17th St. & Constitution Avenue N.W.
Washington, D.C. 20006
Estados Unidos de América

Organización de los Estados Americanos

T. 202.458.3000
www.oas.org

QUINCUAGÉSIMO SEGUNDO PERÍODO ORDINARIO DE SESIONES
Del 28 al 30 de noviembre de 2012
San José, Costa Rica

OEA/Ser.L/XIV.2.52
CICAD/doc.1982/12
24 noviembre 2012
Original: Inglés

MEJORES PRÁCTICAS RECOMENDADAS POR EL GRUPO DE TRABAJO PARA LA COORDINACIÓN E INTEGRACIÓN DE UIF/OIC GRUPO DE EXPERTOS PARA EL CONTROL DEL LAVADO DE ACTIVOS

OEA/Ser.L/XIV. 4.34
CICAD/LAVEX/doc.2/12
11 mayo 2012
Original: Inglés

Abril 26 de 2012

Mejores Prácticas Recomendadas por el Grupo de Trabajo para la Coordinación e Integración de UIF/OIC
Organización de Estados Americanos, Comisión Interamericana para el Control del Abuso de Drogas CICAD (OEA/CICAD)

En el uso y protección de la información de la UIF

El intercambio de información entre las Unidades de Inteligencia Financiera con sus homólogas del exterior es de capital importancia ya que les permite dar un mayor valor agregado a los análisis enviados a las autoridades y a la vez incrementa el impacto de las investigaciones llevadas a cabo a partir de ellos. Es por esto que es necesario que este intercambio se desarrolle de una manera segura y eficiente, utilizando protocolos previamente establecidos que garanticen el uso adecuado de la información y que prevean marcos de acción en caso de presentarse accesos no deseados a la información intercambiada.

Las fugas de información en las UIF pueden tener efectos devastadores en la reputación de aquellos sobre cuya información personal ha sido divulgada de forma inapropiada, especialmente si no han sido acusados de algún crimen o no han sido encontrados culpables después de un proceso judicial. Las fugas de información también comprometen las investigaciones de las agencias de cumplimiento de la ley, ponen sobre aviso a los involucrados en una investigación y erosionan la confianza de los sujetos obligados en el régimen de lucha contra el Lavado de Activos y la Financiación del Terrorismo.

Para incrementar la atención en este tema, el Grupo de Trabajo de Integración entre UIF y OIC del Grupo de Expertos para el Control de Lavado de Activos de la CICAD/OEA, ha identificado estos principios para el uso y protección de la información producida por las UIFs. Consistentemente con los principios en el uso y protección de la información que posee cada UIF, las mismas deben diseñar e implementar sistemas internos, procedimientos y controles para garantizar la confidencialidad de la información que ellos reciben de las contra-partes del extranjero y compartirla con la autorización de las partes interesadas. Esto incluye sus propios reportes cualquier y otra información que contenga información derivada de la fuente original que puede ser una UIF del exterior u otra agencia de una jurisdicción del extranjero.

Dada la importancia de asegurar el uso apropiado y protección de la información de la UIF por terceras partes, de la misma forma en que se hace por medio de los procedimientos y controles implementados en la UIF, es necesario tener en cuenta mejores prácticas desde el momento en que es recibida la información proveniente de una UIF del exterior, hasta el momento en que es diseminada a un tercero interesado, y otros dentro del proceso, o la misma es destruida. Estos sistemas, procedimientos y controles deben asegurarse de que la información que pertenece a una jurisdicción extranjera, así como cualquier referencia al nombre de la institución extranjera que compartió la información, esté debidamente protegida de entregas no autorizadas. Tales sistemas, procedimientos y controles deben incluir, pero no limitarse a lo siguiente:

Funcionarios de la UIF que manejan la información

- La UIF debe seleccionar cuidadosamente las personas encargadas de recibir y manejar la información de jurisdicciones extranjeras. Los nuevos funcionarios deberían someterse a una investigación de antecedentes para asegurarse de que solo personal con alta integridad y honestidad son vinculados para manejar la información sensible de la UIF.
- Los empleados, contratistas y consultores de la UIF con acceso a informaciones provenientes de UIFs extranjeras deben tener en cuenta y cumplir con los requerimientos de seguridad para el manejo de información sensible, especialmente la información enviada por una jurisdicción extranjera.
- Los empleados con acceso a información sensible de la UIF deben tener en cuenta que divulgar información sensible sin la autorización apropiada puede tener serias consecuencias, incluyendo acciones administrativas, disciplinarias o penales (como por ejemplo la terminación de la relación contractual)
- Las UIFs deberían proveer entrenamiento apropiado y continuo a los empleados con el fin de que reconozcan y salvaguarden la información sensible que soporta su misión y operaciones.

