



Prevención de Lavado de Activos y Financiamiento del Terrorismo



Contenido

Novedades
Normativas

Avisos
Importantes

Actualidad





ÍNDICE

NOVEDADES NORMATIVAS

1. [Reglamento de la Ley N° 30424, Ley que regula la Responsabilidad Administrativa de las Personas Jurídicas](#)
2. [Reglamento del Decreto Legislativo N° 1372, Decreto Legislativo que regula la obligación de las personas jurídicas y/o entes jurídicos de informar la identificación de los beneficiarios finales](#)

AVISOS IMPORTANTES

1. [Informe Anual del Oficial de Cumplimiento \(IAOC\) de los sujetos obligados supervisados por UIF-Perú](#)
2. [Plazo para remitir Reporte de Operaciones Sospechosas \(ROS\)](#)
3. [Reserva de la Identidad del Oficial de Cumplimiento](#)

ACTUALIDAD

1. [Atentados terroristas: el importantísimo rol del Oficial de Cumplimiento, a propósito del último atentado producido en Colombia](#)
2. [Los casos más importantes por violación de la Ley de Prácticas Corruptas en el Extranjero \(Fcpa\) del 2018](#)



1 Reglamento de la Ley N° 30424, Ley que regula la Responsabilidad Administrativa de las Personas Jurídicas

Mediante Decreto Supremo N° 002-2019-JUS, vigente desde el 10.01.2019, se reglamenta la Ley N° 30424 que regula la responsabilidad administrativa de las personas jurídicas. El referido reglamento desarrolla las características, principios, procedimientos y etapas que pueden contemplar o tomar en cuenta las personas jurídicas, que voluntariamente adopten un modelo de prevención para los delitos de cohecho activo transnacional, cohecho activo genérico, cohecho activo específico, colusión, tráfico de influencias, lavado de activos y financiamiento del terrorismo.

Se aplica a las entidades de derecho privado, asociaciones, fundaciones, organizaciones no gubernamentales, comités no inscritos, las sociedades irregulares, los entes que administran un patrimonio autónomo y las empresas del Estado peruano o sociedades de economía mixta, que puedan estar expuestas al riesgo de comisión de los delitos antes mencionados.

La finalidad del modelo de prevención, al que se refiere la ley y desarrolla el referido reglamento, es prevenir, detectar y mitigar los mencionados delitos, así como promover la integridad y transparencia en la gestión de las personas jurídicas. El análisis sobre sus implementación y funcionamiento está a cargo de la Superintendencia de Mercado de Valores (SMV), quien emitirá su informe técnico únicamente a solicitud del Fiscal a cargo de la investigación penal.

El reglamento establece que el Modelo de Prevención de las micro, pequeña y mediana empresa (MIPYME) se implementa bajo el principio de adaptabilidad, teniendo en consideración sus condiciones y características, sobre la base de una adecuada gestión de sus riesgos; y corresponde al Ministerio de la Producción, mediante Resolución Ministerial, en un plazo no mayor de 60 días calendario, aprobar los formatos de este modelo.

Finalmente, la referida norma, establece que las personas jurídicas consideradas sujetos obligados en materia de prevención del lavado de activos y financiamiento del terrorismo, pueden utilizar los componentes que conforman dicho sistema para implementar el modelo de prevención al que hace referencia este reglamento; y, que la función de encargado de prevención puede ser asumida por el Oficial de Cumplimiento a dedicación exclusiva o no exclusiva, designado ante la UIF-Perú.

Puede acceder al Decreto Supremo N° 002-2019-JUS, a través del siguiente enlace:

<https://busquedas.elperuano.pe/download/url/reglamento-de-la-ley-n-30424-ley-que-regula-la-responsabil-decreto-supremo-n-002-2019-jus-1729768-3>

2 Reglamento del Decreto Legislativo N° 1372, Decreto Legislativo que regula la obligación de las personas jurídicas y/o entes jurídicos de informar la identificación de los beneficiarios finales

Mediante Decreto Supremo N° 003-2019-EF, vigente desde el 09.01.2019, se reglamenta el Decreto Legislativo N° 1372, que regula la obligación de las personas jurídicas y entes jurídicos de informar la identificación de los beneficiarios finales. Su finalidad es fortalecer la lucha contra la evasión y elusión tributaria, garantizar el cumplimiento de las obligaciones de

asistencia administrativa mutua en materia tributaria, así como la lucha contra el lavado de activos y el financiamiento del terrorismo.

