ECOFEL

EGMONT CENTRE OF FIU
EXCELLENCE & LEADERSHIP

2021

Antecedentes y Finalidad sobre la obligación de Presentar

REPORTES DE OPERACIONES SOSPECHOSAS

Capacitación brindada por ECOFEL

23 y 24 de agosto 2021

El Centro Egmont de Excelencia y Liderazgo de FIU (ECOFEL) realizó el taller regional en línea de las Américas titulado ***"Mejora de la calidad de STR / SAR"***.

El taller en línea se llevó a cabo el lunes 23 y el martes 24 de agosto de 2021, de 10:00 a 12:00 EDT.

Este taller es el tercero de una serie de talleres regionales sobre este tema. A través de estos eventos, el ECOFEL tiene como objetivos:

- **Mejorar el conocimiento de los participantes con respecto a las fortalezas y los impedimentos para la notificación efectiva de transacciones sospechosas.**
- **Cubrir las mejores prácticas y los próximos pasos para mejorar la calidad de STR / SAR**
- **Aumentar las oportunidades de asociaciones de colaboración entre las UIF y las entidades informantes sobre la presentación de informes financieros de investigación.**

Exposición por Mariano Federici

Antecedentes y Finalidad de la Obligación de Presentar ROS

Desde el principio, la estrategia global antilavado de activos y contra la financiación del terrorismo (ALA/CFT) situó al sector privado como un actor fundamental en la lucha contra el LA y el FT.

Las operaciones financieras tienen lugar en el mercado

La libertad de actuación conlleva la responsabilidad de cooperar

El sector privado es el mejor situado para conocer a sus clientes, supervisar las operaciones y detectar sospechas

Base jurídica en el derecho internacional

La Convención de Viena sólo se refería al deber de los países de establecer y mantener canales de comunicación para facilitar el intercambio rápido y seguro de información en relación con los delitos tipificados (incluido el LA).

La Convención de NY sobre CFT de 1999 se refería a la necesidad de que los países prestarán especial atención a las operaciones inusuales o sospechosas y notificarán las operaciones sospechosas. Sin embargo, no se hacía referencia a las UIF.

La Convención de Palermo de 2000 contra la delincuencia organizada transnacional se refirió a la necesidad de que los países establecieran un marco normativo que hiciera hincapié en la necesidad de que las instituciones financieras informaran sobre las operaciones sospechosas. También solicitó a los países que consideraran la posibilidad de establecer una agencia de inteligencia financiera capaz de actuar como centro de recepción, análisis y difusión de información relacionada con el LA.

La Convención de Mérida de 2003 contra la corrupción repitió la fórmula de la Convención de Palermo.

Los estándares originales del GAFI de 1990 no hacían referencia a las UIF, pero sí a las actividades sospechosas y al reporte, estableciendo las siguientes recomendaciones para los países:

Exigir a las IF que presten especial atención a las operaciones complejas e inusualmente grandes y a los patrones inusuales de operaciones sin propósito económico o legal aparente.

Exigir a las IF que documenten estos hallazgos y los mantengan a disposición de los supervisores, los auditores y las autoridades de orden público.

Implementar los ROS, pero dejando la opción de instituirlo como requisito obligatorio o voluntario.

Dado que el concepto de UIF no existía entonces, las normas recomendaban que los ROS se presentaran ante "una autoridad competente", dejando que cada país determinara a qué autoridad asignar dicha responsabilidad.

Establecer la protección legal de las IF que informan de buena fe y la obligación de no revelar (tipping-off).

En los casos en los que no había obligación de informar, se recomendó que FIs terminaran la relación con el cliente.

Establecer un mecanismo de intercambio de sospechas entre los países, ya sea de forma espontánea o a petición

Las enmiendas de 1996 al estándar de GAFI establecieron la obligación de informar con prontitud a las "autoridades competentes" y las notas interpretativas dispusieron lo siguiente:

Ese seguimiento de las operaciones por parte de una IF también tenía que referirse a las operaciones interbancarias o a las operaciones dentro de un grupo.

El término "operaciones" abarque también las operaciones en el sector de los seguros.

Las operaciones sospechosas deben comunicarse independientemente que puedan estar relacionadas con asuntos fiscales, teniendo en cuenta que los blanqueadores de dinero pueden utilizar la excusa fiscal.

Las normas del GAFI de 2003 (las 40+9 Recomendaciones), son el primer lugar donde el GAFI define lo que es una UIF (la única institución creada por el GAFI).

Las UIFs se definen como el centro nacional para la recepción, análisis y diseminación de ROS y otra información relacionada con el LA o el FT. La definición también establece que las UIFs deben tener acceso directo e indirecto a la información financiera, administrativa y policial de manera oportuna requerida para llevar a cabo sus funciones, incluyendo el análisis de los ROS.

Las obligaciones de control de las operaciones y de notificación de las ROS se mantuvieron con algunas variaciones.

La obligación de informar sobre los ROS.

La referencia a mantener la información disponible para los supervisores y las autoridades locales se sustituyó por la palabra "autoridades competentes" de forma más amplia.

Se recomendó que la obligación de informar fuera obligatoria.

Se eliminó la obligación de terminar la relación con el cliente al detectar una sospecha

La actual norma del GAFI establece la obligación de las IF de informar sobre los ROS en virtud de la Recomendación 20:

"Si una institución financiera sospecha o tiene motivos razonables para sospechar que los fondos son producto de una actividad delictiva, o están relacionados con la financiación del terrorismo, debería estar obligada, por ley, a informar rápidamente de sus sospechas a la unidad de inteligencia financiera (UIF)".

La Nota Interpretativa de la Rec. 20 establece lo siguiente:

La referencia a la actividad delictiva en la Rec. 20 se refiere a todos los actos delictivos que constituirían un delito subyacente para el LA o, como mínimo, a aquellos delitos que constituirían un delito subyacente, tal y como exige la Recomendación 3. Se recomienda firmemente a los países que adopten la primera de estas alternativas.

La referencia a la FT en la Rec. 20 se refiere a: la financiación de actos terroristas y de organizaciones terroristas, o de terroristas individuales, incluso en ausencia de un vínculo con un acto o actos terroristas específicos.

Todas las operaciones sospechosas, incluidos los intentos de operación, deben notificarse independientemente del importe de la operación.

