de *actividad de gastos*, el efectivo también es un *tipo de producto* usado por aquellos que financian el terrorismo. Esta es otra área en la que se trabajó en el desarrollo de indicadores relacionados con FTF. Dado los importes relativamente bajos involucrados en financiamiento del terrorismo, se presta a contrabando de efectivo. El uso de billetes de alta denominación (por ej., billetes de EUR 500) a veces lo facilitan. El contrabando lo realizan los terroristas mismos que viajan a la región, como así también los amigos y familiares que viajan a la región una vez que los terroristas estén en su lugar.

También hubo ejemplos donde se establecen cuentas bancarias para cobrar donaciones de depósitos múltiples de poco efectivo que poco después se retiran en diferentes importes en cajeros automáticos (ATM) de autoservicio. Por ejemplo, el dinero se puede retirar rápidamente después del depósito desde cuentas de un ATM, o varios en proximidad cercana (en días consecutivos o varias extracciones con diferencia de días). Sin embargo, una delegación informó que usar ATM y operaciones con tarjeta no fue indicador concluyente, debido a la gran cantidad de ciudadanos que vacacionan en áreas vecinas a las zonas de conflicto, la gran cantidad de ciudadanos que tienen raíces familiares en las mismas áreas fronterizas y el gran contingente de trabajadores legítimos de asistencia, periodistas y diplomáticos que viajan al área. Además, algunos bancos pueden tener información insuficiente sobre la ubicación precisa (por ej., país o código de identificación del ATM) del ATM usado. Algunos indicadores generales que involucran dinero en efectivo y ATM que se informaron incluyen los siguientes:

- La extracción de efectivo repentina, aproximadamente correspondiente al saldo de cuenta actual, justificada como la necesidad para viaje al extranjero.
- El cliente solicita la extracción de fondos en efectivo transferidos anteriormente a su cuenta personal dentro de un período de tiempo corto después de la operación inicial.
- El cliente solicita el pago en efectivo del saldo no utilizado de su cuenta.
- La estructuración de depósitos en efectivo de operaciones más pequeñas para evitar los requisitos de reporte disparados por un umbral específico.
- La estructuración de extracciones de efectivo en varias extracciones de un solo ATM en días consecutivos o en múltiples ATM en ubicaciones cercanas.
- Las extracciones de efectivo usando tarjetas de débito, el mismo día o días consecutivos, en diferentes países a lo largo de la ruta identificable hacia una zona de conflicto.
- Montos bajos en efectivo depositados frecuentemente en terminales autoservicio a cuentas privadas (la cuenta se usa para cobrar donaciones) y poco después, la extracción de los fondos recolectados en terminales autoservicio.
- Grandes depósitos de efectivo seguidos por transferencias internacionales de bajo valor debajo del umbral de reporte.
- Depósitos estructurados en una cuenta de terceros, seguidos de extracciones inmediatas en ATM en el extranjero en áreas de tránsito o jurisdicciones de alto riesgo.

- Cuentas individuales que repentinamente cambian actividades típicas como depósitos numerosos, grandes realizados por ATM y luego consultas repetidas de saldo por teléfono y luego la extracción de grandes montos por ATM.

Caso de estudio: **Acceso continuado a cuentas bancarias por parte de FTF**

De acuerdo con la información financiera sensible, se descubrieron riesgos de financiamiento del terrorismo relacionados con extracciones de divisas extranjeras por ATM realizados por desconocidos en áreas ubicadas cerca de territorios donde opera el EIIL. Estas extracciones fueron tomadas de cuentas bancarias con base en Estados Unidos usando una tarjeta de cheques. Otro riesgo de financiamiento de terrorismo identificado fue la existencia de depósitos grandes en cuentas bancarias seguidas de extracciones de divisas extranjeras en área ubicadas cerca de territorios donde opera el EIIL. Esta información revela los riesgos de financiamiento del terrorismo presentados por la capacidad continua de las personas que se cree que viajaron a áreas ocupadas por el EIIL de tener acceso a sus cuentas bancarias en sus países de origen.

Fuente: Estados Unidos (Informe del GAFI sobre Financiamiento del EIIL, 2015)

Tarjetas de crédito

De manera similar a los clientes de bancos, muchos clientes de tarjetas de crédito son sujetos de una evaluación y categorización dentro de una estructura de riesgo en niveles según un análisis de factores múltiples. Un solicitante o titular de una cuenta de tarjeta de crédito puede estar sujeto a diferentes niveles de debida diligencia dependiendo del nivel que se le asigne. Además, ciertos tipos de productos o servicios pueden estar sujetos a controles o requerimientos intensificados, o no estar disponibles en un cierto país o para un nivel de cliente. La ubicación geográfica del solicitante o del cliente es el factor inicial para el proceso de evaluación de riesgo, pero se pueden realizar ajustes específicos según la evaluación de otros factores de riesgo individuales. Muchos de los indicadores de comportamiento identificados en la Sección II (A) también se aplican a estos productos. Algunos de los indicadores específicos identificados incluyen:

- Adelantos de efectivo repetidos en muchos países vecinos a áreas de conflicto o países que están a lo largo de las rutas seguidas normalmente a/desde áreas de conflicto.
- Pagos con tarjeta de crédito en varios países durante el tránsito (por ejemplo, estaciones de servicio, peajes en las rutas o en ubicaciones cercanas a un aeropuerto).
- El cliente muestra adelantos de efectivo de alto valor en una tarjeta de crédito recientemente emitida.
- Adelantos de efectivo en tarjetas de crédito generalmente sin pago inmediato.
- Dada la capacidad crediticia del cliente, solicitud infundada o injustificada para un aumento máximo del límite de crédito.
- Alcance de los límites de crédito antes de salir de viaje.
- Aparente ausencia de cambio en el uso de una tarjeta de crédito después de la salida en avión a áreas de conflicto (por ej., tarjeta usada en un país propio por una tercera persona) (ver estudio de caso a continuación).
- Repentino uso de tarjetas de crédito en territorios de alto riesgo (por ej., adelantos de efectivo aumentados) cuando el uso fue precedido/seguido por unos meses de inactividad.

- Uso de tarjetas de crédito solo para recibir y realizar operaciones entre personas mientras faltan pagos por bienes y servicios (por ej., personas que actúan como fachada).
- Uso de tarjetas de crédito registradas a nombre de terceros.

Caso de estudio: **Período de quietud en el uso de la tarjeta de crédito**

El uso de tarjetas de débito bancarias en el extranjero seguido por períodos de quietud con respecto al uso de aquellas tarjetas identificadas. En este caso, después de que se registraran los gastos de viaje en la cuenta, la cuenta queda inactiva durante un período de tiempo, dando así la impresión de que el titular de la cuenta no necesita financiación para su viaje al exterior. Cuando la cuenta vuelve a activarse, generalmente es para realizar una compra en una tienda cercana a un aeropuerto.

Otros ejemplos de riesgo incluyen el uso de la tarjeta de crédito de alguna persona en el propio país, mientras que esta persona presuntamente salió a un área de conflicto, para simular que el FTF nunca salió de su país de origen.

Fuente: Francia

Préstamos bancarios/personales

Una tendencia emergente identificada en el informe del GAFI *Riesgos Emergentes de Financiamiento del Terrorismo* incluye FTF sospechados que solicitan préstamos pequeños, a corto plazo de muchos proveedores simultáneamente sin intención de devolverlos. Debajo, hay una muestra de los indicadores identificados:

- Clientes que toman los préstamos bancarios en efectivo y tienden a incumplir.
- El uso de fondos de préstamos bancarios por parte de clientes inconsistentes con los propósitos declarados.
- El cliente solicita un préstamo personal grande y poco después retira una porción significativa en efectivo.
- Toma de pequeños préstamos con varias compañías de préstamo/crédito donde no se realiza el pago.
- Préstamos otorgados (por ej., sobre la base de declaraciones de ingresos falsificadas) cuando hay indicaciones de que las personas pueden huir al exterior.
- Toma de préstamos frecuentes usando ítems de alto valor como garantía.
- Solicitudes de préstamos que parecen injustificadas para los antecedentes económicos y financieros del solicitante.
- Terceros no relacionados que actúan como garantes de préstamos para el solicitante.
- Solicitudes de préstamos fraudulentos para la compra de bienes que no parecen haber sido usados por los solicitantes (por ej., compra de vehículos o electrodomésticos).

