MEJORES PRÁCTICAS SOBRE EL MANTENIMIENTO DE LA CONFIDENCIALIDAD Y SEGURIDAD DE LOS REPORTES DE OPERACIÓN SOSPECHOSA (ROS) EN EL GAFILAT

Desarrollado por el Grupo de Trabajo de Apoyo Operativo (GTAO) del Grupo de Acción Financiera de Latinoamérica (GAFILAT)

Enero de 2018

CONTENIDO

MEJORES PRÁCTICAS SOBRE EL MANTENIMIENTO DE LA CONFIDENCIALIDAD Y SEGURIDAD DE LOS REPORTES DE OPERACIÓN SOSPECHOSA (ROS) EN EL GAFILAT

I. INTRODUCCIÓN

Los Reportes de Operación Sospechosa (ROS) que se presentan a las Unidades de Inteligencia Financiera (UIF)[1] alrededor del mundo constituyen un insumo fundamental en el régimen de detección y combate al lavado de activos y el financiamiento al terrorismo. A través de estos informes, las entidades financieras y las actividades y profesiones no financieras designadas (APNFD) dan parte a las autoridades con relación a transacciones que, debido a la características de la operación, el perfil del cliente o usuario que la realiza o circunstancias en las que se lleva a cabo, podrían potencialmente indicar su vinculación con la comisión del delito de lavado de activos, financiamiento del terrorismo o algún delito precedente a los dos anteriormente señalados.

El presente documento tiene como finalidad presentar una guía y buenas prácticas a nivel de GAFILAT para el mantenimiento de la confidencialidad de los ROS, así como la protección de la información contenida en los mismos. El documento recopila las experiencias en la materia de los países miembros de GAFILAT, a la vez que toma en consideración los trabajos que se han desarrollado en la materia por parte de otros órganos internacionales, como son el Grupo Egmont de Unidades de Inteligencia Financiera y el Grupo de Expertos para el Control del Lavado de Activos de la Organización de Estados Americanos (OEA).

II. ESTANDARES Y TRABAJOS A NIVEL GLOBAL Y REGIONAL CON RELACIÓN A LA PROTECCIÓN DE LOS ROS

a. GAFI

La Recomendación 20 del GAFI es el estándar internacional vigente que marca la necesidad de que las instituciones financieras emitan reportes de aquellas operaciones que, por sus características, pudieran indicar su vinculación al delito de lavado de activos, financiamiento

[1] En adición al término "Unidad de Inteligencia Financiera", dentro de la región y en otras regiones del mundo existen otras denominaciones como "Unidad de Análisis Financiero", "Unidad de Información Financiera" y "Unidad de Investigación Financiera", en adición a nombres específicos otorgados a las autoridades en dicho país. Para efectos de practicidad en el presente documento se utilizará el término "Unidad de Inteligencia Financiera" como denominación genérica para referir a las autoridades encargadas de recibir y analizar los reportes de operaciones sospechosas, en términos de las Recomendaciones 20, 21 y 23 del GAFI, así como de diseminar informes de inteligencia financiera, tanto táctica como estratégica, a otras autoridades relevantes nacionales y a contrapartes extranjeras.

del terrorismo o que involucren fondos de origen ilícito; con base en la Recomendación 23, la obligación de reportar operaciones sospechosas a una autoridad nacional se extenderá también a las siguientes actividades y profesiones no financieras designadas:

- Abogados que realicen operaciones a nombre de sus clientes
- Contadores que realicen operaciones a nombre de sus clientes
- Notarios
- Otros profesionales jurídicos
- Comerciantes de metales preciosos
- Comerciantes de piedras preciosas
- Proveedores de servicios societarios y de fideicomisos

Debido a lo trascendental de la naturaleza de la información contenida en dichos reportes, la Recomendación 21 es específica en cuanto a la necesidad de mantener la confidencialidad y que no se revele a personas externas que se ha emitido un reporte de operación sospechosa, así como el contenido o información relacionada con el mismo; asimismo, la ley debe contar con protección ante responsabilidad penal y civil para quienes reportan de buena fe operaciones sospechosas.

Para los efectos de recibir, recopilar, analizar y diseminar la información financiera contenida en los reportes anteriormente señalados, la Recomendación 29 establece que los países habrán de contar con Unidades de Inteligencia Financiera (UIF), que funcionen como la única autoridad nacional a cargo de recibir este tipo de reportes, analizarlos y con base en la información crear productos de inteligencia financiera de tipo táctico, los cuales responden a una investigación o caso específico, o estratégico, en el cual se analizan tendencias y modalidades de operación de carácter general, así como tipologías y otros productos, los cuales son difundidos para efectos de prevención y detección temprana.

b. Grupo Egmont de Unidades de Inteligencia Financiera

Por otra parte, al ser la recepción, análisis y difusión de ROS una de las tareas específicas que la Recomendación 29 asigna a las Unidades de Inteligencia Financieras (UIF), el Grupo Egmont ha incluido como parte de sus "Principios para el Intercambio de Información entre Unidades de Inteligencia Financiera" un apartado sobre protección de datos y confidencialidad de la información. Los principios relevantes para estos efectos son los numerales 28 a 33, mismos que se presenten a continuación para facilitar la referencia:

> *28. La información recibida, procesada, mantenida o diseminada por las UIF solicitantes debe ser protegida, intercambiada y utilizada, de manera segura, sólo de acuerdo con los procedimientos acordados, políticas y leyes y reglamentaciones vigentes.*

> *29. Las UIF deben, por lo tanto, tener reglas implementadas que regulen la seguridad y confidencialidad de dicha información, incluyendo procedimientos para manejar, almacenar, diseminar y proteger, así como acceder a dicha información.*
>
> *30. Las UIF deben asegurar que su personal tenga los niveles de acceso de seguridad necesarios y comprendan sus responsabilidades en el manejo y diseminación de información sensible y confidencial.*
>
> *31. Las UIF deben asegurar que haya acceso limitado a sus instalaciones e información, incluyendo a los sistemas de tecnologías de la información.*
>
> *32. La información intercambiada deberá ser utilizada solo con el propósito para el cual se solicitó o proporcionó. Cualquier diseminación de la información a otras autoridades o terceros, o cualquier uso de esa información para fines administrativos, investigativos, procesales o judiciales más allá de aquellos autorizados originalmente, deberán estar sujetos a la previa autorización de la UIF solicitada.*
>
> *33. Como mínimo, la información intercambiada deberá ser tratada y protegida con las mismas disposiciones de confidencialidad que aplican a información similar de fuentes nacionales obtenida por la UIF que recibe la solicitud.*

Para efectos de mantener la seguridad y confidencialidad de la información de inteligencia financiera que se intercambia, el Grupo Egmont, con el apoyo del Financial Crimes Enforcement Network (FinCEN, la UIF de los Estados Unidos de América) ha establecido un sistema de intercambio denominado "Red Segura de Egmont" (Egmont Secure Web, ESW), el cual consta de un sistema de correo electrónico inmerso en una red privada y segura, a través del cual los países realizan y responden a solicitudes en un ambiente seguro, con diversos niveles de autenticación y de encriptación de la información.

c. Grupo de Expertos para el Control del Lavado de Activos, Organización de Estados Americanos

A nivel regional americano, el Grupo de Expertos para el Control del Lavado de Activos de la Comisión interamericana para el Control del Abuso de Drogas (CICAD), Organización de Estados Americanos, emitió un par de documentos relacionados con el manejo y protección de la información contenida en los ROS, especialmente cuando esta información es transmitida a terceras autoridades competentes en materia de investigación y procesamiento de los delitos de lavado de activos y delitos conexos. El Grupo de trabajo UIF/OIC (organismo de investigación criminal) desarrolló dos documentos: los "Principios Recomendados sobre el uso y protección de la información obtenida de las UIF" y las "Mejores prácticas recomendadas".

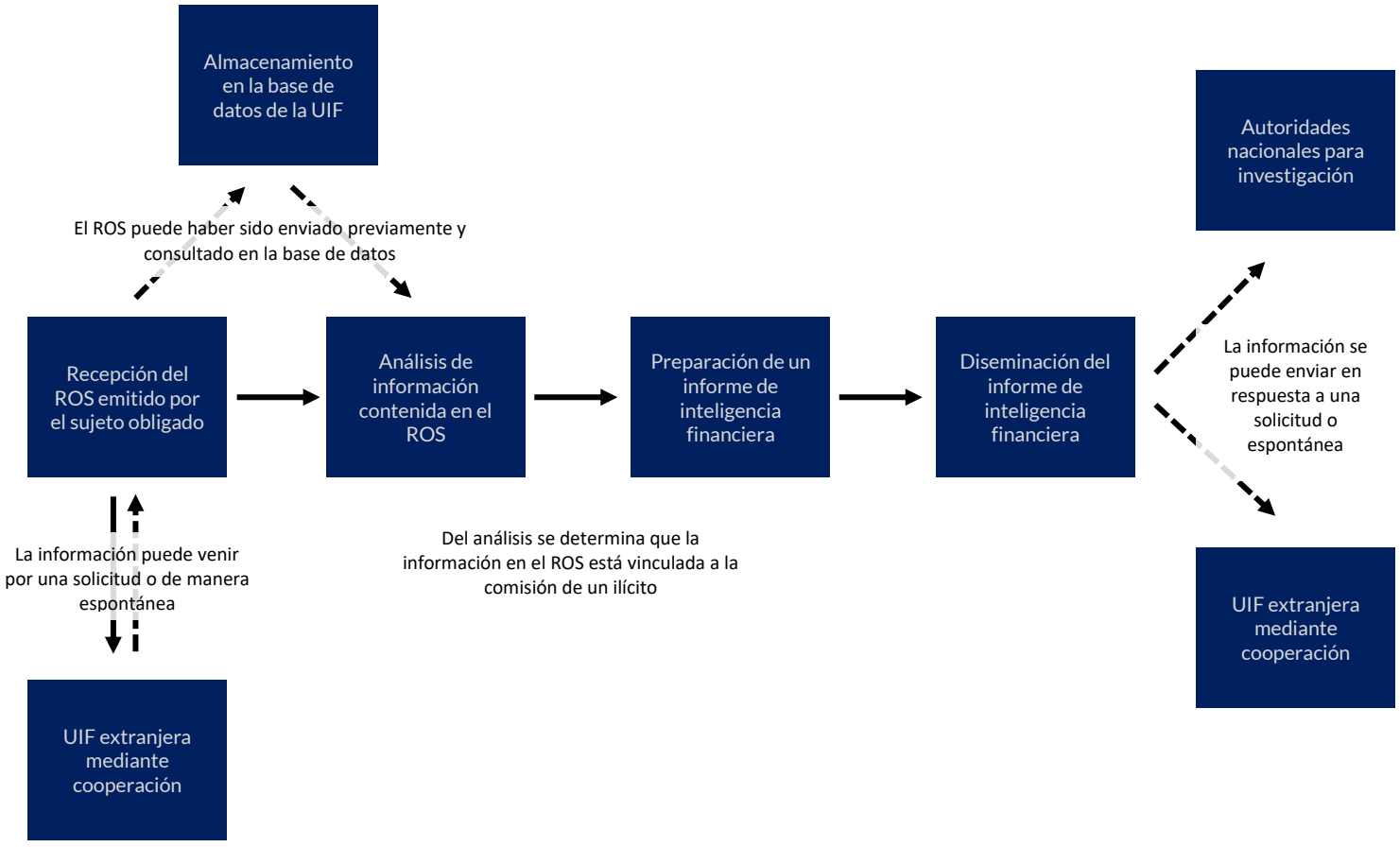
De acuerdo con lo señalado en el documento de Principios Recomendados, la información debe salvaguardarse y estar sujeta a estrictos controles que aseguren que la misma sólo se utilice para los fines autorizados, esto en el caso del intercambio de información entre UIF.