El requisito de notificación debe ser una obligación directa, y no es aceptable ninguna obligación indirecta o implícita de notificar las operaciones sospechosas, ya sea en virtud de un posible enjuiciamiento por un delito de blanqueo de capitales o financiación del terrorismo, o de otro modo (la denominada "notificación indirecta").

La Nota Interpretativa eliminó el requisito que establecía que "todas las operaciones sospechosas deben ser reportadas, incluyendo las que se considera que involucran asuntos fiscales".

La actual norma del GAFI también establece la obligación de que las APNFD presenten ROS en virtud de la Recomendación 23:

Los abogados, los notarios, otros profesionales jurídicos independientes y los contadores deberían estar obligados a informar sobre las operaciones sospechosas cuando, en nombre o por cuenta de un cliente, realicen una operación financiera relacionada con las actividades descritas en el párrafo (d) de la Recomendación 22.

Se recomienda a los países que amplíen la obligación de informar al resto de las actividades profesionales de los contadores, incluida la auditoría.

Los comerciantes de metales preciosos y los comerciantes de piedras preciosas deberían estar obligados a informar de las operaciones sospechosas cuando realicen cualquier operación en efectivo con un cliente que sea igual o superior al umbral designado aplicable.

La Nota Interpretativa de la Recomendación 23 establece lo siguiente:

Los abogados, notarios y otros profesionales jurídicos independientes, así como los contadores que actúen como profesionales jurídicos independientes, no están obligados a notificar las operaciones sospechosas si la información pertinente se obtuvo en circunstancias en las que están sujetos al secreto profesional o a la prerrogativa de los profesionales jurídicos.

Corresponde a cada país determinar los asuntos que estarían comprendidos en el privilegio profesional legal o en el secreto profesional. Esto cubriría normalmente la información que los abogados, notarios u otros profesionales jurídicos independientes reciben de uno de sus clientes u obtienen a través de él: (a) mientras averiguan la posición legal de su cliente, o (b) en el desempeño de su tarea de defender o representar a ese cliente en, o en relación con, procedimientos judiciales, administrativos, de arbitraje o de mediación.

Los países pueden permitir que los abogados, notarios, otros profesionales jurídicos independientes y contadores envíen sus ROS a sus organizaciones autorreguladoras correspondientes, siempre que existan formas adecuadas de cooperación entre estas organizaciones y la UIF.

El hecho de que los abogados, los notarios, otros profesionales jurídicos independientes y los contadores que actúan como profesionales jurídicos independientes traten de disuadir a un cliente de realizar una actividad ilegal no equivale a una revelación (tipping-off).

La Obligación de Presentar ROS según el Estándar Actual del GAFI

- ¿Quién debe reportar?
- Bancos (desde las Recomendaciones originales del GAFI de 1990).
- + Instituciones financieras no bancarias (desde las revisiones de 1996 de las Recomendaciones del GAFI).
- + APNFD (desde las revisiones de 2003 de la Recomendación del GAFI).
- + VASPS (desde las revisiones de 2019 de las recomendaciones del GAFI).
- Otros sectores más allá de las Recomendaciones del GAFI, según lo exija la ley.
- ¿Qué hay que reportar?
- Todas las operaciones sospechosas, incluidas las tentativas de operación, deben notificarse rápidamente a la UIF, independientemente del importe de la operación.
- Cuando la IF sospecha o tiene motivos razonables para sospechar que los fondos son producto de una actividad delictiva o están relacionados con el FT.
- ¿Qué es una operación sospechosa?
- La definición de "sospecha" debe expresarse en los términos más claros posibles. La exigencia de claridad en la definición de una operación sospechosa es especialmente importante en los países en los que el incumplimiento de la obligación de informar conlleva sanciones penales.
- También es importante en otras jurisdicciones, ya que deben establecerse sistemas complejos y costosos para aplicar la obligación de informar. En muchos países, la ley exige que se notifiquen las operaciones "sospechosas", pero no define "sospechoso".

- Los términos "sospechoso" y "sospecha" tienen una amplia gama de significados y pueden incluir situaciones en las que hay un "umbral probatorio" muy bajo.

- Por ejemplo, en el contexto de las leyes del Reino Unido y de Escocia, se ha señalado que el significado ordinario de la palabra incluiría la idea de "imaginar algo sin pruebas o con pruebas escasas".

- Del mismo modo, en los Estados Unidos, el término "sospecha" se ha definido como "la imaginación o la aprehensión de la existencia de algo malo basada sólo en pruebas leves o nulas, sin pruebas definitivas".

- En francés, el término equivalente "soupçon" también tiene varios significados, algunos de los cuales también implican muy poca evidencia como, por ejemplo, "una simple conjetura, opinión, consejo o hipótesis o intuición...".

- ¿Qué es el producto de una actividad delictiva o de la financiación del terrorismo?

- La intención básica de la obligación de reportar, tal y como se recoge en las Recomendaciones del GAFI, es proporcionar a la UIF información sobre las operaciones de fondos que podrían proceder de actividades delictivas.

- Sobre la base de la Convención de Palermo, la obligación de informar en virtud de la Recomendación 20 se define por referencia a la sospecha de que los fondos son "producto de actividades delictivas", que se define en las Notas Interpretativas como:

- "a) todos los actos delictivos que constituyan un delito subyacente de LA en la jurisdicción; o

- b) como mínimo a los delitos que constituirían un delito subyacente según la Rec. 3."

- La Nota Interpretativa añade que "se exhorta firmemente a los países a adoptar la alternativa a).

- Una obligación similar figura en el Convenio Internacional para la Represión de la FT, que establece como norma la notificación de "operaciones sospechosas de proceder de una actividad delictiva"

Fundamentos de la Gestión del Riesgo de LA en Instituciones Financieras

- Las Recomendaciones del GAFI (en particular, la Recomendación 10) proporcionan un marco mínimo para la Diligencia Debida con respecto al Cliente (DDC) y la supervisión de las relaciones con los clientes.

- Como mínimo, una IF debe verificar la identidad y, en la mayoría de los casos, "conocer a su cliente".

- Mediante la recopilación de identificación y verificación de pruebas, una IF puede formarse razonablemente una idea de quién es su cliente y del origen de los fondos del cliente.

- Basándose en estos principios de conocimiento del cliente, las IF examinan y supervisan las operaciones de sus clientes para evitar que se utilicen para el LA/FT y otros delitos financieros, e informan a las UIF.