Caso de estudio: **Solicitud de numerosos préstamos a corto plazo**

Numerosos casos investigados trataban con créditos de montos bajos de clientes (menos de EUR 2.000), que se retiraron en efectivo desde la cuenta del titular dentro de las 24 a 48 horas. Por lo tanto, es más probable que el monto del crédito sea desviado de su intención original para establecer una "caja de ahorros" para financiar un viaje o artículos de logística.

Fuente: Francia

Caso de estudio: **Falta de pago de un préstamo personal**

Una persona recibió dos préstamos personales por un total JOD 7.500. Una vez que dejó de realizar los pagos, el banco intentó llamar a la persona y a su empleador, quien mencionó que la persona estaba ausente del trabajo desde hace un período de tiempo largo.

Después de solicitar información de su homóloga, se le dijo a la UIF que esta persona viajó al país (H) y luego a otro país vecino a la zona de conflicto. La UIF del país (H) derivó el caso al fiscal general competente por una sospecha de participación en financiamiento del terrorismo. El fiscal general competente confiscó sus bienes muebles e inmuebles y los de su familia.

Fuente: Jordania

Cambio de divisas

EL GAFI no ha estudiado ampliamente los riesgos de FT relevantes al cambio de divisas/dinero. Dicho esto, algunos indicadores identificados a la fecha que podrían ser relevantes a este servicio incluyen los siguientes:

- Falta de información con respecto al propósito de la persona y el origen de los fondos.
- Cliente del banco que cambia una gran cantidad de divisas extranjeras a divisas nacionales y que las usa para abrir una nueva cuenta bancaria en un área fronteriza a una zona de conflicto.
- Cambio de un monto significativo de divisas a billetes de denominación alta (por ej., billetes de EUR 500).
- Operaciones de cambio de divisas seguidas por transferencias de dinero internacionales a jurisdicciones de alto riesgo en un período de tiempo corto.
- Red internacional de cambistas de divisas. Comercio internacional entre varios cambistas que residen en jurisdicciones de alto riesgo.
- La red internacional comprende a los cambistas de divisas y entidades de comercio que residen en jurisdicciones de alto riesgo: sistema de compensación y liquidación entre efectivo y *commodities*, sin movimientos transfronterizos.
- Cambistas de dinero en el extranjero sospechados de entregar moneda falsificada.
- Casas de cambio no registradas que usan mecanismos de liquidación de compensación con casas de cambio registradas cómplices que mantienen cuentas bancarias.

- Casas de cambio que toman parte en remates de dólares, tenidos por el banco central, más a menudo de lo necesario dada la magnitud de sus actividades.

Productos y servicios de pago nuevos

El informe *Pautas para un abordaje basado en el riesgo para tarjetas prepagas, pagos móviles y servicios de pago* por Internet (GAFI, 2013c) identifica un rango de factores de riesgo que ayudan a identificar los riesgos de LA/FT asociados con nuevos productos y servicios de pago. El valor puede almacenarse digitalmente en una variedad de productos de pago nuevos (por ej., billeteras electrónicas, tarjetas prepagas, pagos móviles) y estar interconectados para realizar operaciones. Estos productos pueden usarse para operaciones de compra y comercio pero también para permitir la transferencia internacional de fondos entre personas. Los indicadores identificados en este informe relacionados con actividades de gasto y riesgos geográficos podrían ser relevantes para estos productos.

Estos productos y servicios nuevos son operados por una variedad de prestadores de servicios de pago diferentes. Cuando las instituciones no financieras administran estos productos, los requisitos de DDC pueden no ser tan sólidos y por lo tanto, representar una mayor vulnerabilidad de FT.

Pagos por Internet

Los servicios de pago por Internet brindan mecanismos para que los clientes accedan, a través de Internet, incluyendo teléfonos inteligentes, a cuentas prefinanciadas que pueden ser usadas para transferir dinero electrónico o valores guardados en estas cuentas a otras personas o negocios que tengan cuentas con el mismo prestador.

- Una persona que usa muchos perfiles financieros (por ej., billeteras electrónicas) para registrarse en múltiples sistemas de pago.
- Inscripción a billetera electrónica de una jurisdicción/región de alto riesgo.
- Reabastecimiento de la cuenta de una jurisdicción/región de alto riesgo.
- Transferencia remota de dinero desde la billetera electrónica a cuentas de terceros abiertas en una jurisdicción diferente (persona a persona).
- Colocación de detalles financieros en sitios web y redes sociales con contexto extremista o radical.
- Pagos que indican que la cuenta puede ser usada para colecta de fondos para caridad.
- Origen de los fondos grande y diverso (por ej., transferencias bancarias, tarjetas de crédito y financiación en efectivo de diferentes ubicaciones) usado para financiar la misma billetera de dinero electrónico.
- Cuentas bancarias múltiples de bancos ubicados en varias ciudades usadas para financiar la misma cuenta.
- Cuentas en línea vinculadas a personas relacionadas con cargos de terrorismo por nombre, tarjetas de crédito, domicilios, actividad de correo electrónico y *cookies* informáticos. (Por ej., estas cuentas se usaron para comprar piezas electrónicas y tarjetas de celular prepagas en línea).

Caso de estudio: **Pagos de billetera electrónica "muchos a uno"**

Durante una iniciativa de la UIF para monitorear las fuentes abiertas de una red social (es decir, Vkontakte), una publicación llamó la atención. Esta publicación pedía donaciones para brindar asistencia financiera a las familias de terroristas, para Yihad y para financiar la capacitación de terroristas. En esta publicación se mencionaron varios números de billetera electrónica. Una persona propietaria de esas billeteras electrónicas, recibió las transferencias de múltiples individuos ubicados en diferentes países. El dinero en esas cuentas electrónicas luego fue enviado a una cuenta bancaria móvil vinculada con un número de teléfono ubicado en un área de conflicto.

Fuente: Federación Rusa

Tarjetas prepagas

Las tarjetas prepagas son tarjetas cargadas con una cantidad fija de moneda o valores electrónicos. Las tarjetas prepagas recargables con fines generales que están enlazadas a una cuenta bancaria generalmente están sujetas al cumplimiento de DDC. Como los productos bancarios similares, tal como tarjetas de débito, pueden usarse con fines de FT para retirar dinero de ATM en una jurisdicción de alto riesgo (ver la sección anterior sobre *Efectivo y cajeros automáticos*). Además, debajo hay indicadores específicos que también podrían ser relevantes a las tarjetas prepagas con cuenta:

- Tarjetas prepagas extranjeras emitidas en jurisdicciones de alto riesgo.
- Registro de múltiples tarjetas prepagas para familiares, en un contexto de partida a una jurisdicción/región de alto riesgo.
- Uso de transferencias tarjeta a tarjeta a/desde jurisdicción/región de alto riesgo.
- Verificación de operaciones en línea desde una dirección de IP en un corredor de alto riesgo.
- Intento de realizar una operación por encima de la base prepaga, por parte de alguien que no parece conocer el monto de los fondos asignados, por lo tanto, alguien que podría no ser el titular original de la tarjeta.

Con respecto a tarjetas prepagas sin cuenta bancaria, vendidas por minoristas, la identificación generalmente se requiere cuando se supera un umbral de monto máximo o límite de tiempo de recarga. Esas tarjetas pueden recargarse nacionalmente a través de métodos electrónicos de efectivo y llevarse al extranjero sin llamar la atención. Al arribar al país de alto riesgo o al país de tránsito para el financiamiento del terrorismo, los fondos se vuelven a convertir en efectivo a través de múltiples extracciones de ATM extranjeros.

- Uso de tarjetas prepagas registradas bajo identidades falsas o bajo el nombre de otra persona para comprar por Internet.
- Tarjetas cargadas a través de medios de pago anónimos (por ej., cupones pagados en efectivo, montos de efectivo a través de ATM, billetera electrónica).

Tarjetas prepagas de marca en red de circuito abierto vendidas por minoristas con un límite recargable bajo que no requieren identificación. Este tipo de tarjeta prepaga es la que genera mayor preocupación.

- Compras múltiples de tarjetas prepagas que no requieren identificación, a pesar de que las tarifas son más altas que las de una tarjeta prepaga con un umbral más alto pero que requiere identificación.
- Compra de tarjetas prepagas múltiples en casas de cambio durante el cambio de divisas.
- Depósitos de efectivo numerosos a una tarjeta de débito prepaga recargable por parte de sujetos identificados con cargos relacionados con el terrorismo.

