Año 2019 / Edición N° 78

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Prevención de Lavado de Activos y Financiamiento del Terrorismo

Contenido

Herramientas

Actualidad

Superintendencia Adjunta de Unidad de Inteligencia Financiera del Perú

Contenido

ÍNDICE

HERRAMIENTAS

ACTUALIDAD

Herramientas

1 Capacitación en materia de prevención del lavado de activos y del financiamiento del terrorismo bajo el alcance de la Resolución SBS N° 789-2018

Uno de los aspectos más importantes del Sistema de Prevención del Lavado de Activos y del Financiamiento del Terrorismo (SPLAFT), es el referido a la capacitación, la cual debe tener como principal objetivo el sensibilizar al personal sobre la importancia de prevenir el lavado de activos y el financiamiento del terrorismo mediante el cumplimiento de los procedimientos y la utilización de las herramientas definidas para tal fin.

Es por ello que la capacitación en materia de prevención del lavado de activos y financiamiento del terrorismo debe estar enfocada a lograr que los administradores, gerentes, directivos, oficiales de cumplimiento y, en general, todos los empleados de una empresa, tomen conciencia de que al implementar el SPLAFT no se esta cumpliendo con lo dispuesto en una norma, sino que por el contrario a través de la implementación y buen funcionamiento de dicho sistema se están protegiendo a sí mismos, a sus empresas, y a la colectividad en general de los delitos de lavado de activos y financiamiento del terrorismo, y sus delitos fuentes.

Aspectos generales de la capacitación

De conformidad con lo dispuesto en el literal e) del artículo 12 de la Norma para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo aplicable a los sujetos obligados bajo supervisión de la UIF-Perú, en materia de prevención del lavado de activos y del financiamiento del terrorismo, aprobada por Resolución SBS N° 789-2018 (Resolución SBS N° 789-2018), establece que es función del oficial de cumplimiento adoptar las acciones necesarias para la capacitación de las personas que conforman la estructura organizativa del sujeto obligado en materia de prevención y detección del lavado de activos y del financiamiento del terrorismo.

Al respecto, de acuerdo a lo dispuesto en el artículo 20 de la Resolución SBS N° 789-2018, los directores, de contar con dicho órgano de gobierno, y los trabajadores, incluyendo al oficial de cumplimiento, así como el sujeto obligado, cuando este sea persona natural, deben contar como mínimo con una capacitación anual en materia de prevención y/o detección del lavado de activos y financiamiento del terrorismo, dentro de un año calendario, con la finalidad de que estén instruidos de acuerdo a su especialidad y funciones que desempeñen, sobre los aspectos mínimos previstos en el artículo 21 de dicha norma, entre otros aspectos que el oficial de cumplimiento considere relevantes.

A saber:

De acuerdo a lo establecido en la Resolución SBS N° 789-2018, trabajador es toda aquella persona natural que mantiene vínculo laboral o contractual con el sujeto obligado; incluye el gerente general, gerentes, administradores o a quienes desempeñen cargos similares; al oficial de cumplimiento, al oficial de cumplimiento alterno, al oficial de cumplimiento corporativo y al coordinador corporativo, cuando corresponda.

Al respecto, la capacitación es de obligación del sujeto obligado y puede ser dictada por terceros, entidades especializadas o por el oficial de cumplimiento bajo cualquier modalidad, debiendo conservarse una constancia de las capacitaciones recibidas, las que deben encontrarse a disposición de la UIF-Perú, y deben mantenerse en la información correspondiente a cada director o trabajador, en medio físico y/o electrónico. En el caso de que la capacitación haya sido efectuada por el oficial de cumplimiento, este debe emitir una constancia con carácter de declaración jurada en la que indique el día, lugar, tiempo de duración y los temas de la capacitación, así como los nombres y apellidos y cargos de las personas capacitadas.

Asimismo, de conformidad con lo dispuesto en el artículo 25 de la Resolución SBS N° 789-2018, los grupos económicos deben desarrollar políticas y procedimientos corporativos con relación al SPLAFT, incluyendo entre otros, un programa de capacitación en materia de prevención y detección del lavado de activos y financiamiento del terrorismo, el cual puede ser un único programa a nivel corporativo.