- Gracias a este seguimiento, es posible identificar la actividad inusual (al menos desde una perspectiva estadística), y alguna actividad periférica puede justificar una investigación más profunda.

- Cuando la investigación da lugar a una sospecha, la(s) operación(es) sospechosa(s) se comunica a la UIF (tal y como exige la Recomendación 20 del GAFI).

- También se exige a las IF que examinen a las personas expuestas políticamente (PEP) y a las personas y entidades sancionadas que también están vinculadas a la notificación de operaciones sospechosas.

- La mayoría de las grandes IF utilizarán sistemas automatizados para cumplir con estos requisitos, por ejemplo, para la detección de PEP y sanciones, se utilizarán listas disponibles públicamente y compradas para examinar los datos de los clientes.

- El GAFI proporciona orientación sobre el enfoque basado en el riesgo (EBR) en varios sectores y los reguladores también emiten guías específicas para las IF en su jurisdicción.

- Aunque las Recomendaciones del GAFI establecen unas normas mínimas, la forma de aplicar las medidas específicas y la intensidad de estas diferirán de

un país a otro, en función de su exposición al riesgo, que se identifica a través de las evaluaciones de riesgo.

- Estas normas también serán diferentes para cada IF en función de su modelo de negocio y del riesgo inherente atribuible tanto a la IF (en función de sus actividades comerciales) como a un cliente específico (en función de sus atributos).

- La evaluación del riesgo de la empresa influirá entonces en las consideraciones de inversión. Por ello, una empresa de menor riesgo puede disponer de herramientas de control menos modernas que una empresa de mayor riesgo.

- Como mínimo, una IF deberá identificar y verificar al cliente con el que entra en relación.

- En un nivel básico, esto suele implicar la recepción de documentos de identidad, como el pasaporte, el permiso de conducir o el documento nacional de identidad, para ayudar a verificar la identidad del cliente. Dependiendo de la jurisdicción y la legislación local, puede haber métodos electrónicos para verificar la identidad a través de canales remotos

- Por ejemplo, la apertura de cuentas en línea, que incluye la identificación y verificación electrónicas mediante bases de datos de identidad.

- También está aumentando el uso de soluciones de identidad digital

- La evaluación de riesgos determinará entonces qué información adicional debe recopilarse sobre el cliente para completar el proceso de diligencia debida.

  Normalmente, la exposición al riesgo de una IF depende de: el tipo de cliente; los países/áreas geográficas de exposición; los productos y servicios ofrecidos; los tipos de operación, y; los canales de entrega

Identificación de Operaciones Sospechosas

Primera línea de defensa

Los empleados de la primera línea de defensa (por ejemplo, los gerentes de relaciones, los ejecutivos de negocios y las funciones de operaciones de back-office) deben entender los riesgos de LA/FT que se plantean para el negocio en el que trabajan.

Los empleados de la primera línea de defensa desempeñan un papel fundamental en la gestión del riesgo de los clientes y de los terceros y en la escalada oportuna de la actividad potencialmente sospechosa. Las IF no deben confiar únicamente en los sistemas de monitoreo de operaciones para identificar actividades inusuales y potencialmente sospechosas en su población de clientes. Los empleados de la primera línea de defensa desempeñan un papel fundamental en la detección y prevención del LA/FT.

Los empleados debidamente capacitados están en condiciones de identificar operaciones sospechosas y evaluar que la información que antes se consideraba razonable -recopilada a través de las interacciones con un cliente- ahora parece sospechosa. La capacidad de una IF para identificar eficazmente las operaciones sospechosas depende, por lo tanto, de un sólido programa de DDC basado en el riesgo que establezca la comprensión por parte de la IF del riesgo asociado a su base de clientes, así como las prácticas bancarias o necesidades financieras esperadas y habituales del cliente.

La primera línea de defensa es un componente inestimable del programa ALA/CFT de una IF y debe recibir formación sobre el riesgo potencial y la mitigación del riesgo y la presentación de informes dentro de su área de negocio.

Los empleados deben conocer los requisitos normativos dentro del ámbito de su función; las señales de alarma asociadas a sus clientes, productos, servicios, canales de distribución y zonas geográficas; y el procedimiento de escalada adecuado tanto a su dirección como a la segunda línea de defensa, sin comprometer su responsabilidad de informar sobre las operaciones sospechosas

Segunda línea de defensa

La segunda línea de defensa (por ejemplo, los empleados de cumplimiento) proporciona asesoramiento sobre políticas, orientación, garantía, supervisión y desafío a la primera línea de defensa.

Si bien los empleados de la primera línea de defensa pueden investigar las operaciones sospechosas y documentar la investigación resultante, la presentación final del ROS debe ser realizada por el Oficial de Cumplimiento o

el MLRO (Money Laundering Reporting Officer) (en la segunda línea de defensa).

Con este fin, la segunda línea de defensa se encarga de supervisar el programa de investigaciones, compuesto por procesos de supervisión tanto automatizados como manuales. La segunda línea de defensa también se encarga de supervisar los riesgos a los que se enfrenta la IF, como el incumplimiento de leyes y reglamentos, y de informar directamente a la alta dirección sobre la exposición al riesgo de la IF.

Específicamente, la segunda línea de defensa y la primera línea de defensa (según corresponda) deben generar métricas relacionadas con los delitos financieros (por ejemplo, ROS presentados, atrasos en las alertas) para proporcionar a la alta gerencia una visión general adecuada del programa de cumplimiento de la IF, incluida la puntualidad y la calidad del manejo y la resolución de las alertas de monitoreo de operaciones de la IF y el proceso de presentación de ROS.

La segunda línea de defensa debe conservar los registros de toda la información relacionada con el seguimiento de las operaciones y la notificación de actividades sospechosas (normalmente durante un período de 5 años).

Tercera línea de defensa

La función de examinación independientes es responsable de evaluar el diseño y la eficacia operativa de los controles del programa de cumplimiento de una IF, incluido el cumplimiento técnico de las políticas y los procedimientos de ALA/CFT.

Esta función sirve como una "tercera línea de defensa" para identificar lagunas, deficiencias y puntos débiles en los controles operativos que pertenecen o son supervisados por las funciones de negocio, operaciones y cumplimiento de una IF.

Las pruebas independientes deben ser realizadas por un departamento de auditoría interna, auditores externos, consultores u otras terceras partes cualificadas e independientes.