Caso de estudio: **Uso de tarjeta prepaga antes de los ataques**

Se usó una tarjeta prepaga recargable de circuito abierto, gestionada por una institución financiera, en varios países europeos para extracciones en efectivo y gastos pequeños relacionados con viajes: compra de billetes de avión, reserva de habitaciones de hotel, alquiler de autos, pago de combustible, pago de compras en áreas de servicio de autopistas. Las tarjetas prepagas también fueron utilizadas como garantía para el alquiler de un automóvil o reserva de una habitación de hotel. Las operaciones tentadas que excedían el monto cargado disponible en la tarjeta no podían ser vistas por el banco emisor, pero eran detectadas por la compañía administradora del gasto de la tarjeta. Esta compañía, establecida en el país D informó que la UIF del país D, la que a su vez informó a la UIF belga. Entonces fue posible desandar la ruta de los terroristas mediante el análisis de los pagos efectuados con la tarjeta prepaga. Las operaciones rechazadas también eran importantes para ubicar y comprender las rutas terroristas. La investigación mostró que los pagos efectuados con la tarjeta prepaga permitieron la provisión de apoyo logístico a los terroristas.

Fuente: Bélgica

Pagos móviles

Existe una amplia gama de servicios de pago móviles que ofrecen las instituciones financieras y operadores de redes móviles que se han asociado a fin de crear redes de agentes. Los puntos de venta minoristas de las operadoras de redes móviles y otras tiendas minoristas con negocios a la calle ofrecen servicios similares a aquellos que proveen las sucursales bancarias con propósitos limitados (por ej. toma de depósitos y pago en efectivo para saldar operaciones de pago móviles).

- Transferencia transfronteriza de efectivo a jurisdicciones/regiones de alto riesgo.
- Teléfono celular adquirido solo para ser utilizado para pagos móviles y no con fines de comunicación.
- Registración de un teléfono móvil desechable con el proveedor de servicios de pagos móviles.
- Utilización de tarjeta telefónica con valor almacenado abonada en efectivo (particularmente cuando no es necesaria la identificación del cliente).
- El receptor puede solicitar la transferencia a su tarjeta con valor almacenado y retirar los fondos desde cualquier cajero automático.

Plataformas para recaudación de fondos por Internet

Las plataformas para recaudación de fondos pueden ser mal utilizadas con fines de financiamiento del terrorismo mediante la captación de fondos en Internet, ofreciendo múltiples métodos de pago a fin de enviar el dinero internacionalmente. Idealmente, cada individuo que se registra para recaudar fondos en una plataforma de recaudación podría ser verificado con las listas TFS y medios de fuente abierta tal como se menciona en la Sección II.A de este informe.

- Se reunieron importantes sumas provenientes de pocos participantes.
- Un pequeño proyecto que recolecta dinero de individuos relacionados en la vida real (por ejemplo, miembros de una organización local y pequeña sin fines de lucro, un barrio), a pesar de los altos aranceles que toman las plataformas de recaudación de fondos por Internet.
- Pagos recibidos de una jurisdicción/región de alto riesgo.
- Posible mal uso de una campaña para recaudar fondos con fines humanitarios.
- Los gerentes del proyecto utilizan cuentas bancarias sin un vínculo geográfico con el proyecto anunciado.
- Las plataformas para recaudación de fondos que tengan proyectos/fines relacionados con el extremismo violento o radicalismo.

Caso de estudio: **Mal uso de recolección de fondos con fines humanitarios a través de una plataforma para recaudación de fondos por Internet.**

Una organización sin fines de lucro recientemente creada, vinculada con un lugar de culto religioso en un pequeño barrio, creó una campaña para recaudar fondos con fines humanitarios relacionada con escuelas en el exterior *en una plataforma de micromecenazgo (crowfunding).* La mayoría de las donaciones fueron realizadas por pocas personas que viven en el barrio, presumiblemente en relación con la audiencia del lugar de culto. La tarifa del 5,5% que cobra la plataforma de recaudación de fondos, costosa para una pequeña organización sin fines de lucro, debería haber detenido el uso de dicha práctica para reunir dinero entre una audiencia ya establecida. Un individuo de la administración de la organización sin fines de lucro estaba sospechado de tener vínculos estrechos con FTF.

Fuente: Francia

F. INDICADORES RELEVANTES PARA ORGANISMOS SIN FINES DE LUCRO

Si bien no todas las organizaciones sin fines de lucro (NPO) son de alto riesgo y algunas pueden ser de riesgo bajo o directamente no representar ningún riesgo[7], la campaña internacional en curso contra el financiamiento del terrorismo ha identificado casos en los que las entidades terroristas tuvieron como objetivo a algunas organizaciones sin fines de lucro para acceder a los materiales y fondos de estas organizaciones sin fines de lucro y a fin explotar sus redes, abusando en forma intencional de la organización sin fines de lucro. Esta cuestión fue abordada por el GAFI en el *Informe sobre Riesgos Emergentes* de financiamiento del terrorismo pero fue tratada en forma integral en junio de 2014 en el informe del GAFI sobre Riesgo de abuso *terrorista en organizaciones sin fines de lucro.* El capítulo seis del informe del 2014 ofrece una serie completa de indicadores generales e indicadores más concentrados en el financiamiento del terrorismo. También se envió mucho material sobre indicadores de riesgo, específicamente para este proyecto. Los indicadores de muestra recientemente recibidos se pueden clasificar en cuatro categorías generales asociadas con Donaciones, Gastos, Operaciones y Ejecutivos de la Organización sin Fines de Lucro.

[7] Ver *Mejores prácticas sobre la lucha contra el abuso de organizaciones sin fines de lucro* (GAFI, 2015c).

Tal como se indicó en el primer párrafo, en *I. E Uso de Indicadores*, no es objetivo de este informe ser usado como base para involucrarse en prácticas de eliminación del riesgo al por mayor o indiscriminadas. Como tal, los indicadores mencionados a continuación no deberían ser interpretados como una indicación de que las organizaciones benéficas establecidas o respetables, que trabajan en áreas geográficas con presencia de un grupo terrorista, ahora representan un riesgo mayor para las instituciones. Nuevamente, un solo indicador no puede garantizar por sí mismo la sospecha de financiamiento del terrorismo o brindar una indicación clara de dicha actividad. El GAFI recientemente ha actualizado su estándar respecto de las organizaciones sin fines de lucro a fin de garantizar que se encuentra en línea con un enfoque basado en el riesgo y no interrumpe o desalienta las actividades benéficas legítimas.

Donaciones

- Las donaciones significativas de una entidad extranjera o sociedad a la cuenta de una organización sin fines de lucro, especialmente cuando no existe una relación clara.
- La cantidad de pequeñas transferencias de baja denominación depositadas en una cuenta de una organización se ha incrementado sin una razón clara.
- Montos grandes acumulados y montos no justificados adecuadamente, especialmente si se realizaron principalmente en efectivo.
- Múltiples depósitos en efectivo a una cuenta personal (o una condición que establece que el efectivo debe ser transferido a un individuo de un país de alto riesgo) descriptos como "donaciones" o "contribuciones de ayuda humanitaria" o términos similares.
- Alto porcentaje de donaciones/activos a una organización sin fines de lucro provenientes de o que van hacia estados extranjeros que no corresponden con la ubicación financiera del donante.
- Montos altos de donaciones provenientes de un individuo ficticio a una organización sin fines de lucro.
- Un individuo recibe donaciones en una cuenta bancaria destinada a donaciones benéficas y transferencias de dinero a organizaciones que han sido vinculadas con el financiamiento del terrorismo a través de medios electrónicos.
- Donación a una organización sin fines de lucro destinada solo a unos pocos beneficiarios.
- Depósitos utilizando una combinación de instrumentos monetarios atípicos a una actividad comercial legítima.
- Las organizaciones sin fines de lucro que operan en áreas de conflicto reciben donaciones desde entidades corporativas (que tiene intereses comerciales en estas áreas) en sus cuentas en forma directa o a través de una serie de operaciones estructuradas. Dichos fondos podrían estar relacionados con organizaciones terroristas que chantajean a entidades corporativas a través de organizaciones sin fines de lucro.

Caso de estudio: **Desvío de Fondos por parte de Actores Internos de la Organización sin fines de lucro**

Un individuo (Sr. A) creó una fundación benéfica bajo el pretexto de reunir donaciones para los refugiados sirios, personas que necesitan ayuda médica y financiera y para la construcción de mezquitas, escuelas y jardines de infantes. Sin embargo, el Sr. A era el líder de una maniobra organizada en la que las donaciones eran enviadas a un grupo de individuos relacionados con el Sr. A (Grupo A) en vez de a la cuenta de la fundación. En la mayoría de los casos, la primera etapa involucró dinero que era enviado a través de remisoras y luego transportado en efectivo. El dinero era luego enviado ya sea a cuentas de tarjetas de créditos o a billeteras electrónicas. Los miembros del Grupo A colocaron la información relevante (que los fondos son recaudados para los propósitos declarados) en Internet, pero, de hecho, los fondos eran enviados como ayuda para los terroristas y sus familias y la intención era utilizarlos como apoyo financiero para las actividades terroristas.