Del mismo modo, conforme a lo establecido en el

artículo 40 de la Resolución SBS N° 789-2018, en el caso de los sujetos obligados dedicados a la actividad de construcción y/o inmobiliaria, sin perjuicio de su condición de trabajador, la capacitación no es obligatoria para los trabajadores que desempeñen labores no vinculadas de manera directa a la operatividad o giro del negocio del sujeto obligado, como es el caso del personal de limpieza y obreros de construcción civil u otro que determine el oficial de cumplimiento, previa solicitud de autorización al organismo supervisor, con el análisis y el sustento documental respectivo.

En el caso de los nuevos trabajadores, el artículo 20 de la Resolución SBS N° 789-2018 establece que dentro de los treinta (30) días siguientes a la fecha de ingreso del trabajador, el sujeto obligado debe informarles, a través del oficial de cumplimiento, sobre los alcances del SPLAFT, dejando constancia de ello; sin perjuicio de la capacitación anual que dicho trabajador deba recibir.

Requerimientos mínimos de capacitación

De acuerdo a lo establecido en el artículo 21 de la Resolución SBS N° 789-2018, se debe capacitar, de acuerdo con sus funciones, tanto al sujeto obligado si es persona natural o persona jurídica, a sus directores y trabajadores, sobre los aspectos mínimos establecidos en dicho artículo.

Al respecto, dicho contenido mínimo puede resumirse en los siguientes temas:

I. Delitos de Lavado de Activos y del Financiamiento del Terrorismo.
II. Normativa vigente en materia de Prevención de Lavado de Activos y del Financiamiento del Terrorismo.
III. Normas internas del Sujeto obligado.
   a. Riesgo de lavado de activos y financiamiento del terrorismo de la empresa.
   b. Políticas y procedimientos para mitigar el riesgo (normas internas).
   c. Señales de alerta y procedimiento de comunicación de operaciones inusuales.
   d. Responsabilidades de los trabajadores en los procedimientos.
IV. Tipologías.
V. Listas que contribuyen a la prevención del lavado de activos y financiamiento del terrorismo, incluyendo la del Consejo de Seguridad de las Naciones Unidas en materia de Terrorismo, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.

2 Infracciones relacionadas a la obligación de capacitación

De acuerdo a lo dispuesto en el Reglamento de Infracciones y Sanciones en Materia de Prevención del Lavado de Activos y del Financiamiento del Terrorismo, aprobado por Resolución SBS N° 8930-2012 y sus modificatorias, el incumplimiento de las obligaciones relacionadas a la capacitación en materia de prevención del lavado de activos y del financiamiento del terrorismo pueden constituir las siguiente infracciones leves:

- No haber aprobado el programa de capacitación en materia de prevención del lavado de activos y del financiamiento del terrorismo, de acuerdo a la normativa vigente, en caso el sujeto obligado sea una persona jurídica.
- No ejecutar durante el año calendario el programa de capacitación que corresponde al sujeto obligado en caso sea una persona jurídica.
- No haber recibido la capacitación anual sobre prevención del lavado de activos y del financiamiento del terrorismo establecido en la normativa vigente, en caso el sujeto obligado sea persona natural; así como en el caso de los trabajadores, oficial de cumplimiento, gerente general, gerentes, administradores o los que hagan sus veces, cuando el sujeto obligado sea persona jurídica.

Dichas infracciones son pasibles de las siguientes sanciones:

	Persona natural	Persona jurídica
Infracción leve	Amonestación	Amonestación
	Multa no menor a 0.15 UIT hasta 3 UIT.	Multa no menor de 0.50 UIT hasta 10 UIT.

1 Señales de alerta sobre monedas virtuales

Cualquier entidad financiera o no financiera que gestione operaciones de pagos y transferencias de dinero está en la capacidad de identificar actividades irregulares o sospechosas de lavado de activos o financiación del terrorismo. Sin embargo, cuando dichas transacciones involucran monedas virtuales, las actividades de identificación se hacen un poco más complejas ante la falta de señales de alerta disponibles.

A continuación se detallan señales de alerta sobre monedas virtuales.