Asimismo, una UIF deberá tomar las medidas pertinentes de concientización para que los terceros hagan un uso apropiado de la información de inteligencia financiera que les es proporcionada, colaborar con los terceros a quienes proporciona información para poder establecer medidas de seguridad y confidencialidad y, en caso de que aun estableciendo las medidas pertinentes se llegara a tener un uso indebido o entrega no autorizada de la información, en el caso de que la información provenga de otra UIF se deberá notificar inmediatamente a ésta última, en tanto que la UIF que recibió la información que ha sido entregada indebidamente deberá tomar las medidas pertinentes para resolver la situación, así como dar certeza de que en el futuro la situación no se repetirá.

III. LA CONFIDENCIALIDAD DE LOS ROS EN EL CONTEXTO DE GAFILAT

Los trabajos mencionados anteriormente hacen referencia a situaciones o momentos específicos en los cuales los ROS se pueden considerar especialmente vulnerables en cuanto a su confidencialidad y seguridad, consistentes en los momentos en los que la información contenida en los reportes se transmite de una institución a otra: del sujeto obligado a la UIF en el caso de la Recomendación 21, entre UIF en el caso de los Principios del Grupo Egmont y de una UIF a una autoridad de orden público en el caso de los Principios Básicos de la CICAD/OEA. Si bien son momentos en los que se debe tener especial atención, es también fundamental tener un manejo confidencial, seguro y responsable de la información de los ROS en las distintas etapas del proceso de inteligencia financiera.

En términos generales se puede decir que el proceso anteriormente referido consta de las siguientes etapas:



a. Vulnerabilidad de la información en el proceso de análisis y cruce de información

El proceso de análisis es, posiblemente, el proceso que más control tiene en cuanto a la seguridad de la información, puesto que se realiza al interior de las instalaciones de la UIF y por parte de los funcionarios de la misma, aspectos que están sujetos a un número amplio de medidas de protección y seguridad, como se verá en capítulos posteriores. No obstante, lo anterior no significa que estén totalmente exentos de la posibilidad de alguna divulgación no autorizada.

En el proceso de análisis es natural que se comience a trabajar con la información disponible de los ROS, bases de datos internas y externas y otras fuentes para realizar cruces de información, lo cual debería llevar a un producto con valor agregado; en algunos casos, la información disponible en se momento a la UIF podría no ser suficiente para poder hacer todas las conexiones requeridas de los sujetos, entidades, productos, instrumentos y conductas delictivas y de otra naturaleza que permitan sustentar el desarrollo de los casos. Es en

situaciones como la descrita en las que se determina que se requiere solicitar más información al sujeto obligado que emitió el ROS o a otros sujetos obligados que se han encontrado conectados en el análisis. En este sentido, al realizar un requerimiento de información, se podría abrir una vulnerabilidad al revelar el tipo de información que se requiere para completar el análisis. Asimismo, dependiendo de los canales de transmisión de los requerimientos y de la información, así como del personal involucrado, principalmente del lado del sujeto obligado, podrían generarse salidas o divulgaciones no autorizadas en caso de que no se tengan las salvaguardas y tratamientos adecuados para el resguardo de la información.