Esta información fue descubierta a través de investigaciones realizadas por la UIF en base al monitoreo regular de entidades en sus listas nacionales de entidades terroristas designadas y personas relacionadas o en base a información provista por los organismos de seguridad. El análisis de la información reunida permitió a la UIF identificar la relación entre los diferentes casos: los pagadores y receptores comunes y un *modus operandi* similar para el cobro y distribución de los fondos. La cooperación adicional con los organismos de seguridad le permitió a la UIF establecer un vínculo directo entre el señor A y la actividad del EIIL. Esto resultó en varias investigaciones penales relacionadas con el Sr. A. Asimismo, el Sr. A se encontraba incluido en la lista nacional de entidades terroristas designadas, con los procedimientos de congelamiento pertinentes realizados. En virtud de decisiones judiciales, los activos de los miembros del Grupo A se congelaron.

Fuente: Federación Rusa (Informe del GAFI sobre Financiación de la Organización Terrorista Estado Islámico de Irak y el Levante (EIIL) (GAFI, 2015a).

Gastos

- Organizaciones que no tienen intenciones de suministrar beneficencia humanitaria, enviando dinero a jurisdicciones de alto riesgo.
- Uso poco claro de los fondos para gastos que no están vinculados con la actividad de una organización sin fines de lucro.
- Operaciones que manifiestan el propósito de construir una instalación para una organización sin fines de lucro, especialmente si el beneficiario es un individuo que parece no estar relacionado con el proyecto y no se lo puede vincular con un negocio de la construcción.
- Uso de organizaciones benéficas para vender mercadería.
- El pago de mercadería la realiza una tercera parte y no el importador.
- Los gastos "en papel" de la organización sin fines de lucro no es proporcionada a sus expectativas (por ejemplo, el riesgo de que los fondos sean malversados, se les de otro propósito, o estén sujetos a impuestos con fines de financiamiento del terrorismo).

Operaciones

- Las operaciones realizadas en la cuenta de una organización sin fines de lucro son inconsistentes con el patrón y tamaño del propósito o actividad de la organización.

- Operaciones llevadas a cabo por una organización sin fines de lucro que no se corresponden con la actividad declarada por el beneficiario/simpatizante.
- Operaciones caracterizadas por importantes flujos en un período corto y que involucran varias organizaciones sin fines de lucro que muestran vínculos injustificados, tales como compartir el mismo domicilio, representantes o empleados o múltiples cuentas con los mismos nombres recurrentes.
- Transferencia de la mayoría de los fondos recaudados a áreas geográficas habitualmente afectadas por actividades e iniciativas relacionadas con el financiamiento del terrorismo.
- Operaciones requeridas con contrapartes que han sido designadas en listas o que son entidades asociadas con actividades de financiamiento del terrorismo.
- Un individuo deposita fondos en varias cuentas (de su propiedad) y solicita una transferencia de fondos a sí mismo en el exterior con el fin de realizar donaciones.
- Una contribución en efectivo repetida pagada por personas físicas en la cuenta de una organización sin fines de lucro; luego, se transfiere el efectivo a cuentas de personas físicas o jurídicas.
- Solo las operaciones de crédito y en efectivo se realizan en la cuenta de la organización sin fines de lucro.

Ejecutivos de OSFL y otro personal

- Varios individuos con facultad para firmar en una cuenta de un individuo, o una organización sin fines de lucro sin relaciones familiares o comerciales; cambios frecuentes de individuos con facultad para firmar en una cuenta de una organización sin fines de lucro.
- Cuentas que recibieron fondos de organizaciones sin fines de lucro recientemente fundadas y recaudadoras de fondos (las entidades pueden haber cambiado/actualizado su identidad recientemente).
- Se realizan órdenes de pago importantes a las cuentas de los fundadores de la organización sin fines de lucro (u otros individuos conectados con la organización sin fines de lucro, tales como ejecutivos o tesoreros), se realizan operaciones en efectivo en las cuentas de los fundadores de la organización sin fines de lucro de manera constante.
- Los fondos financieros de la organización sin fines de lucro están situados en las cuentas de las personas físicas.
- Datos incompletos acerca del originante de operaciones a favor de una organización sin fines de lucro o a favor de individuos relacionados con la organización.
- Directores (o empleados) de una organización sin fines de lucros que se apropian indebidamente de fondos, tales como cuando los fondos se retiran antes de salir de una zona de conflicto.
- Las cuentas bancarias de los ejecutivos o contratistas, que operan en áreas de conflicto, podrían estar abonando extorsiones/rescates a las organizaciones terroristas en busca de su interés comercial o cobrar extorsiones en nombre de organizaciones terroristas.

G. INDICADORES RELEVANTES PARA EL COMERCIO Y ENTIDADES COMERCIALES

El rápido crecimiento en la economía global ha vuelto a las operaciones financieras asociadas con los bienes y servicios una vía cada vez más atractiva para el movimiento internacional de fondos ilícitos. El GAFI ha abordado las vulnerabilidades de las finanzas ilícitas asociadas con el comercio y las entidades comerciales en una cantidad de informes que incluyen: el Lavado de Activos mediante Operaciones Comerciales (TBML) en el año 2006 y 2012,[8] Financiamiento de la Proliferación en el año 2008[9] y las Zonas de Libre Comercio (FTZ) en el año 2010[10]. Algunos de estos informes han identificado indicadores de riesgo específicos ("alertas"). Si bien no todos están asociados con el financiamiento del terrorismo, algunos son relevantes para este informe y se han incluido.

Atento que los bancos más grandes generalmente ofrecen los tipos de productos y servicios financieros involucrados en el comercio nacional e internacional y en la actividad comercial, probablemente están más expuestos al financiamiento del terrorismo mediante operaciones comerciales. Los tipos de productos y servicios que pueden estar involucrados varían desde transferencias de pagos del importador al exportador a productos financieros sofisticados, tales como cartas de crédito, cobranza documentaria y garantías. El sector financiero también ofrece financiamiento a la exportación para salvar la distancia existente entre la necesidad de financiar la producción, el transporte, etc. y el pago por dichos productos por parte del importador. Los bancos y otras agencias de créditos a la exportación proveen préstamos y crédito a los comerciantes a fin de permitirles la adquisición y reventa de bienes o equipos. Todas las instituciones financieras involucradas en el financiamiento del comercio, sin importar su línea de negocios, cuentan con incentivos comerciales y obligaciones legales para realizar la DDC y el potencial monitoreo de la cuenta. Tanto la naturaleza y exhaustividad de la DDC realizada y cómo está organizada, pueden variar en forma significativa entre las instituciones financieras, de operación a operación y en base a las reglamentaciones en la jurisdicción local. Los indicadores de riesgo relacionados con el comercio pueden incluir:

- Personas físicas involucradas en el comercio y la producción de bienes y tecnología sujetas a la designación o a TFS a nivel nacional o global.
- Relación comercial establecida por personas jurídicas o físicas que podrían estar conectadas con una organización terrorista.
- Brevemente después de la designación, se registra una compañía relacionada y se abre una nueva cuenta.
- Gran cantidad de personas autorizadas a realizar operaciones en nombre de la persona jurídica u organización.
- Transferencias de dinero a jurisdicciones de alto riesgo inmediatamente después de la creación de una entidad legal cuando no se ha establecido una relación comercial.
- Actividades comerciales que emplean dinero en efectivo mediante el uso de MVTS para las operaciones en vez de transferencia electrónicas.
- Actividad operacional entre individuos o entidades con compañías recientemente establecidas sin aparente relación comercial o

[8] *Lavado de activos mediante operaciones comerciales* (APG, 2012)

[9] *Informe de tipologías sobre financiamiento de proliferación* (GAFI, 2008)

[10] *Vulnerabilidades de lavado de activos de las zonas de libre comercio* (GAFI, 2010)

compañías que aparentemente no están operativas (por ejemplo actividad genérica de importación-exportación, sin sitio web, etc.).