El referido reglamento establece los criterios para determinar la condición de beneficiario final, los mecanismos para obtener y conservar su información, las medidas para asegurar la

Novedades Normativas



presentación oportuna de la información y los procedimientos para mantenerla actualizada.

Asimismo, regula el contenido de la declaración jurada del beneficiario final en los siguientes supuestos:

- i) Persona natural que posea como mínimo el 10% del capital de una persona jurídica.
- ii) Persona natural que ejerce el control efectivo de una persona jurídica por medios diferentes a poseer el 10% del capital.

- iii) Cuando no se pueda identificar a ningún beneficiario final.

Puede acceder al Decreto Supremo N° 003-2019-EF a través del siguiente enlace:

<https://busquedas.elperuano.pe/normaslegales/aprueban-reglamento-del-decreto-legislativo-n-1372-que-reg-decreto-supremo-n-003-2019-ef-1729359-1/>

Herramientas



1 Informe Anual del Oficial de Cumplimiento (IAOC) de los sujetos obligados por la UIF-Perú

Definición

El IAOC es informe anual que el Oficial de Cumplimiento emite sobre el cumplimiento de las políticas y procedimientos que integran el Sistema de Prevención de Lavado de Activos y del Financiamiento del Terrorismo implementado por el sujeto obligado en el año calendario anterior.

Aprobación

En el caso de los sujetos obligados bajo el alcance de la Resolución SBS N° 789-2018, el IAOC debe ser aprobado dentro de los treinta (30) días siguientes al vencimiento del período anual respectivo de acuerdo a lo siguiente:

- i) En el caso de **personas jurídicas**, por el directorio u órgano equivalente del sujeto obligado persona jurídica; o, en su defecto, del gerente general, titular gerente o administrador según corresponda, siempre que la persona jurídica, de acuerdo a su estatuto, no esté obligada a tener directorio.
- ii) En el caso de **personas naturales**, la aprobación del IAOC le corresponde a la persona natural titular de la actividad. El informe es aprobado dentro.

En el caso de las Cooperativas de Ahorro y Crédito no autorizadas a operar con recursos del público (COOPAC) de nivel 1, el oficial de cumplimiento debe presentar el IAOC al Consejo

de Administración.

Envío del IAOC

En el caso de los sujetos obligados bajo el alcance de la Resolución SBS N° 789-2018 y los notarios públicos, el IAOC lo envía el sujeto obligado a través del oficial de cumplimiento, a más tardar el 15 de febrero del año siguiente, al organismo supervisor a través del Portal de Prevención del Lavado de Activos y Financiamiento del Terrorismo (plaft.sbs.gob.pe).

En el caso de las COOPAC nivel 1, el IAOC debe ser remitido a la UIF-Perú por el oficial de cumplimiento dentro de los quince (15) días siguientes a la fecha en que se haya presentado al Consejo de Administración.

El no remitir a la UIF-Perú el IAOC dentro del plazo establecido en la normativa vigente constituye infracción grave.



**¡EVITE
SANCIONES!**

El plazo para remitir el IAOC correspondiente al año 2018 vence el día 15.02.2019.

Herramientas



Contenido

En el caso de los sujetos obligados bajo el alcance de la Resolución SBS N° 789-2018, el IAOC contiene como mínimo la siguiente información:

La dirección y teléfono del sujeto obligado, y el correo electrónico del oficial de cumplimiento.	La indicación acerca de si el oficial de cumplimiento ejerce la función como oficial de cumplimiento corporativo o no.	Nombre de los socios, accionistas o asociados y porcentaje de participación en el sujeto obligado, de ser el caso.	Nombre de los gerentes u otros trabajadores responsables de la gestión de la actividad del sujeto obligado, de ser el caso.
Estadística anual del Registro de Operaciones, indicando el número de operaciones registradas y los montos involucrados, discriminando la información en forma mensual.	Estadística anual de las operaciones inusuales detectadas, indicando el número de operaciones detectadas, los montos involucrados u otro aspecto que se considere significativo, discriminando la información en forma mensual.	Estadística anual de las operaciones sospechosas reportadas a la UIF-Perú, indicando el número de operaciones reportadas, los montos involucrados u otros aspectos que se consideren significativos, discriminando la información en forma mensual.	Descripción de nuevas señales de alerta de operaciones inusuales establecidas por el sujeto obligado y tipologías de operaciones sospechosas que hubieran sido detectadas y reportadas, en caso las hubiere.
Políticas de debida diligencia en el conocimiento del cliente, directores y trabajadores, así como de proveedores y contrapartes, de ser aplicable.	Número de capacitaciones en temas relativos a la prevención del lavado de activos y financiamiento del terrorismo, el número de personas que han sido capacitadas; número de personas que fueron capacitadas más de una vez al año, así como el detalle de los temas materia de capacitación de acuerdo con el perfil del destinatario y su función en el sujeto obligado, así como de los riesgos de lavado de activos y financiamiento del terrorismo que enfrentan.	Última fecha de actualización del Manual y Código así como el nivel de cumplimiento de estos por parte de los directores y trabajadores del sujeto obligado, señalando los casos en que alguno ha sido incumplido, las sanciones impuestas y las medidas correctivas adoptadas.	Acciones correctivas adoptadas en virtud de las observaciones y/o recomendaciones que hubiere formulado el organismo supervisor y los auditores internos o externos, cuando corresponda.
Ubicación geográfica de las oficinas, sucursales y agencias.	Informe Anual de Auditoría Interna y/o Externa, según corresponda.	Otros que determine la SBS.	

En el caso de los notarios públicos, el IAOC contiene como mínimo la siguiente información:

Estadística anual de las operaciones inusuales detectadas por los trabajadores, discriminando la información mes por mes.	Estadística anual del Registro de Operaciones, indicando el número de operaciones registradas por mes y el monto involucrado.	Estadística anual de las operaciones sospechosas reportadas a la UIF-Perú, discriminando la información mes por mes, especificando los montos involucrados u otros aspectos que se considere significativos.	Descripción de nuevas señales de alerta de operaciones inusuales y tipos usuales de operaciones sospechosas que hubieran sido detectadas y reportadas, en caso las hubiere.
Políticas de conocimiento del cliente y del trabajador.	Breve descripción de los temas tratados en la capacitación anual en materia de prevención de LA/FT, indicando el número de personas capacitadas. Si el Notario hubiere recibido más de una capacitación, indicar el número de capacitaciones y el número de personas capacitadas en cada una de ellas, especificando si fue nacional o internacional.	Relación detallada de las actividades realizadas en el año para el cumplimiento y actualización del Manual y Código de Conducta para la Prevención del LA/FT, así como los casos de incumplimiento o inobservancia de éste y las medidas correctivas adoptadas.	Relación de las actividades realizadas para el cumplimiento de las normas relativas al Registro de Operaciones y de su mantenimiento por el plazo establecido en las presentes normas.
Cambios y actualizaciones del Manual.	Medidas adoptadas para la verificación y custodia de los legajos de los trabajadores, en cuanto a su contenido y actualización.	Acciones adoptadas respecto a las observaciones o recomendaciones que hubiere formulado la UIF-Perú.	Otros aspectos que el Notario o el Oficial de Cumplimiento considere relevantes.
Otros que determine la SBS.			

Herramientas



En el caso de las COOPAC nivel 1, el IAOC debe contener la información detallada en el Anexo N° 4 del Reglamento para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo aplicable a las Cooperativas de Ahorro y Crédito no autorizadas a operar con Recursos del Público, aprobado por la Resolución SBS N° 5060-2018.

