Año 2020 / Edición N° 92

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Prevención de Lavado de Activos y Financiamiento del Terrorismo

Contenido

Novedades Normativas

Herramientas

Actualidad

Avisos Importantes

Superintendencia Adjunta de Unidad de Inteligencia Financiera del Perú

Contenido

ÍNDICE

Novedades normativas

UIF-Perú notificará por casilla electrónica a sus supervisados

Con la finalidad de agilizar su labor de supervisión, la Superintendencia de Banca, Seguros y AFP (SBS) ha incluido a la casilla electrónica como un canal para la notificación de documentos a los sujetos obligados directamente supervisados por la Unidad de Inteligencia Financiera (UIF-Perú), según la Resolución N° 1982-2020 publicada el 12.08.2020 el Diario Oficial El Peruano.

¿Dónde se ubica la casilla electrónica?

La casilla electrónica se encuentra en el Sistema de Solicitudes de Información - módulo "comunicaciones", dentro de la herramienta informática del Portal de Prevención de Lavado de Activos y Financiamiento del Terrorismo (PLAFT), al que **actualmente los oficiales de cumplimiento vienen accediendo para remitir información a la UIF-Perú.**

plaft.sbs.gob.pe
Sistema de Solicitudes de Información
Módulo "Comunicaciones"

Acciones que se pueden realizar a través del Sistema de Solicitudes de Información

1. La UIF solicita información y/o documentación para el cumplimiento de sus funciones a cualquier sujeto obligado y recibe la respuesta de las referidas solicitudes de información y/o documentación, utilizando para dicho efecto el Portal PLAFT (https://plaft.sbs.gob.pe/)

2. Los sujetos obligados cuyo Sistema de Prevención de Lavado de Activos y Financiamiento del Terrorismo se encuentra supervisado por la UIF, tienen una casilla electrónica en dicho Sistema; a través de la cual les será remitida y solicitada información a efectos de la supervisión del mismo.

Es importante que tenga actualizado su correo electrónico registrado en UIF, pues cada vez que la UIF le haga llegar una comunicación por el Sistema de Solicitudes de Información, podrá recibir una alerta en dicho correo indicándole que tiene un documento por revisar.

Régimen de plazos, días y horario de notificación

La norma publicada establece que el depósito del documento electrónico en dicha casilla podrá efectuarse en cualquier momento y se entenderá notificado en ese acto, salvo que el mismo se hubiera producido en un día no hábil o después de las 16:30 horas de un día hábil. En ese caso, la notificación se entenderá como efectuada a las 08:30 horas del día hábil siguiente.

Obligaciones del Sujeto Obligado

Revisar periódicamente la casilla electrónica asignada para tomar conocimiento de los documentos y/0 actos administrativos que se le notifiquen

Mantener operativo su correo electrónico o servicio de mensajería para recibir las alertas del Sistema

Mantener la confidencialidad y adoptar las medidas de seguridad del nombre del usuario y la clave de acceso a la casilla asignada al oficial de cumplimiento

Aspectos a considerar para el uso de la casilla

El acceso al Portal PLAFT deberá realizarlo el oficial de cumplimiento con su usuario (código y contraseña)

Si el Oficial de Cumplimiento no cuenta con usuario ni contraseña por motivo de extravío, se deberá comunicar a consultasoc@sbs.gob.pe

Si el Oficial de Cumplimiento cuenta con usuario pero se olvidó su contraseña, deberá ingresar al portal plaft.sbs.gob.pe y marcar la opción "Olvidó su Contraseña".

Manual del Usuario

El Manual del uso de la casilla electrónica se encuentra a disposición de los oficiales de cumplimiento en el Portal plaft.sbs.gob.pe

Herramientas

Guía para la aplicación de la debida diligencia en el conocimiento del cliente con un enfoque basado en riesgos, dirigida al sector de construcción y/o inmobiliario

La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS), a través de la Unidad de Inteligencia Financiera del Perú (UIF-Perú), con el apoyo de la Cooperación Alemana para el desarrollo, implementada por Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, ha elaborado una *"Guía para la implementación del Sistema de Prevención de Lavado de Activos y de Financiamiento del Terrorismo con enfoque basado en riesgos dirigida al sector de construcción y/o inmobiliario".*

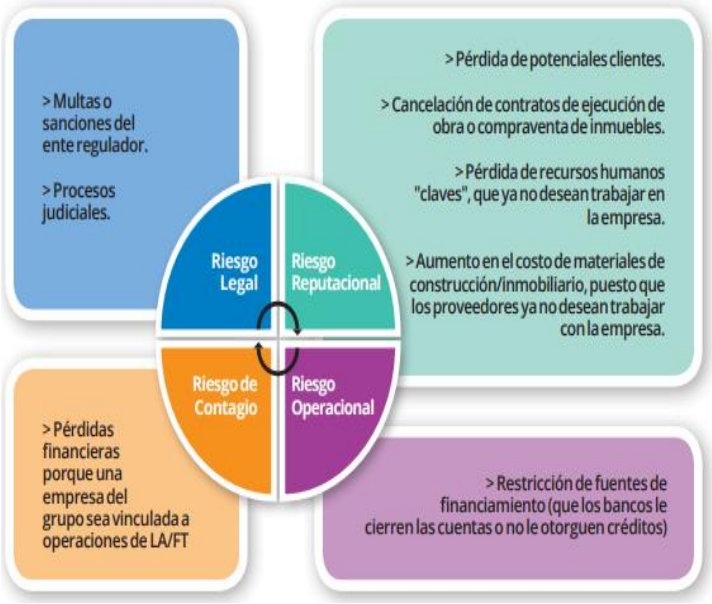
La guía tiene como objetivo presentar, de manera clara y esquemática, los pasos a seguir por los sujetos obligados dedicados a las actividades de construcción y/o inmobiliaria, para el desarrollo y aplicación de los procedimientos de debida diligencia en el conocimiento del cliente, con un enfoque basado en riesgos conforme a la normativa vigente.