Recepción de la información en la UIF

- Cuando una UIF recibe información sensible o información equivalente de otras UIF, la información debe ser manejada de acuerdo con los lineamientos proporcionados por la UIF que envió la información. En el caso de que tales no se provean, debe ser manejada de acuerdo con las políticas de recepción de la UIF que las recibe.
- Las UIFs deberían aceptar solicitudes de información y respuestas a requerimientos hechos desde el exterior electrónicamente, y esta información debería ser encriptada para el proceso de transmisión. De igual forma, la UIF debería responder a un solicitante utilizando el mismo sistema seguro que el solicitante original utilizó para transmitir la información.
- El remitente de un requerimiento de información es quien determina si la información debe ser enviada por medio de un mensaje encriptado o por otros medios. Si el

remitente de una solicitud determina que el correo electrónico provee suficiente protección y envía la información de forma electrónica, el destinatario podría enviar su respuesta utilizando el mismo medio.

Categorización de la información de una UIF del extranjero como "Sensible"

- Como regla general, la UIF receptora debería manejar la información suministrada por otra UIF como "Sensible", y solo debería utilizarla para los propósitos específicos para los cuales la información fue buscada o suministrada.
- Cuando se envía información sensible fuera de la UIF, los documentos deben incluir una declaración alertando al destinatario en una carta de entrega o directamente en el documento, del contenido con información sensible.

> *Por ejemplo:* Este documento hace parte de la información sensible de la UIF (citar el nombre de la UIF). No debe diseminarse sin la expresa autorización de (citar el nombre de la UIF). Refiera las solicitudes y preguntas sobre este documento a (insertar el nombre y dirección de la UIF remitente).

Procedimientos generales de manejo

- Una UIF no puede transferir la información compartida por una UIF del extranjero a una tercera parte sin el previo consentimiento de la UIF que entregó la información.
- Todas las UIFs deberían utilizar la mayor precaución cuando estén manejando información suministrada por otra UIF, con el fin de prevenir cualquier uso no autorizado que resulte en la violación de la confidencialidad.
- La información de otra UIF será tratada y protegida con la misma confidencialidad y reserva que la información que pertenece a la UIF que la recibe.
- Las UIF deberían implementar un registro especial para monitorear y controlar los reportes de información de inteligencia financiera provenientes de las UIFs del extranjero. El registro especial debería contener la información del solicitante, la fecha en que fue recibida, ingresada, asignada a un analista y respondida, y organizada de forma que permita la elaboración de reportes estadísticos incluyendo la evaluación de la eficiencia en la cooperación.

Protección de entrega no autorizada por parte de terceros

- Se recomienda que las UIFs conlleven dos tipos de expedientes: el expediente de consulta principal y el expediente de intercambio de información, además de una copia de seguridad de este último en una caja de seguridad. Esta práctica puede ser una buena

solución para las unidades de inteligencia que, por ley, deben hacer que la información financiera esté a disposición del poder judicial del país.

- La UIF debería anotar en el archivo principal (aquel que originó la solicitud), el requerimiento hecho por su contraparte en el extranjero.
- En el inicio de una relación entre la UIF y terceras partes con acceso a la información de la UIF, se recomienda evaluar la firma de un memorando de entendimiento con la UIF estableciendo las condiciones de la relación de intercambio de información.
- Los sistemas internos de correo electrónico deberán proveer salvaguardias suficientes para permitir la transmisión de la información sensible cuando la UIF opera dentro de una red de área local.
- La información sensible de la UIF debe ser reproducida en las impresoras disponibles en la oficina en la cantidad necesaria para llevar a cabo los asuntos oficiales.
- Debería utilizarse una hoja de portada para prevenir la entrega inadvertida o no autorizada cuando la información sensible de la UIF es trasladada de ubicaciones de almacenamiento no autorizadas, cuando se encuentran presentes personas sin necesidad de saber o cuando la observación casual pueda revelar la información sensible de la UIF.
- La información que se reciba de otras UIF extranjeras no puede ser transferida a otras entidades o personas legales o individuos sin el consentimiento expreso de la unidad que proporcionó la información.
- Cuando se esté enviando información a una UIF del extranjero, debe colocarse una hoja de portada dentro del sobre en la parte de arriba de la carta de remisión, memorando o documento.
- Cuando sea necesario enviar copias físicas de la información sensible de la UIF a través de pisos y/o departamentos dentro de la UIF, los documentos deberían estar en un sobre individual opaco y/o un contenedor seleccionado para prevenir su apertura inadvertida o que revele la evidencia de una posible manipulación. El sobre o contenedor debería mostrar el nombre completo del remitente y el destinatario