Principales observaciones detectadas

Incorrecto	Correcto
× Si no se han detectado operaciones sospechosas, no existe obligación de remitir el IAOC a la UIF-Perú.	✓ Si el oficial de cumplimiento del sujeto obligado no ha detectado operaciones sospechosas, este igual debe remitir su IAOC a la UIF-Perú, dado que la información sobre las operaciones sospechosas reportadas a la UIF-Perú solo constituye una parte de la información que contiene el IAOC.
× Si se ha cumplido con remitir mensualmente a la UIF-Perú el Registro de Operaciones, no existe la obligación de enviar el IAOC.	✓ Si se ha cumplido con la obligación de remitir a la UIF-Perú su Registro de Operaciones, el sujeto obligado debe remitir su IAOC, dado que la estadística anual del Registro de Operaciones solo constituye una parte de la información que contiene el IAOC.
× El oficial de cumplimiento corporativo puede enviar un IAOC respecto de todas las empresas del grupo económico.	✓ Tratándose del oficial de cumplimiento corporativo, este debe presentar un IAOC por cada uno de los sujetos obligados que formen parte del grupo económico. Para ello, la UIF-Perú asigna al Oficial de Cumplimiento un código secreto, correspondiente a cada empresa del grupo económico.

2 Plazo para remitir Reporte de Operaciones Sospechosas (ROS) – Manual de Prevención de LA/FT

De acuerdo a lo establecido en la normativa sectorial, el plazo con el que cuentan los sujetos obligados para remitir ROS es de **veinticuatro (24) horas** desde que la operación es calificada como sospechosa, debiéndose tener en cuenta que el plazo para calificar una operación como sospechosa se sujeta a su naturaleza y complejidad.

El plazo estipulado para remitir ROS a la UIF-Perú debe encontrarse expresamente indicado en el Manual de prevención y gestión de los riesgos de lavado de activos y del financiamiento del terrorismo de los sujetos obligados.

El no reportar a la UIF-Perú las operaciones sospechosas detectadas, realizadas o que hayan intentado realizarse, dentro del plazo establecido en la normativa vigente constituye infracción grave de conformidad con lo establecido en el numeral 17 de la sección Infracciones Graves del Anexo 1 del Reglamento de Infracciones y Sanciones de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, aprobado la Resolución SBS N° 8930-2012.



3 Reserva de la Identidad del Oficial de Cumplimiento

A efectos de preservar la identidad del oficial de cumplimiento, la UIF-Perú asigna códigos secretos tanto al sujeto obligado como al oficial de cumplimiento, oficial de cumplimiento alterno y/o oficial de cumplimiento corporativo, de ser el caso, luego de verificada la documentación e información presentada a la UIF-Perú por el sujeto obligado.

Estos códigos secretos asignados sirven únicamente como identificación en todas las comunicaciones que se remitan a la UIF-Perú.

El sujeto obligado y el oficial de cumplimiento, el oficial de cumplimiento alterno y el oficial de cumplimiento corporativo deben adoptar las medidas necesarias que garanticen la reserva de los códigos secretos asignados.



1 Atentados terroristas: el importantísimo rol del Oficial de Cumplimiento a propósito del último atentado producido en Colombia

Son pocas las labores preventivas que un sistema antilavado puede lograr en materia de prevención del terrorismo. Salvo que se trate de terroristas conocidos, jurisdicciones que patrocinan terrorismo, empresas que venden materia de guerra o señales de alerta muy evidentes, la financiación del terrorismo es difícil de detectar para las entidades en Colombia.

El atentado del día 18.01.2019 en el cual el Ejército de Liberación Nacional (ELN) estalló un carro bomba en la Escuela de Policía General Santander en Bogotá, que dejó un saldo de 21 fallecidos y 68 heridos, es lamentable y condenable en todo nivel y nos exhorta a apoyar firmemente la lucha antiterrorista. Para facilitar esta tarea ciudadana, INFOLAFT señala los pasos que todas las entidades deberían realizar después de conocerse un atentado.

Protocolo de reacción ante acciones terroristas

1. Recauda toda la información básica de fuentes creíbles

Tan pronto como se supo del atentado, la Fiscalía General de la Nación en Colombia desplegó un operativo de investigación en el que muy pronto logró identificar tanto al autor material del acto terrorista como al vehículo utilizado en la explosión. Estos datos son de vital relevancia para la gestión del riesgo de LA/FT pues le permiten a la entidad saber si ha estado vinculada con los individuos o activos involucrados en el hecho.