- Numerosos cheques personales entrantes depositados en las cuentas comerciales sin aparente propósito legítimo.
- Agencias de viaje que facilitan peregrinajes religiosos a destinos en jurisdicciones de alto riesgo y con un costo promedio ofrecido significativamente menor al precio de otras agencias de viajes.
- Pago por entrega de bienes incompatible con el nivel de servicio o estructura geográfica del país al que se envían los bienes.
- El comprador (persona física) de los bienes reside en un lugar, que se encuentra en un país distinto al del receptor final de los bienes ordenados.
- La línea de negocios registrada de la persona jurídica no se compadece con su actividad comercial real, o el beneficiario real de los bienes ordenados no aparece como beneficiario final.
- Numerosas transferencias de dinero entrantes en las cuentas comerciales sin aparente propósito legítimo.
- Repentino incremento de las operaciones en una cuenta bancaria profesional de un MVTS.
- Entidades comerciales con negocios en áreas de alto riesgo que operan con mercadería que podría ser considerada de uso dual o que podría ser utilizada en actividades terroristas.
- Entidades comerciales que realizan actividades comerciales en áreas de alto riesgo que pueden ser vulnerables al abuso o coacción (por ejemplo, pagos a cambio del acceso a puertos y áreas comerciales controladas por grupos terroristas).
- Inversión en compañías de transporte, que permiten el uso intensivo de efectivo, que operan en rutas y zonas vinculadas con actividades ilícitas.
- Inversión de fondos en la creación/operación de compañías que venden/compran vehículos en zonas de conflicto de alto riesgo.
- Volumen comercial inusual en los sectores de empleo de dinero en efectivo localizados en áreas fronterizas con las zonas de conflicto.

Caso de estudio: **Financiamiento del terrorismo mediante operaciones comerciales**

Con posterioridad a la designación de la compañía A como una asociación no autorizada en Israel, la compañía no podía importar bienes a través de los puertos israelíes. A pesar de estas restricciones, la compañía B, una compañía local que importa y comercializa productos alimenticios básicos, cooperó con la compañía A para sortear estas limitaciones. La compañía B primero importó mercaderías hacia Israel y luego un cómplice, la compañía C, liberó los bienes en el puerto y los almacenó. Luego, la compañía B transfirió la mercadería a la compañía A en un territorio de alto riesgo de financiamiento del terrorismo. Como parte del pago de las cuentas, la compañía A transfirió los fondos desde sus cuentas a la compañía B. El valor de la mercadería y las transferencias estaba estimado en varios millones en los nuevos siclos israelíes (NIS).

Fuente: Israel (Riesgos Emergentes de Financiamiento del Terrorismo (FATF, 2015))

Caso de estudio: **Comercialización de mercaderías contrabandeadas con fines de financiamiento del terrorismo**

Se detectaron algunas inconsistencias en la factura comercial que incluían el hecho de que el comprador tuviera un nombre diferente comparado con la transferencia electrónica beneficiaria, que era una empresa transportadora y que podría no ser el receptor final de dichas mercaderías. Asimismo, mientras que el propósito declarado era que la transferencia era por mercadería alimenticia, la factura mencionaba a una empresa de equipamientos médicos, sin consignar un domicilio de entrega. La información proveniente de los organismos de seguridad reveló un nexo entre la compañía de equipamiento médico y una organización terrorista.

Fuente: Francia

Comercio ilegal de antigüedades/patrimonio cultural

La Resolución del Consejo de Seguridad de las Naciones Unidas (RCSNU) 2199 impone una moratoria global respecto del comercio de objetos culturales provenientes de Siria (desde el 15 de marzo de 2011) y de Irak (desde el 6 de agosto de 1990). Tal como se mencionó en el *Informe del Secretario General sobre la amenaza que representa el EIIL (Da'esh) a la paz y seguridad internacional y la gama de iniciativas de las Naciones Unidas en apoyo a los Estados Miembros para contrarrestar la amenaza*, en vista de la escala del saqueo y su significativo valor económico, es probable que las redes delictivas estén almacenando numerosos artículos. Una vez que la atención disminuya, los individuos y grupos involucrados en las redes transnacionales delictivas comenzarán a introducir otros artículos lavados en el mercado.

El EIIL parece beneficiarse principalmente de este comercio ilícito en las etapas preliminares fundamentalmente mediante la venta de permisos de excavación a los ciudadanos y contratistas locales, como así también gravando la venta de monedas, pequeñas esculturas, alfarería y mosaicos que los ciudadanos y contratistas locales obtienen mediante excavación, y cobrando un impuesto a las antigüedades contrabandeadas fuera de su territorio. Las Naciones Unidas destacan que mientras que los márgenes de ganancias para las antigüedades saqueadas en el primer punto de venta son potencialmente pequeños, resulta necesario que se comercialicen volúmenes significativos de antigüedades si se quieren generar fondos significativos[11]. Se está realizando un acercamiento a los organismos de seguridad, los comerciantes de arte, las casas de subastas, los museos y el mercado de antigüedades a fin de alentar una mayor vigilancia para rastrear y detener la venta de artefactos culturales saqueados y vendidos, pero no resulta claro cómo afectaron al sector financiero formal las operaciones relacionadas. Toda operación financiera que se relacione con bienes culturales que se podrían haber originado en Siria, Irak o Libia debería estar sujeta a

[11] *Desafíos que enfrentan las entidades comerciales en la implementación de la resolución 2199 del Consejo de Seguridad (2015)*. (RSNU, 2016).

un escrutinio detallado y medidas de prevención. Las jurisdicciones también se encuentran bajo la obligación de informar la interdicción en su territorio de antigüedades transferidas hacia o desde el EIIL (ver párrafo 15 de la RCSNU 2253 (2015) y el párrafo 12 de la RCSN 2199 (2015)).

- Operaciones financieras en relación con bienes culturales similares a aquellos mencionados en la RCSN 2199 y por el Consejo Internacional de Museos (ICOM) en la Lista Roja de Emergencias de Antigüedades Iraquíes en Riesgo (2003), la Lista Roja de Emergencia de Objetos Culturales Sirios en Riesgo (2013) y la Lista Roja de Emergencia de Objetos Culturales Libios en Riesgo (2015).
- Operaciones financieras relacionadas con antigüedades provenientes de Irak y Siria (incluidas pequeñas piezas, tales como monedas y estatuillas) que se ponen a la venta en Internet y redes sociales.
- Operaciones financieras relacionadas con envíos de equipos de control/escaneo subterráneo, tales como detectores de metales utilizados por los saqueadores para excavar artefactos antiguos y objetos culturales.
- Declaraciones de importación falsas que manifiestan que los artefactos se originan en países fronterizos con Siria e Irak.

Industria del petróleo y del gas

Los aportes de las partes interesadas y el sector privado indicaron la solicitud de indicadores específicamente relacionados con el EIIL. Mientras que muchos de los indicadores en este documento están relacionados con las amenazas específicas asociadas con el EIIL, esta sección se concentra específicamente en aquellos indicadores asociados con la producción de petróleo y operaciones de refinería, que incluyen la compra, envío o comercialización de equipos de perforación petrolera y refinería.

La RCSN 2199 requiere a todos los estados que prevengan todo comercio directo o indirecto de petróleo o productos derivados del petróleo, refinerías modulares y material conexo con el EIIL. La RCSN 2199 también enfatiza que todos los estados deben congelar los activos relacionados con grupos del EIIL, como así también con aquellos de personas, agrupaciones, empresas y entidades asociadas, incluido su petróleo, productos derivados del petróleo, refinerías modulares y material conexo. Las instituciones deberían, por lo tanto, estar al tanto de los tipos generales de equipamientos y repuestos de perforación y refinería de la industria de los hidrocarburos que el EIIL pudiera estar interesado en adquirir. Algunos indicadores que pueden ser relevantes incluyen:

- Conexiones financieras con empresas, agentes, proveedores de repuestos petroleros ubicados en áreas de alto riesgo.
- Individuos o entidades que repentinamente compran y/o envían equipos petroleros a Siria, Irak o estados fronterizos, cuando la actividad no es consistente con la línea comercial del cliente.
- Empresas pantalla utilizadas para disimular el comercio y venta de productos derivados del petróleo y repuestos relacionados con el petróleo.
- Operación que involucra posibles empresas pantallas (por ejemplo, empresas que no tienen un alto nivel de capitalización o muestran otros indicadores de empresas pantalla).
- Se consigna a una empresa de fletes como el destino final del producto.

- Las instrucciones de la transferencia o pago desde o debido a partes no identificadas en la carta de crédito original u otra documentación.
- Un cliente nuevo solicita una operación de carta de crédito que espera la aprobación de una nueva cuenta.
- La operación involucra el uso de cartas de crédito modificadas repetidamente o frecuentemente extendidas.