Señales de alerta relacionadas con la *Darknet*

El concepto de red oscura, también conocido por su nombre original en inglés *darknet*, es una colección de redes, paralelas a las plataformas indexadas por los motores de búsqueda, usadas para compartir información y contenidos digitales (por ejemplo, textos, software, canciones, imágenes, películas, o monedas virtuales) que preserva el anonimato de las identidades de quienes intercambian dicha información. Las señales de alerta son:

- Un cliente realiza transacciones con direcciones de plataformas de criptomonedas que se han vinculado a lugares de la *darknet* u otra actividad ilícita.
- La dirección de un cliente aparece en foros públicos asociados con actividades ilegales.
- Las transacciones de un cliente se inician desde direcciones IP asociadas con Tor (el explorador de la *darknet*).
- Los análisis de *blockchain* indican que la billetera virtual que transfiere la criptodivisa tiene fuentes sospechosas de fondos, entre los que se encuentra la *darknet*.
- Una transacción sigue cursos irregulares en su flujo, lo que sugiere una intención de oscurecer el origen o destino de los fondos.

Señales de alerta relacionadas con plataformas de intercambio *peer-to-peer* (P2P)

Una red *peer-to-peer*, conocida como red entre iguales o red entre pares (P2P, por sus siglas en inglés), es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino a partir de una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y

servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados. Las señales de alerta son:

- Un cliente recibe múltiples depósitos en efectivo o transferencias bancarias de distintas jurisdicciones o sucursales de una institución financiera o personas y, a continuación, utiliza estos recursos para adquirir monedas virtuales.
- Un cliente recibe una serie de depósitos de fuentes dispares que, en conjunto, equivalen a transferencias de fondos a una plataforma de intercambio de moneda virtual.
- El número de teléfono o la dirección de correo electrónico del cliente está conectado a una conocida plataforma de intercambio de criptomonedas o plataforma P2P que ofrece servicios de intercambio de estos instrumentos.

Señales de alerta relacionadas con negocios de servicios de dinero de origen extranjero no registrados

- Un cliente transfiere o recibe fondos, incluso a través de sistemas bancarios tradicionales, de un cambista no registrado de monedas virtuales extranjero u otra plataforma que no tenga relación con el lugar donde el cliente realiza negocios.
- Un cliente utiliza un cambista de activos virtuales o una empresa de servicios monetarios localizada en el extranjero en una jurisdicción de alto riesgo que carece o que se sabe que no cuenta con las reglamentaciones adecuadas de ALA CFT, incluidas las medidas de debida diligencia para conocimiento del cliente.
- Un cliente dirige grandes cantidades de transacciones de activos virtuales a entidades en jurisdicciones con reputación de ser paraísos fiscales.
- Un cliente que no se ha identificado para el intercambio de valores o de moneda, o no está registrado como tal, utiliza la ganancia de su negocio para ejecutar grandes cantidades de transacciones de dinero, lo que puede indicar que el cliente está actuando como un cambista irregular.

Señales de alerta relacionadas con quioscos de criptomonedas no registrados o que operan de manera ilícita

- Un cliente opera múltiples quioscos de criptomonedas en ubicaciones que tienen una incidencia relativamente alta de actividad delictiva.
- Un gran número de transacciones de diferentes clientes se envían y reciben desde la misma dirección de billetera virtual.

Señales de alerta relacionadas con otras actividades potencialmente ilícitas

- Un cliente realiza transacciones con plataformas de monedas virtuales o direcciones que se han vinculado a extorsión, *ransomware* u otra actividad ilícita.
- Las transacciones de un cliente se inician desde direcciones IP que no son de confianza, direcciones IP de jurisdicciones sancionadas o direcciones IP previamente marcadas como sospechosas.
- Uso de servicios de red privada virtual (VPN) o Tor para acceder a cuentas de intercambio de criptomonedas. Recuerde que la VPN permite que un computador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada
- Un cliente realiza múltiples operaciones rápidas que involucran varias monedas virtuales sin un propósito relacionado, lo que puede ser un indicador de los intentos de romper la cadena de custodia en las *block chain* respectivas u oscurecer aún más la transacción.
- Un cliente proporciona una identificación o credenciales de cuenta compartidas por otra cuenta.
- Un cliente realiza transacciones o ejecuta rápidamente conversiones múltiples entre varios tipos de activos virtuales por debajo de los umbrales de diligencia debida, registros o reportes, y luego transfiere el valor del intercambio.
- Surgen discrepancias entre las direcciones IP asociadas con el perfil del cliente y las direcciones IP desde las cuales se inician las transacciones.
- Un cliente significativamente mayor que la edad promedio de los usuarios de la plataforma abre una cuenta y participa en un gran número de transacciones, sugiriendo su papel potencial como mula de activos o víctima de explotación financiera.
- Un cliente muestra poco conocimiento del funcionamiento de las criptomomendas, no obstante participa ampliamente en transacciones que las involucran.
- Un cliente rechaza u omite entregar información propia del proceso de conocimiento del cliente o sobre origen de fondos.
- Un cliente compra grandes cantidades de criptomonedas sin respaldo económico o de forma incoherente con su perfil financiero histórico, lo que puede indicar lavado de activos, mulas de dinero o estafas.
- Una misma dirección de billetera virtual se utiliza para dos cuentas identificadas como pertenecientes a dos clientes diferentes.
- Múltiples cambios en la dirección de correo electrónico y otra información de contacto para una cuenta o cliente.