Para el caso en concreto, la fiscalía señaló como autor a José Aldemar Rojas Rodríguez, un explosivista del ELN que perdió la mano derecha en un accidente con un explosivo entre 2008 y 2010. En relación con el vehículo, el ente acusador confirmó que se trataba de una Nissan Patrol, del año 1993, con placa LAF 565.

Adicionalmente, las autoridades capturaron a otro hombre relacionado con el atentado, que habría estado en comunicación con José Aldemar Rojas durante la ejecución de los hechos. Se trata de Ricardo Andrés Carvajal quien con posterioridad a su detención aceptó su participación en el ataque.

2. Buscar en las bases de datos de la entidad cualquier relación con el atentado

Una vez que se han recopilado los datos básicos de los individuos y activos involucrados en el ataque terrorista, es necesario cruzarlos con las bases de datos que la entidad utilice para gestionar el riesgo de LA/FT para verificar si ha existido algún tipo de vinculación.

Esta tarea significará revisar si los terroristas han sido clientes, usuarios, proveedores o empleados, pero no se limita a ello. Adicionalmente, conviene verificar si el individuo ha tenido otro tipo de vínculos indirectos como haber sido beneficiario de productos o servicios o haber visitado la empresa por cualquier razón. Para dicho efecto, deben revisarse bases de datos generales, así como especializadas o específicas.

En cuanto al vehículo, y dependiendo del tipo de negocio y la actividad económica que lleve a cabo la empresa, será necesario analizar si existieron vínculos como por ejemplo la constitución de prendas, la expedición de pólizas de seguros, la prestación de servicios de reparación o mantenimiento y el ingreso a las instalaciones de la empresa.

3. Si aparecen coincidencias es necesario profundizar en ellas

Hallar la coincidencia es apenas una parte de la tarea. En caso de que se evidencie un vínculo directo o indirecto con los sujetos o activos involucrados en un atentado es necesario proceder a comprender la naturaleza de dicha relación.

Para ello es recomendable individualizar a todas las personas dentro de la empresa que tuvieron que ver con la vinculación e indagar a través de ellas la naturaleza del vínculo. Frente a estas personas también se sugiere buscar si hay coincidencias que puedan mostrar vínculos con organizaciones o células terroristas y que sea necesario denunciar a las autoridades.

4. Proceda a reportar y denunciar

Sobre la base de encontrar señales de operaciones sospechosas de canalización de recursos a actividades terroristas se requiere hacer inmediatamente el proceso de Reporte de Operaciones Sospechosas a la Unidad de Inteligencia Financiera.



5. La labor continúa

Después de realizado el reporte es posible seguir profundizando sobre el caso. Con el devenir de las horas es probable que las autoridades continúen vinculando individuos o activos a las investigaciones y conviene realizar el ciclo de gestión del riesgo tantas veces como esto ocurra.

6. Estar atento a colaborar con las autoridades

Es previsible que, si se ha reportado o denunciado, las autoridades se comuniquen a obtener información adicional. Esto no es, bajo ningún concepto, una acción de auditoría o vigilancia. Es el desarrollo de una investigación

en la que hay que colaborar a esclarecer los hechos y a evitar nuevas acciones de terrorismo.

7. Actualice su sistema con las lecciones aprendidas

A partir de los hechos conocidos del ataque conviene actualizar los eventos de riesgo contemplados en el sistema de prevención de los riesgos de LA/FT y verificar si los controles existentes son suficientes ante la existencia de nuevos eventos. En caso de que no lo sean, se deben implementar nuevos controles para los nuevos eventos de riesgo.

Fuente:

<https://www.infolaft.com/atentados-terroristas-el-importantisimo-rol-del-oficial-de-cumplimiento/>

2 Los casos más importantes por violación de la Ley de Prácticas Corruptas en el Extranjero (Fcpa) del 2018

Durante el año 2018, dieciséis (16) empresas pagaron una cifra récord de USD 2.890 millones a título de sanción o para terminar anticipadamente investigaciones derivadas de violaciones a la Ley de Prácticas Corruptas en el Extranjero (Fcpa). En la categoría de “megacasos” hubo tres acciones de cumplimiento: Petrobras que desembolsó USD alrededor de USD 1.780 millones, SocGen que pagó USD 585 millones y Panasonic que entregó USD 280 millones.