A fin de limitar la capacidad del EIIL de beneficiarse financieramente del petróleo producido en sus territorios, el CFIG ha colaborado con la industria internacional del petróleo para crear una lista ilustrativa del equipamiento de perforación y refinería petrolera[12], que el EIIL probablemente podría necesitar para continuar con su producción de petróleo y operaciones de refinería. Esta lista puede ser utilizada para identificar el equipamiento y prevenir el envío o trasbordo de equipamiento de perforación y refinería y material relacionado al territorio controlado por el EIIL. Esta lista puede compartirse con los representantes de la industria petrolera, las compañías de logística, las autoridades de control transfronterizo y los productores de equipamiento de perforación y refinería petrolera. La lista podría ser igualmente beneficiosa para los grandes bancos corporativos y el sector financiero que se dedica al financiamiento del comercio.

[12] *Lista ilustrativa de equipos de perforación y refinería de petróleo* (Depart. De Estado, EE. UU., 2016)

III. COMPARTIR INFORMACIÓN CONTEXTUAL PARA MEJORAR LOS INDICADORES DE RIESGO

Si bien los indicadores de riesgo son una herramienta útil, no son un substituto para las relaciones estrechas entre el sector privado y público para intercambiar información sobre riesgos de financiamiento del terrorismo. Los estándares del GAFI requieren que los países desarrollen marcos legales y operativos fuertes para informar al sector privado acerca de los riesgos de LA/FT y para garantizar que el sector privado tome en cuenta el riesgo de LA/FT en el curso de sus negocios. El informe sobre *Riesgos Emergentes de Financiamiento del Terrorismo* del GAFI resaltó la necesidad de combinar los datos provenientes de los sujetos obligados con la información contextual y sanitizada proveniente de las autoridades. Dada la urgencia y la naturaleza urgente de estas cuestiones, la capacidad de compartir información relacionada con el financiamiento del terrorismo en forma rápida y segura es esencial. Esta sección se centra solo en los mecanismos nacionales para mejorar el intercambio de información entre el sector público y privado a fin de mejorar los indicadores de riesgo.

En respuesta a los riesgos actuales de FT, el GAFI está realizando un amplio trabajo sobre el intercambio de información dentro y entre el sector público y privado. Consultas sobre este informe revelaron una serie de pasos útiles para mejorar la colaboración público-privada y los esfuerzos conjuntos a fin de identificar y comunicar riesgos y desarrollar indicadores de riesgos. Esta sección ofrece una evaluación preliminar de estas herramientas.

Quienes respondieron también destacaron una serie de factores que previenen o restringen el intercambio efectivo de información en el contexto del financiamiento del terrorismo tanto a nivel nacional como multilateral. El terrorismo y la información de FT, por su naturaleza, es altamente sensible y necesita protección incluso entre las autoridades competentes. La falta de confianza entre las autoridades competentes y el sector privado puede inhibir el intercambio de datos sensibles. El sector público tiene la dificultad de equilibrar la confidencialidad de la información operativa sensible y concienciar respecto de los riesgos de FT con los actores interesados. Deberían desarrollarse relaciones para aprovechar las habilidades de ambos lados mediante la creación de una comunidad de expertos que pueda mejorar dichas capacidades. La comunicación debe ser un proceso continuo ya que el sector privado necesita tener una comprensión precisa del entorno de riesgo en constante cambio.

A. OBSERVACIONES A SUJETOS OBLIGADOS

Los indicadores de riesgo asisten al sector privado (y a las UIF) en la identificación de determinados comportamientos sospechosos que pueden estar relacionados con el FT. Sin embargo, el sector privado siempre está buscando una guía más fuerte y oportuna y las observaciones del sector público respecto de la calidad y utilidad de sus reportes de operaciones sospechosas (ROS) a fin de mejorar su identificación y métodos de análisis. La orientación, las observaciones o el acercamiento tienen un elemento muy táctico en sí atento que ofrecen a los sujetos obligados información significativa o "específica" con el propósito explícito de ayudar al sector privado a brindar un mejor reporte de actividad sospechosa. Este ciclo (o "circuito de comentarios") finalmente conduce incluso a un mejor acercamiento por parte de las autoridades competentes hacia los sujetos obligados, que a su vez mejora la presentación de reportes.

La revisión y las observaciones a las autoridades públicas, cuando es posible, sobre los borradores de perfiles de riesgo e indicadores del sector privado antes de su emisión le resultan útil al sector privado para tener un producto más efectivo.

Caso de estudio: **Los Países Bajos**

Los Países Bajos ofrecen un ejemplo acerca de cómo sus autoridades prueban indicadores con el sector privado para evaluar su viabilidad y utilidad. Se refinan los borradores de perfiles de riesgo en base a los resultados preliminares suministrados por los sujetos obligados. Una vez finalizados, la autoridad competente comunica los perfiles de riesgo a los sujetos obligados en forma de guía. En este caso, la guía y los comentarios continuos mejoran la efectividad del desarrollo de los indicadores de FT.

Caso de estudio: **Australia**

Australia suministró un ejemplo acerca de cómo ofrece orientación y comentarios sobre los ROS a una serie de actores clave en forma periódica. En forma trimestral, la UIF y los organismos de seguridad se reunirán con los cuatro bancos más importantes para debatir cuestiones de cumplimiento y comentarios sobre los ROS. Estos encuentros han resultado en un incremento del 300% de los reportes de operaciones sospechosas.

B. TIPO DE INFORMACIÓN COMPARTIDA

Cuando brindó comentarios preliminares sobre este informe, el sector privado enfatizó que los indicadores de riesgo son útiles pero que necesitan estar acompañados por información contextual detallada. Si bien es difícil compartir esta información en este informe, los participantes identificaron una serie de modos en los que las autoridades pueden ofrecer al sector privado la información que necesitan, a través de un acercamiento general y orientado, sin comprometer la confidencialidad de la información.

Las autoridades deben comprender en forma apropiada qué tipos de información e inteligencia son de valor para el sector privado en la identificación de la actividad terrorista. Las respuestas indican que la mayoría de las autoridades competentes puede ofrecer a los sujetos obligados casos de estudio sanitizados y tipologías sobre FT y que no existen barreras legales respecto de este tipo de datos. Este tipo de información generalmente es producida por la UIF en la forma de un informe anual, boletín informativo o boletín electrónico. A menudo, se pueden compartir versiones más detalladas de casos de estudio con entidades específicas a través de los canales apropiados.

Las Evaluaciones Nacionales de Riesgo son otro mecanismo útil para comunicar el estudio de casos y tipologías. Estas evaluaciones son útiles para involucrarse con el sector privado en una etapa inicial y para aumentar la conciencia sobre los riesgos específicos. Un desafío identificado implica a aquellos países que no cuentan con estudio de casos o tipologías relacionadas con el FT en su propia jurisdicción, y que pueden ofrecer solo estudios de casos relativos a otra jurisdicción.

El sector privado por lo general busca asistencia e información contextual más detallada proveniente del sector público, la cual puede ser sensible, para ayudar a interpretar los datos con los que cuentan. Algunas entidades del sector privado han destacado la importancia de recibir un listado de individuos relevantes (es decir, personas que se encuentran siendo monitoreadas, vigiladas o investigadas) de las autoridades competentes. Estos enfoques basados en las listas pueden ayudar a identificar operaciones específicas y a detectar la red de sujetos relacionados con aquellos listados. Sin embargo, compartir las listas de sujetos es un tema sensible ya que la preservación de la confidencialidad de las investigaciones y operaciones en curso es una prioridad para las autoridades de los organismos de seguridad. Algunos participantes del sector privado, particularmente aquellos con mucho volumen de datos, han enfatizado que incluso si no fuera

posible divulgar los detalles de los hechos de un caso, una indicación general del tipo de actividad que se lleva a cabo puede asistirlos para suministrar inteligencia financiera adicional.

El sector privado puede mantener datos acerca de un cliente con fines de DDC tales como domicilios de Protocolos de Internet (IP), números de teléfonos móviles y datos de geolocalización. En combinación con la información proveniente de las autoridades competentes, dicha información de DDC puede resultar útil para la identificación de actividad de FT potencial. Las autoridades competentes han señalado a países en particular que pueden representar un mayor riesgo de financiamiento del terrorismo o han identificado ciertos negocios que pueden representar un mayor riesgo de seguridad. Por ejemplo, los organismos de seguridad han compartido información acerca de determinadas ciudades o barrios donde están viviendo conocidos intermediarios y facilitadores para los FTF. En algunos casos, las autoridades ofrecerán un análisis de datos detallado sobre áreas geográficas relativas a fronteras, logística o áreas de tránsito. En otros casos, los organismos de seguridad han compartido información financiera que obtienen de grandes incautaciones (por ejemplo, conocimientos de embargo, recibos, etc.) a bancos, que la utilizan para verificarla en los registros de su sistema para identificar cualquier operación sospechosa relevante.