Fuente:

https://www.infolaft.com/30-senales-de-alerta-sobre-monedas-virtuales/

2 Señales de alerta sobre corrupción

El Grupo Egmont ha compilado en el documento denominado *"Set of Indicators for Corruption Related Cases from the FIU's Perspective"* un conjunto de indicadores que, cuando se consideran en el contexto de una transacción o interacción con el cliente, ayudan a identificar la corrupción y al lavado de los productos de la corrupción.

Al respecto, de dicho documento se han extraído y adaptado las señales de alerta más importantes con el fin de que las empresas las integren a sus sistemas de prevención de lavado de activos y financiación del terrorismo o a sus sistemas de ética empresarial en caso de tenerlo.

Señales de alerta de distorsión de licitaciones públicas con fines de fraude

- ✓ La contraparte que es persona jurídica o agrupación de personas jurídicas (tipo consorcio o unión temporal, por ejemplo) que haya ganado varias de las licitaciones más grandes de

diferentes autoridades.

- ✓ La contraparte que es contratista o subcontratista con el Estado y que ha sido adjudicatario de varios contratos a largo plazo sin justificación aparente o razonable.
- ✓ La contraparte que exige la inclusión de cláusulas no razonables para la ejecución del contrato, como son restricciones para la ubicación del contratista, plazos que no se pueden cumplir según la lógica o plazos muy ajustados de cumplimiento, etc).
- ✓ La contraparte que es subcontratista y tiene directores comunes o vínculos con la administración de su contratista controlante.
- ✓ La contraparte es funcionario público que quiere depositar cheques emitidos por empresas constructoras.
- ✓ La contraparte es un individuo o persona jurídica de derecho privado que anteriormente fue beneficiario de contratos de obras públicas.
- ✓ La contraparte es una persona jurídica con poca o nula experiencia en contratación de servicios altamente complejos y técnicos pero que recibe contratos y proyectos gubernamentales de este tipo. La persona jurídica no es idónea para ejecutar un contrato público por su tamaño, su experiencia o su área de negocios.
- ✓ La contraparte es una persona jurídica o grupo de personas jurídicas contratista de una empresa estatal que recibe pagos muy altos por bienes o servicios que normalmente deberían costar menos en comparación con los precios normales de mercado para productos o servicios equivalentes.
- ✓ La contraparte es un funcionario público con competencias en la gestión de contratos gubernamentales o públicos de adquisición de activos de alto valor que imparte instrucciones de transferencia de fondos internacionales desde y hacia cuentas comerciales o personales.