Para comparar estas cifras, INFOLAFT trae un recuento de lo recaudado por el gobierno de Estados Unidos por imposición de sanciones relacionadas con violaciones a la Fcpa en los últimos cinco años:

- 2017: 11 compañías pagaron poco más de USD 1.920 millones a título de sanción o para terminar anticipadamente investigaciones.
- 2016: 27 empresas pagaron USD 2.480 millones.
- 2015: 11 empresas pagaron USD 133 millones.
- 2014: 10 empresas pagaron USD 1.560 millones.
- 2013: 12 empresas pagaron COP 731 millones.
- 2012: 12 empresas pagaron USD 259 millones.

Adicionalmente, cuatro individuos resolvieron cargos civiles por violaciones de la Fcpa ante la Comisión de Bolsa y Valores de Estados Unidos

(SEC por su nombre en inglés) mientras otros seis se declararon culpables de cargos penales relacionados con estas violaciones y ocho más fueron condenados.

Casos más importantes del año 2018

Panasonic Corporation y Panasonic Aviation Corporation (30 de abril): estas empresas, con sede en Osaka, Japón, acordaron un pago total de USD 280 millones para resolver diversas infracciones a la ley Fcpa luego de que las autoridades estadounidenses comprobaran pagos indebidos vinculados a la unidad de tecnología para el entretenimiento en vuelos en Medio Oriente y Asia. Según la acusación del Departamento de Justicia de Estados Unidos (DOJ) Panasonic ofreció un contrato de consultoría a un funcionario gubernamental de una aerolínea estatal por valor de USD 875 mil para inducir al funcionario a ayudar a la empresa a obtener contratos durante seis años contados a partir de 2007. Tras este pago, la aerolínea estatal adjudicó negocios a Panasonic que le generaron al menos USD 92 millones en ingresos.

Société Générale S.A. (4 de junio): esta empresa, que es una de las más importantes en Europa en la prestación de servicios financieros, pagó USD 585 millones luego de que el Departamento de Justicia de Estados Unidos (DOJ) acusara a una de sus subsidiarias, SGA Société Générale Acceptance N.V., de haber pagado al menos USD 90 millones a funcionarios de régimen sirio durante el gobierno de Muhamad al Gadafi para obtener y mantener negocios y contratos.



Credit Suisse Group AG (5 de julio): la unidad de Hong Kong de esta entidad pagó al DOJ y a la SEC una suma de USD 76.7 millones por haber establecido un plan de contratación que implicó la adjudicación de empleos a amigos y familiares de funcionarios chinos para ganar negocios bancarios.

Sanofi (4 de septiembre): este laboratorio pagó a la SEC una suma de USD 25 millones luego de que autoridades estadounidenses evidenciaran sobornos a funcionarios en todo el Medio Oriente y en Kazajstán para ganar negocios.

Petróleo Brasileiro S.A. – Petrobras (27 de septiembre). El DOJ y la SEC impusieron multas por USD 1.780 millones a la compañía estatal petrolera de Brasil por haber entregado sobornos a políticos y partidos políticos en Brasil. Petrobras

firmó un acuerdo de no procesamiento con el DOJ que determinó una sanción penal de USD 853.2 millones y una orden administrativa con la SEC que requirió la devolución de USD 933.5 millones a título de devolución de ganancias obtenidas ilícitamente.

Beam Suntory Inc. (2 de julio), el tercer productor mundial de bebidas destiladas detrás de Diageo y Pernod Ricard, pagó a la SEC un total de USD 8.2 millones por haber realizado pagos indebidos en India. Beam pagó la sanción sin admitir o negar las acusaciones.

Fuente:

<https://www.infolaft.com/los-casos-mas-importantes-por-violacion-a-la-fcpa-de-2018/>