Otra manera en la cual la información podría transmitirse a personal que no tiene la necesidad de tratar dicha información podría darse al realizar consultas entre los propios funcionarios al interior de la UIF, donde información de determinada sensibilidad pudiera ser compartida ante una duda en el análisis o para resolver aspectos de su procesamiento, involucrando a personal que, si bien también está sujeto a condiciones de confidencialidad, no requiere conocer la información. Ésta es una vulnerabilidad que pudiera ser menor frente a otras que tiene la información, especialmente si se considera que la misma puede ser reducida con la implementación de medidas que cubran a todo el personal de la UIF independientemente de su área de adscripción o responsabilidades.

b. Vulnerabilidad de la información en proceso de transmisión entre partes involucradas

Si bien en todas las etapas existen riesgos de que la información pueda ser utilizada de manera indebida o disponible a terceros no autorizados para acceder a la misma, son las etapas en las que la información es entregada en las cuales se han enfocado los esfuerzos y estándares que buscan preservar la confidencialidad de la información. Por ejemplo:

- La Recomendación 21 del GAFI hace referencia específica al momento en el que los sujetos obligados hacen envío de un ROS, al señalar que no se debe informar a otras partes sobre el contenido o la propia presentación de un ROS a las autoridades competentes;
- Los Principios de Intercambio de Información del Grupo Egmont señalan que la confidencialidad de la información se deberá salvaguardar en la información que es intercambiada entre contrapartes con medidas, por lo menos, iguales a las de información obtenida de fuentes nacionales, y;
- Los Principios Mínimos y Guía del Grupo de Expertos para el Control del Lavado de Activos de la OEA establecen medidas para asegurar y proteger la confidencialidad de la información de inteligencia financiera que es difundida a las autoridades de investigación criminal y orden público.

Adicionalmente, con relación a la diseminación de los productos de inteligencia, los cuales proveen valor agregado a partir del análisis de la UIF, estos pueden tener diferentes usuarios dependiendo de la naturaleza del mismo, de la siguiente manera:

- Los informes de inteligencia operativa o táctica se encaminan a servir como insumo o base para investigaciones o casos específicos de lavado de activos, financiamiento del terrorismo u otro tipo de delitos conexos; la UIF puede generar un informe de inteligencia a partir de su análisis y éste derivar en una investigación o caso, o puede darse también el caso inverso, en el cual las autoridades de orden público ya se encuentran desarrollando una investigación y solicitan la colaboración de la UIF para los efectos pertinentes;
- Informes sobre tendencias, métodos y tipologías, los cuales pueden ser de utilidad a las autoridades, así como a entidades del sector privado y al público en general, con el fin de conocer y estar al tanto de los últimos desarrollos y modos de operación de la delincuencia en materia financiera, con lo cual se puede prevenir la comisión de delitos. Estos últimos generalmente omiten la información personal o los datos precisos contenidos en los ROS y presenten información de carácter muy general, lo cual los hace susceptibles de ser compartidos a un público mayor.

Entre las vulnerabilidades que se han detectado en la transmisión de la información se encuentran que los canales de transmisión al usuario de la información (generalmente en el caso de las fiscalías en los informes de inteligencia financiera) no cuenten con la suficiente seguridad. Lo anterior es especialmente cierto cuando la entrega de los informes de inteligencia debe realizarse en un documento impreso, que sirva como sustento para el inicio de las acciones por parte del Ministerio Público. Asimismo, el uso de equipos de comunicación (computadoras, tabletas y teléfonos móviles, principalmente) que no estén cifrados o con protecciones suficientes, o el envío a personal que no tiene una necesidad de conocimiento, podría significar una vulnerabilidad en la entrega.

Lo anterior puede ser atendido por medio de protocolos de entrega de la información (cadenas de custodia o manuales de procedimientos) que establezcan claramente los canales de entrega y recepción, los procedimientos y formalidades, así como las personas o cargos que tienen autorización para realizar dichos procedimientos.

II. MEDIDAS GENERALES DE PROTECCIÓN DE LA SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN DE LOS ROS

a. Marco general de protección a los ROS por parte de las UIF de GAFILAT

A nivel de GAFILAT, y en consistencia con los estándares internacionales, todos los países han establecido dentro de su legislación y normativa la atribución y obligación a los sujetos bajo el régimen ALA/CFT a emitir ROS, de acuerdo con la siguiente tabla:

País	Legislación	Artículo
Argentina	Ley N° 25.246	Arts. 20Bis y 21
Bolivia	Decreto Supremo 24771 de 31 de julio de 1997	Art. 30
Brasil	Ley N° 9.613/1998 (reformada por la Ley N°12.683/2012)	Arts. 9 a 11
Colombia	Decreto Ley 663 de 1993, Estatuto Orgánico del Sistema Financiero; Ley 190 de 1995 y Ley 1121 de 2006	Art. 102 (DL 663 de 1993)
Ecuador	Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos	Art. 4 d) y Art. 5
Estados Unidos de América[2]	Bank Secrecy Act (BSA)	31 CFR, Capítulo X
Guatemala	Decreto No. 67-2001 "Ley contra el lavado de dinero u otros activos" y Acuerdo Gubernativo No. 118-2002 "Reglamento de la Ley contra el lavado de dinero u otros activos"	Arts. 11, 26, 27 y 36 (Ley) y Art. 16 (Reg.)
Honduras	Decreto 144-2014 "Ley Especial contra el Lavado de Activos"	
México	Ley de Instituciones de Crédito (LIC)	Art. 115, Frac. II
Panamá	Ley 23 del 27 de abril de 2015	Art. 54
Paraguay	Ley N° 1015/97 "Que previene y reprime los actos ilícitos destinados a la legitimación de dinero o bienes"	Art. 19
Perú	Ley N°27693, Ley N°29038 y Decreto Legislativo N° 1106	Arts. 3 (núm. 3), 10 y 11 (Ley 27693), Art. 3 (Ley 29038) y Primera Disposición Complementaria (Decreto)
Uruguay	Ley N° 17.835, con modificaciones introducidas por las Leyes 18.494 y 19.355	Arts. 1 y 2

b. Seguridad física y de documentos impresos

La seguridad física es un aspecto fundamental en el proceso de seguridad de un entorno, complementario a la seguridad lógica de sistemas y que se puede apoyar en procesos tecnológicos para su implementación y automatización. El personal a cargo de la misma deberá diseñar políticas y lineamientos que hagan prevalecer la seguridad dentro de un

[2] Los Estados Unidos de América participan en el GAFILAT con calidad de observador. En este sentido, y debido a la importancia de dicho país en el contexto de América Latina, se incluyen ejemplos e información relevante del país.

entorno, de tal manera que se generen mecanismos de protección en torno al principal activo de las UIF, que es la información.

Al respecto de documentos impresos, Si bien la mayor parte de las UIF dentro de la región ha migrado a sistemas de recepción y análisis de los ROS en los cuales se minimice el uso de los documentos impresos, en algunos casos el proceso se encuentra en implementación o aún se tiene la práctica de manejar información impresa principalmente en alguna de las siguientes etapas:

- Recepción de los ROS enviados por los sujetos obligados
- Utilización interna de los documentos para su análisis y procesamiento
- Producción y entrega de informes de inteligencia que se entregan a la fiscalía y otras autoridades relevantes

En el caso de la recepción de ROS enviados por sujetos obligados, la práctica más recurrente al recibirlos en formato impreso es digitalizarlos inmediatamente, tras lo cual el respaldo físico puede destruirse o ser enviado a un archivo físico.

Si bien la migración a los sistemas electrónicos tiene como efecto la reducción del número de documentos físicos que utilizan los analistas, en muchos casos siguen imprimiéndose documentos para su trabajo interno por parte de las UIF, principalmente por temas de practicidad y facilidad en el manejo. Para tales efectos, se tienen diversas medidas implementadas entre las UIF de la región para evitar que dichos documentos impresos sean difundidos de manera accidental o voluntaria, como son protocolos de destrucción de los documentos una vez que se ha concluido su utilización, su almacenamiento en bóvedas o archivos con controles restringidos de acceso y la revisión de los documentos que portan los funcionarios a la conclusión de la jornada laboral, entre otros; combinados con las restricciones de acceso de equipos de fotografía o grabación, incluyendo los teléfonos móviles y equipos de cómputo, se minimiza la posibilidad de que documentos de uso interno de las UIF salgan de las instalaciones de la misma.

Por lo que respecta a una política efectiva y eficiente sobre el ingreso o salida de documentación impresa, se sugiere contar con registros precisos en las entradas donde se pueda especificar el tipo de documentación que se porta y reforzar dicha tarea con autorizaciones especiales para aquellas áreas que por el origen de sus actividades requieren ingresar o extraer documentación impresa.

Una medida efectiva empleada por parte de la UIF de México para asegurar un correcto control sobre la responsabilidad de sacar información impresa es el uso de papel con distintivos o “marcas de agua” difíciles de detectar a simple vista, que permitan relacionar a un sujeto con el documento extraído. En adición a lo anterior, se ha implementado una política de restricción de impresión de documentos.

Otra medida que es posible implementar es un sistema de seguimiento de los documentos, donde se registran las credenciales de acceso del usuario que imprimió los archivos o que está llevando el caso. Lo anterior cumple una doble función, pues otorga la responsabilidad concreta del cuidado de dicha información y documentación al funcionario que la utiliza, a la vez que permite trazar donde pudo darse alguna fuga en caso de que la información sea divulgada sin autorización. Sistemas como el anterior son utilizados en UIF de Perú, concretamente.

c. Seguridad informática

De acuerdo con la recopilación realizada, un número significativo de UIF de la región ha migrado a sistemas informáticos para la recepción de los ROS, lo cual tiene un número de ventajas y desventajas, comparativamente con la recepción en papel:

Ventajas de un sistema en línea	Desventajas de un sistema en línea
Permite la incorporación inmediata a la base de datos de la UIF	Requiere adecuación de sistemas informáticos y de conectividad de los Sujetos Obligados
Se le puede dar una trazabilidad a los equipos que tienen acceso a los ROS	Requiere de un proceso de alta en el sistema, el cual puede requerir de un proceso demorado al momento de ser implementado
Se puede restringir el acceso de información a aquellas personas que deben conocer del caso por sus funciones	La información puede pasar por varias personas antes de ser transmitida, por lo que es más factible que se divulgue o se haga un uso inadecuado de la misma
Permite la carga en bloque de los ROS	Elevados costos de implementación y capacitación
Permite validar en tiempo real los campos solicitados en formulario ROS	Compra de herramientas informáticas especializadas costosas
Permite la carga de documentos adjunto de sustento de envío ROS	Requiere de una solución de almacenamiento robusta

Con relación a las desventajas se puede observar que, en algunos de los casos, las mismas se presentan únicamente en los casos en los que recién se busca implementar el sistema, como son la generación de un elevado número de usuarios, la capacitación en el uso de la plataforma y los problemas técnicos que, habitualmente, son más recurrentes en un inicio. También las limitaciones en la asignación y ejercicio de los presupuestos pueden tener un impacto en la implementación de sistemas tecnológicos seguros.

Entre las medidas de seguridad que se han implementado en algunos de los países con la finalidad de proteger las instalaciones de las UIF, se incluyen las siguientes:

- Accesos con credencial personal o biométrico a las instalaciones;
- Diferenciación de niveles de acceso, dependiendo del rango del funcionario y del área de adscripción;
- Instalación de sistemas de circuito cerrado;
- Restricción o prohibición total al ingreso de sistemas de computación (notebooks, tabletas, teléfonos móviles, etc.) o medios de almacenamiento y otros dispositivos de grabación a las instalaciones de la UIF;
- Inhabilitación de utilización de memorias USB

Ejemplo 1. Políticas aplicables en la IVE (Guatemala) para equipos propiedad de la UIF o que contienen información de la UIF

- Todo equipo de cómputo portátil propiedad de la UIF que sea asignado a un funcionario deberá tener activo el cifrado de su disco duro y deberá solicitar PIN de arranque del sistema operativo al momento de encender el equipo.
- Los dispositivos de almacenamiento portátil autorizados para escritura de información deberán cifrarse y estar protegidos con contraseña.
- Todo dispositivo móvil (teléfono celular o tableta) que contenga información Institucional, deberá gestionarse se manera que se garantice la protección de la información y/o la limpieza remota del dispositivo en caso sea reportado como robado o perdido.

d. Seguridad del personal

Las medidas de seguridad implementadas con relación al personal que trabaja en las UIF se pueden dividir, en términos generales, en dos momentos principales:

Momento de la incorporación del funcionario

En el momento del ingreso o incorporación del funcionario, algunas de las UIF que integran el GAFILAT realizan, en adición a las pruebas habituales para el ingreso a un trabajo, tienen otro tipo de requisitos como son la firma de declaraciones juradas y acuerdos de confidencialidad, la aplicación de pruebas de control de confianza que incluyen (sin necesariamente limitarse a) exámenes toxicológicos y pruebas de polígrafo, entre otras.

Seguimiento de las labores del funcionario

Algunas de las medidas generalmente implementadas para efectos de garantizar la seguridad de la información por parte del personal incluyen la prohibición de uso de teléfonos móviles o equipos de cómputo o almacenamiento personales, así como la portación de credenciales de identificación en todo momento.

En las legislaciones de algunos países del GAFILAT se tienen disposiciones en las que no se puede revelar el nombre del personal adscrito a la UIF por motivos de seguridad, lo cual está plasmado en las leyes de protección de información, transparencia o acceso de información pública, con lo que se protege la identidad de los funcionarios. Esta medida es especialmente relevante para los casos de los países que, por ley, no permiten el llamado de analistas y otros funcionarios a comparecer, testificar o dar opinión pericial en procesos judiciales.

Accesos de los funcionarios y colaboradores de la UIF

Independientemente de los controles de confianza a los que estén sujetos los funcionarios y colaboradores de la UIF, se considera necesario contar con políticas que señalen la responsabilidad y compromisos que adquieren los funcionarios al ingresar a las instalaciones de la UIF. A manera de ejemplo se mencionan algunos de los controles implementados por parte de la UIF de México[3]:

- Exclusa o puerta de acceso debidamente reforzada
- Punto de inspección visual
- Uso de bandas de rayos X para la inspección de bolsos, mochilas u otros objetos
- Arco detector de metales
- Paleta de detectora de metales portátil
- Cámaras de seguridad y sistema de circuito cerrado
- Personal calificado de reacción ante incidentes
- Revisión a vehículos que ingresen a las instalaciones por medio de inspecciones personales y uso de espejos
- Área de espera separada de las instalaciones donde el personal desempeña sus funciones

e. Seguridad en el proceso de diseminación a terceras partes.