Como mínimo, los empleados encargados de realizar las pruebas independientes no deben participar en la función que se está comprobando ni en otras funciones de ALA/CFT que puedan comprometer su independencia.

La auditoría basada en el riesgo ayuda al Consejo de Administración y a la alta dirección de una IF a identificar las áreas débiles, a priorizar esas áreas para su corrección y a garantizar la provisión de recursos adecuados, la supervisión y la formación de los empleados afectados.

Métodos de Monitoreo de las Operaciones

Un programa de monitoreo de operaciones debe considerar los riesgos LA/FT de los clientes, contrapartes, negocios, productos, servicios, canales de entrega y mercados geográficos de la IF, además de ayudar a priorizar las alertas de alto riesgo.

Sin embargo, la sofisticación de los sistemas de supervisión puede variar en función de los riesgos ALA/CFT de una IF.

Los sistemas de vigilancia suelen incluir la identificación o remisión de los empleados, sistemas basados en operaciones (manuales), sistemas de vigilancia (automatizados) o una combinación de ellos.

En general, las IF deben adoptar procesos y procedimientos de control para supervisar la actividad de los clientes que sean acordes con el tamaño y la naturaleza de la línea de negocio y los riesgos de LA/FT que plantea su base de clientes pertinente. Los procesos manuales

y/o los sistemas de supervisión deben demostrar razonablemente que las operaciones que conllevan el mayor riesgo de LA/FT están sujetas a un mayor escrutinio.

En el caso de los clientes o las relaciones comerciales que se identifican como de bajo riesgo, las IF pueden considerar la posibilidad de supervisar y revisar las operaciones con una frecuencia reducida.

Control manual

Una IF puede tratar de utilizar un sistema de supervisión manual de las operaciones, que suele centrarse en categorías específicas de operaciones (por ejemplo, las que implican grandes cantidades de dinero en efectivo, las que tienen como destino o proceden de determinadas zonas geográficas) e incluye una revisión manual de varios informes generados por los sistemas de la IF para identificar actividades inusuales.

El tipo y la frecuencia de las revisiones y los informes resultantes utilizados deben ser proporcionales al perfil de riesgo ALA/CFT de la IF, a la naturaleza, el tamaño y la complejidad de sus operaciones, y cubrir adecuadamente a los clientes, las contrapartes, los negocios, los productos, los servicios, los canales de entrega y los mercados geográficos.

Los informes generados por el sistema suelen utilizar un determinado umbral monetario para detectar actividades inusuales. El empleado superior responsable de una IF debe evaluar periódicamente la idoneidad de los criterios de filtrado y los umbrales utilizados en el proceso de supervisión y evaluar periódicamente a la Alta Dirección y, cuando sea necesario, notificar al

Consejo de Administración (como parte de las actualizaciones periódicas), sobre la idoneidad del diseño de los informes de supervisión manual.

Las IF deben estar atentas al hecho de que los riesgos complejos y cambiantes de la delincuencia financiera pueden socavar la eficacia de los sistemas de supervisión manual y, por lo tanto, los sistemas de supervisión manual también deben ser revisados de forma independiente para que los criterios de filtrado sean razonables.

Control automatizado

Los sistemas automatizados de supervisión de operaciones pueden abarcar múltiples tipos de operaciones y utilizar diferentes reglas para identificar actividades potencialmente sospechosas. Además, muchos sistemas pueden adaptarse a lo largo del tiempo en función de la actividad histórica, las tendencias o la comparación interna entre pares.

Una vez elaborados los parámetros y los filtros, deben revisarse antes de su aplicación para identificar las posibles lagunas en la cobertura, con el fin de abordar los posibles esquemas de delincuencia financiera que puedan no haberse contemplado.

Una vez establecida, la IF debe revisar y probar las capacidades y umbrales del sistema en forma periódica, de acuerdo con su perfil de riesgo. Esta revisión debe centrarse en parámetros o filtros específicos a fin de garantizar que la información prevista se capture con precisión y que el parámetro o filtro sea adecuado para el perfil de riesgo particular de la IF, incluida la aplicabilidad de los escenarios de detección, las reglas subyacentes, los valores de umbral y las suposiciones utilizadas.

Una IF también debe tratar de revisar su programa de monitoreo de operaciones por lo menos una vez al año para tener en cuenta los cambios en los procedimientos internos de la IF; las leyes y regulaciones locales; y las mejores prácticas.

Enfoques proactivos basados en la inteligencia

Las IF han comenzado a invertir en la formación y el desarrollo de sus propias unidades o capacidades de inteligencia.

Estas unidades tratan de maximizar el uso de los datos y la información disponible tanto a nivel interno -dentro de la IFcomo externo -en todas las jurisdicciones y negocios- para hacer frente a los esquemas de LA/FT, consolidar la capacidad analítica y eliminar cualquier silo jurisdiccional y de negocios.

Esto ha llevado a algunas entidades financieras a pasar de un enfoque de supervisión puramente a nivel de operación a la adopción de un enfoque de supervisión "a nivel de cliente" o "de red".

Con este enfoque, las investigaciones previas pueden aplicarse para informar y perfeccionar los modelos de riesgo, que luego pueden utilizarse para

personalizar la supervisión de las diferentes líneas de negocio y tipos de clientes.

Estas mejoras se centran en mirar más allá de las operaciones individuales o de los clientes individuales para identificar la red más amplia en la que opera un cliente - mirando al cliente como una entidad - lo que permite a las IF gestionar redes de cuentas e informar sobre estas redes, que a su vez, aumenta las oportunidades de interrumpir esa red.

Este modelo aleja la información de los informes sobre operaciones sospechosas individuales y la acerca a las entidades y redes sospechosas con una visión de cómo fluyen los fondos entre ellas.

Revisión de Alertas y Presentación de ROS (*Timing)*

Consideraciones generales:

Un proceso eficiente de gestión y disposición de alertas es esencial para salvaguardar la integridad financiera de las IF, ayudar a las fuerzas del orden en la identificación e investigación de la actividad delictiva y satisfacer las expectativas reguladoras relativas a la notificación puntual de actividades sospechosas.

El proceso de gestión y disposición de alertas debe contar con el personal adecuado y sin cuellos de botella, y debe incluir un proceso para la presentación acelerada de informes urgentes en los casos apropiados. Se entenderá que las "alertas" incluyen las alertas automatizadas de supervisión de operaciones, las remisiones de los empleados y las solicitudes de las fuerzas de seguridad.