Almacenamiento

- La información reservada de la UIF debe ser almacenada, como mínimo, en un archivero, cajón o gaveta de escritorio, compartimiento superior, aparador, compartimento cerrado o similar.
- La información reservada de la UIF debe ser almacenada en un cuarto o área dotada de control de acceso físico como un cuarto cerrado bajo llave, o en un área de trabajo restringida controlada por un seguro de clave o un lector de tarjeta.

Diseminación y acceso

- El acceso a la información reservada de una UIF extranjera debe hacerse con base en la necesidad de saber, según sea determinado por el titular de la información. Sin embargo, cuando haya incertidumbre de si una persona tiene necesidad de saber, el

titular de la información deberá solicitar las instrucciones de difusión a su supervisor de nivel superior o al gerente.

- Las personas que tengan información de una UIF del extranjero deben cumplir con cualquier acceso adicional y / o restricción de difusión que podrá ser citada en el documento.
- Las UIFs que soliciten información de las UIFs extranjeras deben revelar el destinatario de la información. La autorización para divulgarla a partes adicionales debe ser obtenida antes de su difusión.
- El nombre de la UIF extranjera debe ser ocultado como la fuente, así como de otros identificadores, tales como números de control de documentos antes de las acciones de la UIF que solicitan esa información con terceros.
- Las agencias de cumplimiento de la ley con acceso a la información de los Reportes de Operaciones Sospechosas (ROS) y la información derivada de la UIF local o en conexión con información recibida de una UIF, deberían utilizar esta información de guía cuando el investigado pueda conducir a evidencia de actividad criminal.
- La UIF debería evaluar la firma de Memorandos de Entendimiento (MOU, por sus iniciales en inglés), con terceras partes que tendrán acceso a la información de la UIF en el que se defina la relación de intercambio de información.
- La UIF debería requerir a los usuarios, solicitantes y destinatarios de su información mantener una copia o anotación de las alertas sobre la confidencialidad de todos los documentos relacionados con la UIF, de la forma en que se comparten con la agencia, tanto con los investigadores de las agencias de cumplimiento de la ley, como con los fiscales.
- En vista de que la información es compartida, existe una mayor vulnerabilidad en aquellos receptores que puedan tener un menor entendimiento de la confidencialidad de la información. De esta forma, la UIF debería conservar una bitácora de la información de la UIF y/o información de una UIF del extranjero que puede ser entregada a otras agencias.

Órdenes de protección

- En los casos en que las autoridades judiciales insistan en la presentación de evidencias o ROS de una UIF del extranjero como evidencia en procesos judiciales, la UIF debería, (si el ordenamiento legal se lo permite), trabajar con la oficina del Fiscal para solicitar medidas de protección contra la entrega de tal información. El Departamento legal de la UIF debería contactar a su contraparte dentro de su jurisdicción para determinar el alcance y debido proceso de tales instrumentos legales.

Reporte de Incidentes

- Los empleados o personal contratista que observen o estén al tanto de la pérdida, compromiso, sospecha de compromiso, o entrega no autorizada de información confidencial de una UIF del extranjero, deben reportar inmediatamente, al oficial de

seguridad, otro oficial competente o titular de la UIF, si no existe un departamento de seguridad u otro departamento competente.

- El titular de la UIF, o el oficial que actúa a su nombre, debería reportar sin dilación al titular de la UIF, o al enlace competente, del extranjero la divulgación no autorizada de información confidencial.

- El titular de la UIF, o el oficial que actúa a su nombre, habiendo detectado la diseminación no autorizada de la información sensible de una UIF del extranjero, debe ordenar una completa investigación para determinar los detalles y preparar un reporte para ser entregado a la UIF del extranjero que suministró la información, incluyendo lo siguiente:

    a) Si hubo o no un incidente. Si no hubo pérdida, compromiso, o diseminación no autorizada, las personas responsables de la investigación deberían confirmarlo;

    b) Los eventos que conllevaron a la diseminación no autorizada de información;

    c) Qué información fue diseminada, y si la información era reservada de las agencias de cumplimiento de la ley;

    d) Cómo fue divulgada la información;

    e) A quién le fue revelada la información;

    f) Qué funcionarios gubernamentales tuvieron acceso a la información;

    g) La(s) persona(s) responsable(s);

    h) Las causas del incidente;

    i) Las acciones que fueron tomadas para minimizar el daño o neutralizar potenciales compromisos adicionales.