En la práctica totalidad de los acuerdos y memorandos de entendimiento (MDE) que se firman utilizando los modelos y requisitos consistentes con los estándares se incluyen cláusulas en las que se establece que la información que es recibida por una UIF de parte de una homóloga

[3] El listado presentado menciona solo algunas de las características de los controles de acceso a las instalaciones de la UIF de México y no es exhaustiva a todos los controles implementados en la actualidad o que pudieran ser implementados en un futuro.

extranjera deberá ser tratada, como mínimo, con las mismas medidas y protocolos de protección que son aplicables a la información que proviene de fuentes nacionales.

En un número elevado de UIF de la región no se hace entrega del ROS recibido por parte del sujeto obligado, sino que la información contenida en el mismo hace parte del informe de inteligencia financiera que es difundido a las autoridades relevantes, como pudiera ser la fiscalía. Adicionalmente, en estos casos no se hace identificación concreta del sujeto obligado que presenta propiamente el ROS, con lo que se busca proteger la identidad de la entidad que reporta.

III. PRINCIPALES DESAFÍOS EN LA PROTECCIÓN DE ROS

a. Recepción de ROS e información de inteligencia financiera por parte de sujetos obligados y contrapartes extranjeras

Disposiciones relacionadas con la información sobre emisión de ROS

La protección de la información contenida en un ROS comienza desde el momento en el cual la operación que lo justifica es realizada o intentada y las estructuras o personal encargados del cumplimiento de los Sujetos Obligados deciden emitir un ROS. En este momento, en seguimiento a los estándares internacionales, todos los países deben contar con medidas en las cuales se prohíba expresamente revelar la información contenida en un ROS o incluso el hecho de que el mismo es emitido a la UIF.

Dado que esta protección se encuentra contenida en las Recomendaciones del GAFI, los países han desarrollado disposiciones por medio de las cuales expresamente se hace esta prohibición.

Intercambio de información internacional con estructuras de cumplimiento ubicadas en distintos países

De acuerdo con la interpretación de los ordenamientos jurídicos vigentes en la actualidad dentro de la región, no se tienen disposiciones por medio de las cuales se regule si un Sujeto Obligado ubicado en uno de los países de la región pueda informar a una entidad del sector privado, fuera de dicho país (generalmente en el país donde se encuentra la oficina matriz o controladora del Sujeto Obligado local) sobre la emisión de un ROS para efectos de un programa de cumplimiento conjunto. En este sentido, de acuerdo con las experiencias recopiladas, la práctica recurrente de interpretación relacionada con el tema sería que, al no existir una regulación específica, los sujetos obligados NO estarían en posibilidad de compartir dicha información con otras entidades de su mismo grupo económico fuera del país; no obstante, se tiene también la experiencia de interpretación en la que, ante la ausencia de una restricción expresa, las entidades que forman parte de un mismo grupo financiero estarían en posibilidad de informarse mutuamente sobre la presentación de un ROS.

Ejemplo 2. Legislación mexicana relacionada con la posibilidad de las instituciones financieras de compartir información relacionada con delitos de LA/FT

De acuerdo con lo señalado en las Disposiciones de carácter general a las que hace referencia el Art. 115 de la Ley de Instituciones de Crédito, las entidades podrán intercambiar información sobre operaciones siempre y cuando se busque fortalecer las medidas de prevención y detección de delitos de LA/FT.

b. Consulta o entrega no autorizada de la información contenida en los ROS

Ante casos en los cuales se diera una divulgación o entrega no autorizada de información contenida en los ROS a un tercero, las UIF disponen de un marco legal que guía las actuaciones relevantes. En términos generales, las legislaciones que establecen u otorgan facultades a las UIF son las que establecen directamente que el personal adscrito a las mismas deberá guardar la confidencialidad de la información y somete a quien proporcione indebidamente información a un tercero a sanciones administrativas, sin prejuzgar de las responsabilidades penales a las que el funcionario pudiera estar sujeto.

Uno de los retos que es importante atender en materia de confidencialidad es asegurar que todas las autoridades y funcionarios relevantes estén propiamente capacitados y concientizados con relación a la protección de la información de inteligencia financiera. En algunos casos se ha encontrado que los usuarios de la información en las agencias de investigación y orden público no están muy familiarizados con la necesidad de proteger la inteligencia financiera, lo cual se debe atender acercándose a dichas autoridades y dando el debido seguimiento a dichos esfuerzos.

c. Uso de la información proveniente de los ROS por parte de autoridades investigativas y de orden público

Revelación de la identidad de los sujetos que emiten reportes de operación sospechosa

Entre algunos países del GAFILAT no se tiene contemplada la remisión de los ROS a las autoridades investigativas para llevar los casos, sino que se aporta valor a la información recibida. Para efectos de la diseminación del análisis de operaciones sospechosas y otra información relevante a la que tienen acceso las UIF en la región, como podría ser información de bases de datos o reportes de operaciones distintos a los sospechosos que se establezcan en los regímenes legales, las UIF de la región elaboran informes de inteligencia financiera que aportan herramientas a los órganos competentes.