Revisión de la alerta:

Los empleados de la IF deben revisar una alerta y determinar si se justifica una investigación adicional. La base subyacente para la determinación debe documentarse de acuerdo con los procedimientos de investigación de una IF. Una IF puede optar por someter las decisiones de revisión de alertas a una revisión de Control de Calidad (“CC"), antes de la disposición final.

Cuando los hechos disponibles en la fase de revisión de la alerta son o pueden ser suficientes para justificar la presentación de un ROS sin más investigación, o cuando la operación puede requerir atención inmediata, los empleados deben escalar inmediatamente la actividad alertada a la autoridad designada para la decisión del ROS para una revisión acelerada.

Investigación de casos:

Para cualquier actividad alertada que se determine que requiere más investigación, los empleados deben llevar a cabo y completar (al menos preliminarmente) una investigación de la actividad alertada, documentar los resultados de cualquier investigación o análisis realizado, y hacer una recomendación sobre si se debe presentar un ROS.

Cuando el investigador de un caso tenga conocimiento de una actividad que requiera atención inmediata, los empleados deben elevar inmediatamente la actividad a la autoridad designada para la toma de decisiones en materia de ROS para una revisión acelerada.

Las solicitudes de información no respondidas durante la investigación de un caso no deben retrasar la presentación oportuna de recomendaciones con respecto a la presentación de un ROS. Las IF deben definir el plazo razonable de la RFI para permitir al cliente responder a las consultas planteadas durante la investigación de un caso como parte del proceso de RFI. Este plazo de RFI debe ser de [X días] a partir de la fecha de generación de la alerta.

Toma de decisiones de STR:

El Oficial de Cumplimiento o el MLRO deben revisar la recomendación de investigación de un caso y decidir si la actividad es sospechosa dentro de los [X días] de la fecha de generación de la alerta.

En caso de escalamiento para una revisión acelerada, el Oficial de Cumplimiento o el MLRO deben revisar la actividad y decidir si es sospechosa dentro de las [24 horas] de la fecha de escalamiento. Cuando sea apropiado, el Oficial de Cumplimiento o el MLRO también deben escalar la actividad para una posible salida y cierre de la cuenta.

Presentación de STR:

En ausencia de una escalada para una revisión acelerada, el Oficial de Cumplimiento o el MLRO debe presentar un ROS a la UIF dentro de los [X días de la fecha de determinación de que una operación cumple con la definición de actividad sospechosa].

En el caso de una escalada para una revisión acelerada, el Oficial de Cumplimiento o MLRO debe presentar un ROS a la UIF dentro de [24 horas de la determinación]. Todos los posibles ROS deben ser revisados para comprobar su exactitud e integridad antes de su presentación, de acuerdo con los procedimientos aplicables.

Actividad que requiere atención inmediata:

Las situaciones que requieren atención inmediata incluyen las infracciones denunciables que están en curso (por ejemplo, parte de un esquema de LA en curso, según lo indicado por una autoridad policial apropiada) y las operaciones que la IF sospecha que pueden estar relacionadas con el FT.

Vigilancia y notificación de actividades sospechosas continuas:

Los empleados deben revisar cualquier actividad nueva relacionada con un ROS anterior [en un plazo de X días desde la última operación notificada]. Cuando dicha revisión descubra una actividad sospechosa continuada, los empleados deberán presentar un ROS en un plazo máximo de X días a partir de la fecha de la presentación del ROS anterior.

Puede haber situaciones que requieran la presentación de un ROS antes de X días después del ROS inicial. Una "revisión posterior al ROS puede realizarse manualmente o a través de los sistemas/escenarios de supervisión de operaciones automatizados y continuos de las IF.

Estructura y contenido de un ROS

En algunos países, la facultad de decidir la forma y el contenido de los informes se delega en la UIF. En otros, los anexos a la ley contienen los elementos que deben notificarse. Los elementos pueden suprimirse de las listas o añadirse a ellas mediante reglamentos emitidos por el gobierno.

En la mayoría de los países, los ROS se presentan electrónicamente y la UIF suele proporcionar un formato o plantilla uniforme. Dicha plantilla suele estar dividida en las siguientes secciones:

Campos estructurados, cuyo objetivo es capturar el siguiente tipo de datos de forma estructurada:

Información sobre el tema

Información sobre actividades sospechosas

Información de la entidad informante

Campo narrativo, cuyo objetivo es obtener un relato detallado de la operación sospechosa que se comunica, abordando las siguientes cuestiones:

¿quién? ¿qué? ¿cuándo? ¿dónde? y ¿por qué? - de la actividad sospechosa que se comunica a la UIF.

El método de operación/modus operandi (¿o cómo?) también es importante y debe incluirse en el relato.

¿Quién realiza la transacción sospechosa?

Describa el objeto del ROS (u otro informe), también conocido como sospechoso(s), incluyendo el conductor, el beneficiario y los titulares de cuentas involucrados en la transacción o actividad.

Proporcionar información de identificación de las partes implicadas en la transacción, como la ocupación y el cargo o puesto del sospechoso en la empresa.

Enumere los propietarios efectivos, los directores, los funcionarios y las personas con autoridad para firmar, si es posible. Si la transacción o actividad implica a una entidad, incluya información sobre la propiedad, el control y la estructura de la empresa.

Proporcione detalles sobre el papel de cada persona o entidad en cada una de las transacciones financieras descritas. Es importante entender quién envía y recibe los fondos.

Si hay más de una persona o entidad implicada en la actividad sospechosa, explique las relaciones entre las personas o entidades (si se conocen).

Aunque la información no siempre esté disponible, debe incluirse en la medida de lo posible. Por ejemplo, los domicilios de los sospechosos son importantes; las IF que presenten los expedientes deben anotar no sólo la dirección principal del sospechoso, sino también otras direcciones conocidas. También es importante documentar todos los números de identificación asociados al sospechoso o a los sospechosos, como los números de los pasaportes y de los permisos de conducir.

¿Qué instrumentos o mecanismos se utilizan para facilitar la transacción o actividad sospechosa?

Revisar los instrumentos o mecanismos utilizados en la actividad sospechosa (por ejemplo, transferencias electrónicas, moneda extranjera, cartas de crédito y otros instrumentos comerciales, cuentas de corresponsalía, giros postales, tarjetas de crédito/débito, etc.).