- La UIF debe mantener el hecho de que se presentó una entrega no autorizada de información tan confidencial como sea posible desde el momento en que se tenga conocimiento del incumplimiento hasta el final de la investigación.

Rendición de cuentas por parte de terceros

- Si se ha detectado la fuga de información que pertenece a una UIF del extranjero, y no se ha identificado dentro de la UIF la persona o personas responsables, la UIF debería contactar los destinatarios externos de la información tales como agentes del cumplimiento de la ley y fiscales con quienes la información haya podido ser compartida. Una vez se hayan contactado las agencias, la UIF debería explicar los roles o responsabilidades de las personas que poseen la información reservada no autorizada proveniente de una UIF del extranjero, de acuerdo con los principios para el Uso y Protección de la Información de la UIF.

- La UIF debería apoyar al tercero o al solicitante, a identificar cualquier documento que pueda haber sido recibida de la UIF que contenga la información que involucre a la UIF del extranjero.

- Si luego de revisar la respuesta del tercero, la UIF encuentra una entrega no autorizada, debe solicitar al tercero llevar a cabo una investigación completa para determinar los detalles y preparar un reporte para ser entregado a la UIF del extranjero que contenga lo siguiente:

    a) Un reporte de la confirmación de la revelación de un reporte de información que contenía información de una UIF del extranjero;

    b) Si la información fue compartida con personas naturales o jurídicas, oralmente o por escrito, local o internacionalmente a contra-partes u otros a través de cartas rogatorias o tratados de asistencia judicial mutua;

    c) Qué información fue revelada;

    d) La persona o personas responsables;

    e) Las acciones tomadas para minimizar el daño o neutralizar los potenciales compromisos adicionales.

- En seguimiento a la solicitud de la UIF; la tercera parte debería conducir una investigación de los eventos que conllevaron a la entrega no autorizada. En este caso la UIF debería:

    a) Tramitar, si es apropiado, la firma de un Memorando de Entendimiento (MOU, por sus iniciales en inglés), con aquellas partes interesadas (usuarios de la información de la UIF);

    b) Si fuera necesario, la UIF debería compartir los lineamientos para el uso y la protección de los reportes con las partes interesadas locales tales como los agentes de cumplimiento de la ley, autoridades judiciales que usan su información.

- Los Reportes de Operaciones Sospechosas (ROS) y la información derivada de la UIF local o la información que esté relacionada con la información recibida de otra UIF, debería ser utilizada como información de guía de tal forma que cuando sea investigada, pueda conducir a la evidencia de actividades criminales.

- La UIF y las terceras partes nunca deberían revelar el hecho de que un ROS existe, o que un ROS ha sido ingresado localmente o en una jurisdicción del extranjero a (1) ninguna persona que esté relacionada en el ROS, (2) entidades privadas que buscan información de conformidad con una investigación en curso o (3) a cualquier tercero no competente

(p.e entidades diferentes a las agencias gubernamentales centrales o estatales que apoyen la evaluación de instituciones financieras, investigaciones, juicios o llevando a cabo actividades de inteligencia o contra inteligencia para protegerse contra el Lavado de Activos o el Financiamiento del terrorismo);

- Las UIF o terceras partes nunca deberían adjuntar o referenciar la información de un ROS perteneciente a UIF del extranjero en acusaciones para búsqueda, decomiso, citaciones, acusaciones, documentos de acusación, mociones, respuestas a las mociones o notas de prensa.

- Se recomienda que cuando estos documentos sean almacenados, las autoridades responsables separen los ROS de los archivos de casos oficiales y tomen precauciones adicionales cuando se graben casos con varios ROS en un Disco Compacto o Medio de Almacenamiento Magnético.

- En algunas jurisdicciones, los Reportes de Investigación (ROI) preparados por el personal de las agencias del cumplimiento de la ley están sujetos a ser revelados a los defensores en los casos, por esta razón, los ROI deberían describir las transacciones y no deberían hacer referencia a los ROS que contengan cualquier información que podría revelar que un ROS fue entregado.

- Las terceras partes siempre deberían utilizar documentos de soporte suministrados por la UIF como evidencia en la judicialización de un caso y no los ROS o la información suministrada por una UIF del extranjero que solo constituye acusaciones no sustanciadas o sospechas.