Con relación a la información que contemplan los citados reportes, se tiene una disparidad en cuanto al contenido de información relacionada con los sujetos obligados emisores del informe, puesto que en la mitad de los casos se informó que los informes de inteligencia hacen referencia a la fuente de la que provienen, incluyendo el sujeto que emite el reporte, mientras que la otra mitad de los países señaló que la identidad del sujeto obligado que remite el reporte no se indica en el informe de inteligencia.

Uso de los informes de inteligencia financiera por parte de los sistemas de inteligencia

En algunos de los países que conforman la región, las UIF forman parte de un sistema de inteligencia que no solamente se dedica al análisis de casos relacionados con LA/FT, sino que conforman un sistema integral de inteligencia para la seguridad nacional que abarca las distintas amenazas a la seguridad de la población, el Estado y las instituciones.

Inclusión de los informes de inteligencia financiera en los procesos judiciales

Entre algunos países de GAFILAT no se tiene contemplado que los informes de inteligencia financiera tengan, por definición, carácter probatorio y se consideran solo para fines de desarrollo de inteligencia. No obstante, en algunos casos las UIF podrán elaborar productos de inteligencia especiales u otorgar autorización para que los informes ya diseminados puedan ser utilizados en procedimientos, con el carácter necesario.

Concretamente, la Unidad de Análisis Financiero y Económico (UAFE) del Ecuador es parte del subsistema de inteligencia, de acuerdo con la Ley de Seguridad Pública del Estado. En tal carácter, se tiene la facultad de compartir la información de un ROS, de manera excepcional y en cumplimiento de sus funciones de combate a los delitos de LA/FT, en atención a los requerimientos de la Secretaría Nacional de Inteligencia conservando en todo momento el sigilo o reserva de la información

Protección de Sujetos Obligados con relación a la emisión de ROS

Es una práctica recurrente dentro de los países de GAFILAT que se cuente con una disposición relacionada con la exención de responsabilidad para personal en las áreas encargadas de cumplimiento y/o emisión de ROS ante el uso de información. Lo anterior es una disposición que se considera adecuada, en términos de las comunicaciones sobre potenciales operaciones vinculadas a LA/FT de buena fe.

A continuación, se presenta, a manera de ejemplo el Art. 18 de la Ley N° 25.246 de la República Argentina:

Artículo 18. – El cumplimiento, de buena fe, de la obligación de informar no generará responsabilidad civil, comercial, laboral, penal, administrativa, ni de ninguna otra especie.

Asimismo, se incluye el Artículo 30 de la Ley Contra el Lavado de Dinero u Otros Activos, Decreto 67-2001 del Congreso de la República de Guatemala:

"Artículo 30. Exención de responsabilidad. Se exime expresamente de responsabilidad penal, civil o administrativa, y de cualquier tipo a las personas obligadas, sus propietarios, directores, gerentes, administradores, funcionarios, representantes legales y empleados debidamente autorizados que hubieren proporcionado la información en cumplimiento de esta ley."

Participación de funcionarios de las UIF en procedimientos judiciales

De acuerdo con la información recopilada, a nivel regional esta participación se puede dar de tres maneras:

Los funcionarios de la UIF no son llamados dentro de los procedimientos	**Los funcionarios de la UIF pueden participar en los procedimientos, con base en los informes realizados**	**Los funcionarios de la UIF pueden participar en calidad de peritos, pero no vinculado al desarrollo de informes**
En estos casos existe una protección legal que impide a los jueces citar a personal de la UIF involucrado en el análisis y desarrollo de informes de inteligencia a comparecer ante tribunales, ya sea en calidad de peritos o para sustentar su informe	Los analistas pueden ser citados a declarar o prestar testimonio en procesos penales relacionados LA/FT o en otros procesos (acción de extinción de dominio), derivado de las denuncias e informes que se presentan al ente investigador, con la finalidad de sustentar dichos documentos.	El personal puede participar en calidad de testigo pericial dentro de procesos judiciales en los casos, debiendo comparecer a audiencias, con la posibilidad de ser interrogados.
Ejemplos de países		
Colombia	Ecuador, Guatemala, México[4], Perú	Guatemala

Un caso singular es el de los Estados Unidos de América, donde, si bien la Ley no establece ninguna restricción a que se pueda dar un citatorio a un analista de FinCEN, no se tienen registros de que haya sucedido tal situación; lo que sí ha sucedido es que se ha llamado a agentes especiales de FinCEN a testificar como custodios de registros relacionados con los requisitos de la Bank Secrecy Act que hayan sido certificados por parte de FinCEN como evidencia en procedimientos penales.

[4] En el caso de México, se podrá llamar a funcionarios de la UIF únicamente cuando ésta tenga el carácter de denunciante de delitos de LA/FT. Adicionalmente, para salvaguardar la identidad de los funcionarios, con base en la legislación vigente, el Órgano Judicial se abstendrá de poner en vista de las demás partes los datos de identificación del funcionario de la UIF.


GAFILAT