Comprender el número de métodos diferentes empleados para iniciar la negociación de fondos, como Internet, acceso telefónico, correo, caja de depósito nocturno, marcación remota, mensajeros u otros.

Describa la fuente de los fondos (como originador) o el uso de los fondos (como beneficiario). Al documentar el movimiento de fondos, identifique todos los números de cuenta en la IF afectada por la actividad o transacción sospechosa y, cuando sea posible, proporcione cualquier número de cuenta que tenga en otras IF y los nombres/ubicaciones de las otras IF involucradas en la actividad reportada

¿Qué instrumentos o mecanismos se utilizan para facilitar la transacción o actividad sospechosa?

Revisar los instrumentos o mecanismos utilizados en la actividad sospechosa (por ejemplo, transferencias electrónicas, moneda extranjera, cartas de crédito y otros instrumentos comerciales, cuentas de corresponsalía, giros postales, tarjetas de crédito/débito, etc.).

Comprender el número de métodos diferentes empleados para iniciar la negociación de fondos, como Internet, acceso telefónico, correo, caja de depósito nocturno, marcación remota, mensajeros u otros.

Describa la fuente de los fondos (como originador) o el uso de los fondos (como beneficiario). Al documentar el movimiento de fondos, identifique todos los

números de cuenta en la IF afectada por la actividad o transacción sospechosa y, cuando sea posible, proporcione cualquier número de cuenta que tenga en otras IF y los nombres/ubicaciones de las otras IF involucradas en la actividad reportada.

¿Cuándo tuvo lugar la actividad o transacción sospechosa?

Si la actividad tiene lugar durante un periodo de tiempo, facilite la fecha en que se observó por primera vez la actividad o transacción sospechosa y describa la duración de la actividad.

Para comprender mejor el historial y la naturaleza de la actividad, así como el flujo de fondos, las IF deben proporcionar información sobre cada transacción individual en orden cronológico (por ejemplo, fechas individuales e importes de las transacciones, en lugar de sólo el importe agregado).

Proporcione información sobre cuándo se completó o se intentó completar la transacción. Si la transacción no se completó, la IF debe indicarlo en la descripción.

¿Dónde tuvo lugar la actividad o transacción sospechosa?

Explique si varias oficinas de una misma IF estuvieron involucradas en la actividad o transacción sospechosa que se denuncia. Indique las direcciones de esas oficinas.

Especifique si la actividad o transacción sospechosa implica a una jurisdicción extranjera. En este caso, enumere la jurisdicción extranjera, la IF, la dirección y cualquier número de cuenta involucrado o afiliado a la(s) actividad(es) o transacción(es) sospechosa(s).

Esta información debe incluir cualquier lugar que intervenga en la cadena completa de la transacción, incluidos los originadores y beneficiarios finales en la medida en que pueda determinarse.

¿Por qué cree la IF que la actividad o transacción es sospechosa?

Describa el sector o la empresa y por qué la actividad o la transacción es inusual para el cliente. Tenga en cuenta los tipos de productos y servicios implicados en la actividad y las actividades previstas de clientes similares.

Evaluar por qué la actividad creó una alerta para la IF o activó una alerta en el sistema.

Estas respuestas variarán en función del tipo de IF (por ejemplo, una institución de depósito frente a una compañía de seguros) y una IF también debe considerar factores como:

Los tipos de productos y servicios que ofrece la IF;

Los tipos de cuentas que el cliente tiene en la IF;

La actividad comercial normalmente esperada del cliente (si es cliente de la IF), y por qué no es una actividad normal o esperada;

La finalidad del pago o de la transacción, en la medida en que se conozca, se informe, se alegue o se cuestione; y

Si la actividad fue resultado de una alerta automatizada, el escenario o la regla que generó la alerta.

¿Cómo se produjo la actividad o transacción sospechosa?

Describa cómo se cometió la transacción o el patrón de transacciones (es decir, el "modus operandi" o el método de operación).

Por ejemplo, si parece que hay varios cheques depositados que coinciden con transferencias electrónicas salientes de las cuentas, la narración debe incluir información sobre los cheques y las transferencias salientes (incluyendo fechas, destinos, importes, cuentas, frecuencia y beneficiarios de las transferencias de fondos).

ROS defensivos

- La presentación defensiva es la práctica de presentar ROS sobre transacciones que las IF no consideran verdaderamente sospechosas para reducir el riesgo de sanciones reglamentarias por no presentar ROS.

- Aunque puede haber algún aspecto de la transacción o actividad que cree una posible sospecha, los archivos defensivos no informan sobre la actividad que la IF considera realmente sospechosa.

- Por lo tanto, en general se desaconsejan las presentaciones defensivas, dado que dichas presentaciones disminuyen el valor de los ROS, incluso provocando un aumento de las presentaciones no valiosas.

- Un ROS, un RAS y otros tipos de informes deben ser de la mejor calidad posible, incluso en el sentido de que deben tener una narrativa claramente escrita con suficiente detalle que articule exhaustivamente los factores que implican la transacción o actividad sospechosa reportada.

- Los ROS defensivos suelen indicar la existencia de un sistema ineficiente de supervisión de las transacciones y un sistema débil de controles internos de una IF, y en algunas jurisdicciones podrían ser objeto de sanciones administrativas.

Presentación y modificación de ROS presentados

- Las IF deben presentar los ROS directamente a la UIF utilizando los portales en línea.
- Esto suele requerir el registro de las IF en el sistema de la UIF como condición obligatoria para poder informar.

- Tras la presentación del informe, suele ser obligatorio que el declarante de la IF adjunte documentos complementarios que acompañen a la presentación, incluidos, entre otros, la documentación de Conozca a su Cliente (KYC), copias de la documentación de identificación, formularios de apertura de cuentas, recibos de transacciones, estados financieros y otros documentos que puedan ser relevantes para la investigación.

- Una vez que un informe es presentado y aceptado en el sistema, ni el Oficial de Cumplimiento, ni el MLRO, ni los empleados de la UIF pueden aplicar cambios y enmiendas al informe por información faltante o incorrecta. Sin embargo, se puede exigir a las IF que presenten información adicional.

- Las IF deben asegurarse de que el declarante utilice el número de referencia web correcto del informe inicial. Para evitar este tipo de incidentes y para salvaguardar la integridad de los datos del sistema, las IF deben verificar la calidad y la exactitud de la información cargada.