La información relativa a incidentes en tiempo real debería ser más detallada y más específica para permitir que el sector privado adopte acciones inmediatas. Sin embargo, tal como se mencionó arriba, la información relativa a individuos y eventos específicos generalmente está sujeta a restricciones. Estos desafíos prácticos existen con respecto a las investigaciones en curso o activas de terrorismo o financiamiento del terrorismo. En estos casos, generalmente es difícil compartir información, incluso a través de un caso de estudio sanitizado. Las autoridades y entidades no pueden, por lo tanto, actuar de buena fe debido a las restricciones legales, protección de la privacidad y cuestiones relativas a la responsabilidad. El establecimiento de excepciones o protocolos podría permitir a las autoridades compartir información con el sector privado, si se necesita en forma urgente, cuando se esté desarrollando un incidente de la vida real donde hay, o podría haber, muertes.

Caso de estudio: **Estados Unidos**

Las regulaciones de Financial Crimes Enforcement Network (FinCEN) de Estados Unidos bajo el Artículo 314(a) de la Ley PATRIOTA DE ESTADOS UNIDOS permiten a FinCEN comunicarse con más de 43.000 puntos de contacto en más de 22.000 instituciones financieras para localizar cuentas y operaciones de personas que puedan estar involucradas en terrorismo o lavado de activos. FinCEN realiza estos requerimientos para fines propios de análisis e investigación y en nombre de organismos de seguridad federales, estaduales, locales y algunos del extranjero (por ej., la Unión Europea). El Artículo 314(a) brinda información indicativa solamente (inteligencia financiera) y no es sustituto de una citación u otro proceso legal, utilizado generalmente después de la identificación de información relevante para obtener la información con otros fines de investigación o probatorios.

A través de un sistema de comunicación expeditivo, el proceso del Artículo 314 de FinCEN permite a un investigador brindar información indicativa sensible directamente a los sujetos obligados. FinCEN brinda un sistema de correos electrónicos seguro para diseminar esta información confidencial. Según la información inicial provista por las instituciones financieras, el foco de investigación rápidamente apunta directamente a otras ubicaciones y actividades relevantes. Además, FinCEN organizará y realizará debates de intercambio de información con las instituciones financieras adecuadas para emitir solicitudes de información de conformidad con el Artículo 314(a). Esta sociedad de cooperación entre la comunidad financiera y los organismos de seguridad permite disparar información a ser identificada, centralizada y rápidamente evaluada.

El sector privado considera que la orientación, los asesoramientos y las notificaciones específicos y orientados son el tipo de información más útil. Estos asesoramientos a veces se envían a través de canales seguros, dependiendo de la confidencialidad de los datos. Brindan información contextual sólida sobre la actividad de FT orientada, se focalizan al sector privado en las áreas de riesgo y explican no solo los indicadores potenciales de la actividad sino también cómo puede el sector privado encontrarse con ellos dentro de sus operaciones. En algunos casos, esta orientación incluirá una lista de personas físicas o personas jurídicas de alto riesgo asociadas con la actividad. Sin embargo, para que esa información sea de mayor utilidad para el sector privado, las autoridades del sector público deberían incluir información específica, datos personales (nombre, fecha de nacimiento) de estas personas/entidades de alto riesgo. Las sanciones financieras específicas nacionales e internacionales contra personas y entidades deberían enviarse en forma proactiva a instituciones financieras, ligeramente antes de la publicación oficial para garantizar un mejor monitoreo y el desbaratamiento de cualquier intento de movimiento de fondos antes del proceso de congelamiento.

Caso de estudio: **Federación Rusa**

La UIF rusa (Rosfinmonitoring) desarrolló un conjunto de indicadores CFT de múltiples capas para las instituciones financieras rusas. Estos indicadores se dividen en tres grupos:

1) Una característica regional (vincular la operación a un área específica);
2) Criterios de iniciación;
3) Criterios de soporte (auxiliares).

Para ayudar en la identificación de un territorio específico como la zona de mayor amenaza terrorista, uno debería usar información oficial disponible, publicada por organismos internacionales (intergubernamentales), incluyendo asociaciones de UIF. Las operaciones cubiertas por los indicadores del Grupo 1 se definen como de iniciación, es decir, operaciones sujetas a estudio junto con la consideración de las operaciones de soporte (auxiliares), que están cubiertos por los indicadores del Grupo 2.

Algunos indicadores luego se desarrollan como temas tales como:

Los indicadores de FTF se dividen a su vez en dos categorías:

- indicadores de categoría externa que reflejan un modelo de comportamiento y las características específicas de las operaciones con fondos realizadas por los FTF en las áreas de alto riesgo; y
- indicadores de categoría interna que reflejan el modelo de comportamiento y los detalles específicos de las operaciones con fondos realizadas por los FTF dentro de su área de origen.

Los indicadores respecto a "centros radicales" y "estructuras comerciales" consisten en las categorías de indicadores de "iniciación" y "suporte" (auxiliares). Como resultado, se debe observar que el uso de un conjunto de indicadores de múltiples capas permite a las instituciones de crédito y a las UIF evitar "interferencias" innecesarias (datos irrelevantes) en las operaciones reportadas y focalizarse en grupos específicos de operaciones de los sospechosos de estar relacionados con el financiamiento del terrorismo.

C. MECANISMOS PARA INVOLUCRARSE CON EL SECTOR PRIVADO

Los participantes de este proyecto subrayaron la importancia de una relación de ida y vuelta entre los sectores público y privado. Las autoridades desarrollaron una variedad de mecanismos para facilitarlo. Estos mecanismos pueden incluir reuniones formales y reuniones informativas informales, tanto entre dos entidades como con entidades múltiples. La mayoría de los países indicaron que realizan al menos un foro o seminario por año con el sector privado para tratar riesgos y tendencias de FT. El énfasis de estas reuniones difiere dependiendo de la autoridad competente involucrada (por ej., organismo de seguridad, UIF o supervisor). Independientemente de la autoridad que lo organiza, generalmente se incluye a las entidades operativas como los organismos de aplicación de la ley y de seguridad para brindar ejemplos prácticos o información específica sobre riesgos. En otros casos, se realizan seminarios de riesgo de FT como parte de las conferencias, los seminarios y la capacitación de sujetos obligados. Además, esta participación puede ocurrir como iniciativa del sector privado y no del gobierno para permitir una discusión más expansiva de la actividad potencial de FT.

Las reuniones "mano a mano" periódicas y oportunas con interesados seleccionados y acreditados por la seguridad son un mecanismo útil para discutir observaciones específicas. Las autoridades competentes (especialmente la UIF o los organismos de seguridad) generalmente pueden brindar observaciones sobre si la sospecha reportada tiene fundamentos o no mediante la provisión de ejemplos sobre cómo usaron finalmente esta información las autoridades garantes del cumplimiento de la ley y judiciales. Quienes respondieron también observaron que al brindar observaciones específicas, las autoridades garantes del cumplimiento de la ley u otras autoridades deberían intentar reunirse directamente con los oficiales de cumplimiento y con los empleados responsables de identificar actividades sospechosas relacionadas con el financiamiento del terrorismo. Generalmente, las autoridades pueden discutir el contenido de un ROS con el sujeto obligado. Esto permite a los sujetos obligados entender mejor sus sistemas de monitoreo de riesgo y determinar si se necesita realizar ajustes. Como se observó más arriba, las observaciones pueden ser inhibidas debido a la existencia de información confidencial con respecto a investigaciones relacionadas con terroristas.

La comunicación puede ocurrir bajo el auspicio de protecciones legales establecidas, foros protegidos o acuerdos de confidencialidad suscritos. Las jurisdicciones indicaron que un mecanismo efectivo para promover el intercambio efectivo de datos sensibles o de seguridad nacional es que los empleados clave del sector privado estén autorizados y aprobados para recibir dicha información. En estos casos, las agencias de cumplimiento de la ley, de seguridad o de inteligencia mantendrán reuniones mano a mano con compañías seleccionadas en el sector financiero donde los empleados clave tengan aprobación para los fines de la reunión. Entonces, se comparte información sensible o clasificada relacionada con el FT, incluyendo casos activos. Otra manera es tener foros de discusión con protección legal donde todas las autoridades competentes relevantes del sector público y privado puedan abordar tendencias, casos y problemas de FT en forma confidencial pero no clasificada.