Señales de alerta de riqueza no justificada o proveniente de corrupción

- ✓ Los sujetos en una transacción son Personas Expuestas Políticamente (PEP) nacionales o extranjeras, sus familiares o asociados cercanos según lo define el Gafi y reciben o envían cantidades inusualmente grandes de fondos en diferentes tipos de moneda.
- ✓ Fondos recibidos en cuentas bancarias de personas, personas jurídicas o grupos de personas jurídicas sin conexión visible con una PEP u otros funcionarios, pero que se sabe por otras fuentes de información que están controlados por ellos, o por personas relacionadas con ellos.
- ✓ El representante o apoderado de una PEP (es decir, abogado, secretario, contador), abre una cuenta bancaria y compra bienes costosos o bienes de lujo. Se presume que en este caso hay la intención expresa de pasar por alto el proceso de detección de diligencia debida del cliente para las PEP.
- ✓ La contraparte en una operación es empleado directo o indirecto de una PEP, como un jardinero o un conductor, que recibe fondos que superan significativamente sus ingresos de empleo legítimos. El grupo Egmont recuerda que este tipo de «mulas de dinero» se pueden utilizar para ocultar la titularidad real de los activos de una PEP con el fin de evadir los controles reforzados.
- ✓ Las PEP, sus familiares o asociados cercanos u otros funcionarios, reciben o compran acciones (o la opción de comprar acciones) en una empresa a cambio de servicios; en una empresa donde la compra es financiada por un proveedor; en una empresa donde el precio de compra está por debajo del valor del activo neto de la empresa; o en una empresa a cambio de un dividendo desproporcionado frente al precio de compra.
- ✓ Las PEP, sus familiares o asociados cercanos u otros funcionarios reciben garantías de préstamo de una corporación pública o un organismo gubernamental, o un préstamo en condiciones más favorables que las usuales.
- ✓ Las PEP, sus familiares o asociados cercanos, u otros funcionarios, reciben grandes cantidades de dinero por su asistencia a talleres, conferencias, o como consultores de proyectos, para disfrazar el origen de los fondos.
- ✓ Las PEP, sus familiares o asociados cercanos u otros funcionarios realizan transacciones con fondos soberanos de inversión o empresas vinculadas con el gobierno.
- ✓ Las PEP, los miembros de su familia o asociados cercanos u otro funcionario han comprado criptomonedas en montos totales superiores a sus ingresos legalmente declarados.
- ✓ Transacciones que tienen lugar en las cuentas de las PEP, los miembros de su familia o asociados cercanos u otros funcionarios que involucran depósitos en efectivo o retiros frecuentes y en cantidades inusuales.
- ✓ Transacciones entrantes de jurisdicciones extranjeras (específicamente de jurisdicciones con registro de empresa simplificado o de paraísos fiscales) en cuentas de una PEP, sus familiares o asociados cercanos u otros funcionarios y la información de remesa es vaga (por ejemplo, se refiere a ‘honorarios de consultoría’).

Actualidad

- ✓ El uso de mecanismos irregulares de transferencia de dinero de tipo *hawala* por parte de las PEP, sus familiares o asociados cercanos u otros funcionarios.
- ✓ Certificados de depósito a término de empresas con el objetivo principal de que el capital y los intereses generados por la inversión se transfieran inmediatamente a las cuentas bancarias de un partido político.
- ✓ La transferencia de fondos de la cuenta bancaria de una entidad privada a una cuenta bancaria personal de una persona relacionada con una PEP u otro funcionario, y el posterior movimiento de los fondos a cuentas de terceros. Si estos fondos finalmente se trasladan al extranjero es un indicador que el uso de las cuentas es a modo de nodo temporal.
- ✓ Transferencia de fondos de las cuentas bancarias de las PEP, sus familiares o asociados cercanos u otros funcionarios a vehículos de alto riesgo en el extranjero, como fideicomisos corporativos.
- ✓ Las PEP, sus familiares o asociados cercanos u otros funcionarios establecen personas jurídicas que compraron terrenos y edificios de valor significativo a pesar de la ausencia de cualquier otra actividad comercial.
- ✓ Las PEP, sus familiares o asociados cercanos u otros funcionarios han realizado transacciones en efectivo que involucran grandes cantidades (por ejemplo, cambio de moneda, uso de efectivo para comprar bienes de alto costo, etc.).

Otras señales de alerta relevantes para la corrupción

- ✓ Información pública que vincula a la contraparte con la corrupción u otros delitos financieros.
- ✓ La contraparte solicita abrir una cuenta para integrarla a una estructura económica compleja que no tiene justificación para su grado de complejidad. Esto podría indicar la intención de ocultar al beneficiario real.
- ✓ La contraparte es una PEP que solicita con expresa urgencia un servicio o actuación, (por ejemplo la cancelación de una hipoteca).
- ✓ En la debida diligencia de la contraparte o de la transacción aparecen como justificación de las inusualidades palabras y frases que a menudo se usan como eufemismos para coimas (por ejemplo, comisiones, tarifas de comercialización, recargos, etc.).

Fuente:

https://www.infolaft.com/integre-estas-senales-de-alerta-sobre-corrupcion/

Para revisar el documento "Set of Indicators for Corruption Related Cases from the FIU's Perspective":

https://egmontgroup.org/sites/default/files/filedepot/external/Corruption%20red-flags-final%20version_20181030.pdf