Obligación de revelar (tipping-off)

- La obligación de no revelar (tipping-off) y respetar las normas de confidencialidad se detallan en la Recomendación 21 del GAFI:

- Las IF, sus directores, funcionarios y empleados deben ser:

- (a) protegidos por la ley de la responsabilidad penal y civil por el incumplimiento de cualquier restricción a la divulgación de información impuesta por contrato o por cualquier disposición legislativa, reglamentaria o administrativa, si comunican sus sospechas de buena fe a la UIF, incluso si no sabían con exactitud cuál era la actividad delictiva subyacente, e independientemente de si la actividad ilegal se produjo realmente; y

- (b) se les prohíbe por ley revelar ("tipping-off") el hecho de que se está presentando un informe de transacción sospechosa (STR) o información relacionada con la UIF. Estas disposiciones no pretenden inhibir el intercambio de información en virtud de la Recomendación 18.

- Para evitar que los fondos sospechosos sean transferidos fuera de la institución declarante y para no perjudicar las investigaciones al dar a conocer a los sospechosos, es importante que las instituciones declarantes no informen a los titulares de las cuentas y a los clientes de los ROS que proporcionan a la UIF.

Obligaciones después de presentar un ROS

- Consideraciones generales

- Tras la presentación de un ROS, la UIF puede o no dirigirse a la IF con instrucciones específicas, solicitudes de información adicional, comentarios o más orientación relacionada con el ROS, o con la relación comercial en general.

- En estos casos, estas comunicaciones se dirigirán generalmente al Oficial de Cumplimiento o al MLRO. Sin embargo, es posible que las IF no reciban instrucciones, solicitudes de información adicional u otros comentarios de la UIF en relación con los ROS que se han presentado; o que la recepción de dichas comunicaciones se retrase más allá de lo que consideran un período de tiempo razonable.

- En tales casos, las IF deben seguir sus políticas internas en relación con dichos clientes y deben determinar el manejo apropiado del ROS y de la relación comercial en general, tomando en consideración todos los factores de riesgo involucrados.

- Además, las FIs deben conservar todos los registros y documentos relativos a los ROS y los resultados de todos los análisis o investigaciones realizados [durante al menos cinco (5) años].

- Posibles pasos post-ROS

- Al informar de un ROS a la UIF, la IF podría tomar los siguientes pasos:

- Siga las instrucciones, si las hay, de la UIF en relación tanto con la transacción notificada como con la relación comercial en general.

- Identificar todas las cuentas o relaciones relacionadas o asociadas de los clientes notificados y realizar una revisión de dichas cuentas o relaciones. Si procede, aplicar procedimientos de diligencia debida reforzada (EDD) basados en el riesgo y de supervisión continua.

- Clasificar el cliente o la relación comercial, incluidas las cuentas relacionadas/asociadas y la relación con los clientes denunciados, como de alto riesgo y aplicar procedimientos adecuados de EDD basados en el riesgo y de supervisión continua para mitigar los riesgos asociados de blanqueo de capitales y financiación del terrorismo.

- En general, a menos que la UIF les ordene específicamente que lo hagan, las IF no están obligadas a realizar las transacciones que sospechan, o tienen motivos razonables para sospechar, que están relacionadas con un delito.

- Tomar las medidas oportunas para decidir si se mantiene o no la relación comercial en función de su apetito de riesgo.

- Pasos adicionales post-ROS

- Reevaluar el riesgo de la relación comercial y reevaluar el perfil de riesgo del cliente, cuando sea necesario.

- Iniciar una revisión de diligencia debida de la cliente mejorada.

- Considerar la realización de una investigación de antecedentes mejorada (incluyendo, si procede, el uso de un servicio de investigación de terceros).

- Solicitar al cliente datos, información o documentos adicionales para realizar las transacciones (por ejemplo, pruebas de licencias o autorizaciones pertinentes, documentos aduaneros, documentos de identificación adicionales, referencias bancarias o de otro tipo).

- Restringir el uso de determinados productos o servicios por parte del cliente.

- Cualquier otra medida razonable, acorde con la naturaleza y el tamaño de sus negocios, y teniendo en cuenta la obligación de evitar el revelar (“tipping-off“) al cliente.

Inmunidad para las entidades informantes y el personal para los ROS realizados de buena fe

- Las Recomendaciones del GAFI han establecido como norma (desde 1990) que una persona que presenta un ROS de buena fe debe ser inmune a la responsabilidad por las consecuencias legales de haberlo presentado.

- La ley que exija la presentación de los ROS debe dejar claro que quienes hacen los informes están exentos de los requisitos legales de secreto profesional y confidencialidad.

- Las personas que presenten los informes de buena fe también deben estar protegidas contra la posible responsabilidad de las personas mencionadas en los informes, que, si se enteran de la existencia de los ROS, podrían intentar obtener una indemnización por daños y perjuicios de las personas que presentaron los ROS.

- Las leyes sobre la inmunidad de los sujetos obligados varían en su alcance.

Retroalimentación de la UIF a los sujetos obligados

- La retroalimentación de la UIF es la principal herramienta para proporcionar información a los sujetos obligados sobre la calidad de sus ROS.

- La retroalimentación a los sujetos obligados puede realizarse a través de diferentes métodos:

- Comentarios del sector

- Reporteros principales frente a reporteros bajos

- Información específica para cada IF

- Los comentarios pueden hacerse llegar a través de diferentes canales:

- Sesiones/reuniones presenciales grupales/concretas

- Reuniones virtuales grupales/específicas

- Informes de opinión

- ¿Deben hacerse públicas las sesiones/reuniones/informes de opinión?

- Ventajas y desventajas

- La retroalimentación de la UIF debe estar debidamente preparada de antemano y basarse en una investigación previa adecuada sobre la calidad de los STRS realizados por la UIF. Debe haber un objetivo claro para la sesión de retroalimentación, en función del público al que se dirija.

- Esta investigación se suele llevar a cabo a través de proyectos de análisis estratégico que se centran en el análisis de muestras de ROS, ya sea de todo el sector, de un grupo de entidades informantes o de una entidad individual, y en la identificación de tendencias comunes en los puntos fuertes y débiles de la información.