En algunos casos, se han establecido grupos de trabajo de FT específicos entre el sector público y privado. Entre los ejemplos se encuentra el Grupo de Inteligencia Conjunto sobre Lavado de Activos (JMLIT, Joint Money Laundering Intelligence Taskforce)[13], el Foro de Periodistas Principales de Australia (Major Reporters Forum) y el Consejo de Alianza de Seguridad Nacional de Estados Unidos (DSAC) (Domestic Security Alliance Council)[14]. Estos tipos de grupos de trabajo brindan un foro para la colaboración operativa que es instrumental para mejorar las funciones de análisis e investigación de todas las partes involucradas.

[13] Joint Money Laundering Intelligence Taskforce (NCA, nd)

[14] www.dsac.gov

Suiza también brindó un ejemplo útil de dicha interacción, que involucra a otros participantes de otros sectores que no son sujetos obligados para promover una mejor discusión y comprensión de los riesgos.

Caso de estudio: **Egipto**

La Federación de Bancos Egipcios (FEB) se constituyó como una entidad independiente sin fines de lucro. La FEB conecta a todos los bancos egipcios y bancos extranjeros que trabajan en Egipto. Los objetivos de la FEB son discutir y compartir problemas comunes entre los miembros de la federación; esto, además de brindar opiniones sobre proyectos de ley y de sugerir modificaciones a legislación actual relacionada con el sector bancario.

En 2003, se creó una Asociación de Oficiales de Cumplimiento como iniciativa de la FEB. Todos los oficiales de cumplimiento de los bancos que operan en Egipto son miembros de esta asociación. Se llevan a cabo reuniones periódicas para discutir acerca de sugerencias o problemas con respecto a la lucha contra el FT y el LA. El Banco Central de Egipto y la UIF egipcia (EMLCU) generalmente son invitados para asistir a estas reuniones y brindar comentarios y asistencia técnica sobre los problemas que postulan los oficiales de cumplimiento.

Además, existe la necesidad de tener un mecanismo o proceso dentro de una jurisdicción para que el sector privado informe operaciones potenciales de FT o al menos aquellas que parecen indicar que puede ocurrir un acto de terrorismo en forma inminente a los servicios de aplicación de la ley/seguridad prácticamente en tiempo real. Esto presupone que la autoridad competente tiene el canal para recibir este tipo de información y puede actuar en consecuencia. Los ejemplos incluyen teléfonos de atención exclusivos.

IV. CONCLUSIONES

Este informe representa un avance significativo en la manera del GAFI de desarrollar indicadores de riesgo para ayudar a detectar actividades terroristas y de financiamiento del terrorismo. El informe reconoce que la detección de la actividad de financiamiento del terrorismo es un proceso plural y no puede apoyarse sobre indicadores solitarios e independientes que puedan introducirse en sistemas automatizados. El GAFI se involucró con una cantidad de entidades del sector privado para asegurarse de que este informe sea relevante y útil para ellos en su trabajo cotidiano, y para que pueda ser puesto en funcionamiento en línea con los métodos de los bancos y otras instituciones financieras. Este tipo de colaboración sirve como modelo para los esfuerzos futuros del GAFI en la identificación de los riesgos de lavado de activos o financiamiento del terrorismo.

Los indicadores de riesgo de financiamiento del terrorismo deberían tener en cuenta varias actividades de control, tal como:

- Monitoreo del nombre;
- Monitoreo de las operaciones;
- Monitoreo de los pagos, y
- Debida diligencia de comportamiento en el entorno de capacitación.

Estos indicadores deberían servir como aporte para las herramientas de minería y diagramación de datos, como así también disparar investigaciones adicionales.

Mientras que los indicadores identificados son amplios y están en continua evolución, se usan mejor cuando se aplica otra información contextual de fuentes públicas y de organismos de aplicación de la ley nacionales. Un abordaje basado en reglas no puede determinar riesgos de financiamiento del terrorismo, pero un abordaje basado en el riesgo puede ser implementado con un diálogo bidireccional dinámico entre las instituciones financieras y las autoridades públicas.

Mejorar el intercambio de información es un tema complejo a niveles nacional y multilateral. Este informe apunta a establecer mecanismos nacionales prácticos para mejorar el intercambio de información acerca de riesgos de terroristas y financiamiento del terrorismo a medida que se relacionan con los identificadores relacionados. La Sección III de este informe es solamente una pequeña porción del trabajo que planea hacer el GAFI sobre intercambio de información. Esperamos que este informe pueda ser utilizado en otras corrientes de trabajo a nivel internacional.

Este informe no persigue el fin de ser una herramienta de control de cumplimiento de la autoridad de supervisión. A nivel nacional, las autoridades competentes deberían aprovechar esta oportunidad para usar el informe como un catalizador para:

- Involucrarse con el sector privado,
- Implementar observaciones específicas sobre reportes de actividad sospechosa relacionada con el financiamiento del terrorismo y ayudar a las instituciones financieras a especificar sus procesos de monitoreo,
- Compartir información contextual sobre terrorismo y financiamiento del terrorismo que podría disparar la detección preventiva de terroristas potenciales.

Para evaluar la efectividad de este informe, el GAFI monitoreará cómo comunican las autoridades los indicadores y las medidas tomados para mejorar la sociedad con el sector privado sobre la base del uso de los indicadores de riesgo.

BIBLIOGRAFÍA Y REFERENCIAS

FATF (2015a) *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL),* FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html

FATF (2015b) *Emerging Terrorist Financing Risks,* FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

FATF (2015c), *Best Practices on Combating the Abuse of Non-Profit Organisations*, GAFI, París, www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html

FATF (2014), *Risk of terrorist abuse in non-profit organisations*, GAFI, París, www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html

FATF (2013a), *International Best Practices on Targeted Financial Sanctions for Terrorist Financing*, GAFI, París, www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-finsanctions-tf-r6.html

FATF (2013b) *The role of Hawala and other similar service providers in money laundering and* terrorist financing, GAFI, París, www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html

FATF (2013c) *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, GAFI, París, www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html

FATF (2011) *Organised Maritime Piracy and Related Kidnapping for Ransom*, GAFI, París, www.fatf-gafi.org/publications/methodsandtrends/documents/organisedmaritimepiracyandrelatedkidnappingforransom.html

FATF (2010) *Money laundering vulnerabilities of Free Trade Zones*, GAFI, París, www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingvulnerabilitiesoffreetradezones.html

FATF (2008) *Typologies report on Proliferation Financing*, GAFI, París, www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

FATF (2002) *Guidance for Financial Institutions in Detecting Terrorist Financing*, GAFI, París, www.fatf-gafi.org/publications/fatfrecommendations/documents/guidanceforfinancialinstitutionsindetectingterroristfinancing.html

APG (2012) *Trade-based money laundering*, APG, Sydney, www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaunderingtypologies.html

NCA (nd) *Joint Money Laundering Intelligence Taskforce*, National Crime Agency, Londres www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit, accedido en mayo 2016.

UNSC (2016) *Challenges business entities face in implementing Security Council resolution 2199 (2015),* Consejo de Seguridad de Naciones Unidas, Nueva York, https://www.un.org/sc/suborg/en/sanctions/1267/monitoring-team/reports. Ver Documento S/2016/213.(UN SC, 2016)

UNSC (nd) *Consolidated United Nations Security Council Sanctions List*, Consejo de Seguridad de Naciones Unidas, Nueva York https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

US DOS (2016) *Illustrative List of Oil Drilling and Refinery Equipment*, Departamento de Estado de EE. UU., Washington, www.state.gov/e/enr/c71196.htm

FATF

www.fatf-gafi.org

junio de 2016

Detección del financiamiento del terrorismo: *Indicadores de riesgo relevantes*

El GAFI desarrolló los indicadores en este informe para ayudar a los organismos gubernamentales y a entidades seleccionadas del sector privado a detectar y desbaratar los flujos financieros de terroristas y organizaciones terroristas. El GAFI decidió no distribuir este informe en forma pública, para preservar la utilidad de estos indicadores y otra información relevante.

Las autoridades nacionales competentes serán responsables de comunicar este informe a las entidades relevantes del sector privado en su país. Los destinatarios de este informe deben mantener esta información en secreto y no duplicar, compartir o comunicarla de otra manera a terceros, sin la autorización previa de sus autoridades nacionales competentes.