- El nivel de detalle a la hora de proporcionar información dependerá de si se realiza a través de sesiones de grupo o específicas. Algunas sesiones de retroalimentación pueden centrarse sólo en la identificación de tendencias repetidas agregadas en la presentación de informes deficientes, mientras que otras pueden proporcionar ejemplos específicos de ROS deficientes, o una combinación de ambos.

- Es importante que en las sesiones de retroalimentación se aborden las deficiencias en cuanto a la puntualidad, la precisión y la exhaustividad de los ROS. La retroalimentación debe proporcionarse en los campos estructurados del ROS y en el campo narrativo.

- Recuerde que la retroalimentación no sólo debe estar relacionada con las deficiencias. El feedback también puede ser positivo y compartirlo es una buena forma de equilibrar las sesiones de feedback.

Prácticas de intercambio de información: Privado-Privado

- Promover un intercambio de información financiera lo más amplio posible puede ayudar a reforzar la detección de actividades sospechosas, mejorar la calidad de los informes sobre transacciones sospechosas y aumentar la protección de la integridad financiera.

- La Recomendación 18 del GAFI establece que los grupos financieros deben implementar programas para todo el grupo contra el LD y el FT, incluyendo políticas y procedimientos para compartir información dentro del grupo con fines ALD/CFT.

- La Nota Interpretativa establece que las funciones de cumplimiento, auditoría y/o ALD/CFT a nivel de grupo deben recibir información sobre los clientes, las cuentas y las transacciones de las sucursales y filiales cuando sea necesario a efectos de ALD/CFT.

- Esto debe incluir información y análisis de transacciones o actividades que parezcan inusuales (si se realizó dicho análisis); y podría incluir un ROS, su información subyacente, o el hecho de que se haya presentado un ROS.

- Del mismo modo, las sucursales y filiales deben recibir dicha información de estas funciones a nivel de grupo cuando sea pertinente y adecuada para la gestión de riesgos.

- Deben establecerse salvaguardias adecuadas sobre la confidencialidad y el uso de la información que se intercambia, entre otras cosas, para evitar el "tipping off". Los países pueden determinar el alcance y la extensión de este intercambio

de información, basándose en la sensibilidad de la información, y su relevancia para la gestión del riesgo ALD/CFT.

Asociaciones de intercambio de información: Público-Privado

- Las asociaciones público-privadas (APP) establecidas demuestran que la inteligencia financiera se desarrolla y se utiliza de forma más eficaz y eficiente cuando hay cooperación y se comparte la información pertinente en los marcos adecuados, produciendo en el proceso ROS de mayor calidad y mejor enfocados.

- Tanto el gobierno como el sector privado tienen algo que aportar y sacar de la asociación.

- El gobierno tiene acceso a la información sobre los objetivos, el modus operandi y la inteligencia encubierta, y requiere el acceso a la información financiera pertinente que poseen los sujetos obligados.

- El sector privado dispone de una gran cantidad de información financiera específica de los clientes y de otro tipo para realizar análisis, quiere evitar que sus instituciones sean explotadas por delincuentes o terroristas, y debe identificar y notificar las actividades sospechosas (según lo establecido por cada régimen nacional de lucha contra el lavado de activosy la financiación del terrorismo, en consonancia con las normas del GAFI).

- El intercambio activo de información ayuda a ambas partes a desempeñar sus funciones con mayor eficacia.

- Las APP son un mecanismo para luchar de forma proactiva contra el LA/FT, pero no pretenden sustituir a los regímenes de ROS.

- Las APP son una extensión del régimen de ROS en estas jurisdicciones y proporcionan mecanismos adicionales para compartir información entre los sectores público y privado, impulsando la recopilación de inteligencia de mayor calidad y con fines específicos.

Otros mecanismos para mejorar el flujo y la calidad de las ROS

- Para mejorar el cumplimiento de las obligaciones de notificación de los ROS, los mecanismos adicionales pueden ayudar a fomentar la mejora del flujo y la calidad de los informes:

- Proporcionar orientación puede ayudar a aclarar las expectativas legales y reglamentarias y ayudar a las entidades informantes a comprender y cumplir eficazmente sus obligaciones de informar en virtud de las leyes y reglamentos aplicables.

- Los programas de sensibilización y formación pueden dirigirse a las instituciones de los sectores que muestren mayor necesidad de mejora. El objetivo inmediato de la participación del personal de la UIF en la formación de los sectores seleccionados sería fomentar la mejora de la presentación de informes, pero también podría considerarse el inicio de la relación bilateral entre la UIF y las entidades del sector.

- Sin embargo, también hay que prever medidas correctivas para garantizar que todas las instituciones afectadas comprendan el carácter obligatorio de la obligación de informar y que se ejerzan contra las instituciones deficientes una vez que se hayan probado otras acciones sin producir los resultados deseados. El uso de sanciones en los casos apropiados también sirve para dejar clara a toda la comunidad de informadores la determinación de la UIF (u otro organismo de supervisión) de llegar a niveles de información satisfactorios.

- En algunos países, el incumplimiento de la obligación de informar en virtud de las leyes ALA/CFT por parte de personas físicas y jurídicas puede constituir una violación del derecho penal.

Puntos principales

- La presentación de ROS en una recomendación fundamental según el estándar del GAFI.

- Los ROS son la principal fuente de información para el desarrollo de la inteligencia financiera por parte de las UIFs

- La presentación de ROS es la culminación de un proceso que requiere el funcionamiento eficaz de otros componentes del programa de cumplimiento ALA/CFT (principalmente políticas y procedimientos eficaces de DDC/KYC y de supervisión de las transacciones).

- La detección eficaz de las transacciones sospechosas requiere unas prácticas sólidas de gestión de los riesgos de los delitos financieros y una fuerte capacidad de supervisión de las transacciones.

- Los sistemas automatizados de seguimiento de las transacciones y la aplicación de un enfoque proactivo basado en la inteligencia para la prevención y la detección de los delitos financieros pueden contribuir a mejorar la calidad de las comunicaciones por indicio.

- La retroalimentación es la principal herramienta para proporcionar información sobre la calidad de los ROS a las entidades informantes.

- Las prácticas de intercambio de información en todo el grupo pueden contribuir a mejorar la calidad de los ROS.

- Las APP pueden ayudar a producir ROS de mayor calidad

- La orientación, la sensibilización y la formación pueden ayudar a aclarar las expectativas normativas de la obligación de informar.

- Un uso racional y proporcionado de las sanciones también puede servir para disuadir del incumplimiento y elevar la calidad de la información