Dentro de los aspectos que contiene la guía se encuentra un breve resumen de los riesgos de lavado de activos y financiamiento del terrorismo en el Perú, así como su impacto en las referidas actividades económicas a nivel nacional.

Asimismo, este documento contiene conceptos generales tales como la definición de lavado de activos y financiamiento del terrorismo, delitos precedentes, riesgos de lavado de activos y financiamiento del terrorismo (LA/FT) en el sector de construcción y/o inmobiliario, riesgos asociados al LA/FT, gestión de riesgos de LA/FT, entre otros conceptos que resultan de utilidad para los sujetos obligados dedicados a la actividad de construcción y/o inmobiliaria.

De igual modo, la referida guía explica las siguientes actividades que abarca el proceso de gestión de riesgos de LA/FT:

Es importante tener en cuenta que el riesgo de LA/FT, es parte inherente de una empresa, se encuentra presente en su desarrollo, crecimiento y consolidación. Dicha exposición permanente al riesgo, puede afectar la proyección futura de la empresa y su estabilidad, por lo cual, de no desarrollar e implementar un adecuado sistema de prevención de LA/FT, podría materializarse el riesgo en la empresa y generarle las siguientes consecuencias e impactos de riesgos asociados:



La citada guía también explica de manera breve los regímenes de debida diligencia en el conocimiento del cliente, así como las etapas de identificación, verificación y monitoreo.

Cabe precisar que los conceptos descritos en la guía son generales y los pasos establecidos, como parte de la metodología de trabajo, son referenciales. Es necesario que los sujetos obligados dedicados a la construcción y/o inmobiliaria analicen el contenido de la guía para establecer procedimientos que se ajusten a la realidad operativa del negocio y a su nivel de exposición a los riesgos de LA/FT, teniendo en cuenta lo dispuesto en la normativa vigente.

Puede acceder a la "Guía para la aplicación de la debida diligencia en el conocimiento del cliente con un enfoque basado en riesgos, dirigida al sector de construcción y/o inmobiliario" en el siguiente enlace:
https://www.sbs.gob.pe/Portals/5/jer/GUIAS_OC/files/Guia-DDC-2020.pdf

Fraude: ¿cómo reconocer posibles casos?

La Unidad de Inteligencia Financiera de EE.UU. (Fincen) expuso varias señales de alerta que pueden ayudar a empresas y entidades financieras a identificar presuntos defraudadores.

La emergencia originada por el Covid-19, ha generado vulnerabilidades que pueden incidir en el incremento de estafas cibernéticas alrededor del mundo. Por ello, Fincen publicó un documento *denominado "Asesoramiento sobre cibercrimen y delitos cibernéticos que explota la pandemia por el Covid-19".*

En dicho documento, la autoridad estadounidense advierte que *"la importante migración hacia el acceso remoto (…) presenta oportunidades para que los delincuentes exploten los sistemas remotos de las instituciones financieras y los procesos orientados al cliente".*

En ese sentido, se observa una tendencia en la que ciberdelincuentes atacan las aplicaciones remotas y los entornos virtuales para robar información confidencial, comprometer la actividad financiera e interrumpir las operaciones comerciales. Asimismo, se observan casos de cibercriminales que usan listas de credenciales robadas (nombres de usuarios, direcciones de correo electrónico y contraseñas asociadas) para realizar intentos de inicio de sesión automatizados para obtener acceso no autorizado a las cuentas de las víctimas.

Fincen asegura que los delincuentes buscan socavar los procesos de verificación de identidad en línea, mediante el uso de documentos de identidad fraudulentos, los cuales .pueden crearse manipulando imágenes digitales de documentos de identidad legítimos emitidos por los gobiernos o para alterar la información y/o las fotografías que allí se muestran.

Señales de alerta de posibles fraudes

Con el propósito de ayudar a las instituciones financieras a detectar, prevenir e informar posibles actividades delictivas relacionadas con el Covid-19, Fincen hizo publico un listado de señales de alerta, el cual se detalla a continuación:

1. Ortografía: Hay que prestar atención a la ortografía de los nombres registrados en las cuentas financieras, ya que a veces se encuentran inconsistencias con la información de identidad emitida por el gobierno

2. Imágenes editadas: Es común encontrar imágenes borrosas o de baja resolución, así como defectos en las áreas alrededor de los rostros en los documentos.

Asimismo, se debe tener cuidado con las imágenes en documentos de identidad que muestren signos visuales indicativos de una posible manipulación. Tal es el caso de incongruencias en la coloración cerca del borde de la cara, o bordes o líneas dobles en rasgos faciales delineados.

3. Manipulación de campos: Otra señal de alerta es la de documentos de identidad en los que se observen irregularidades visuales que indiquen manipulación digital, especialmente en torno a los campos de información, por ejemplo, dentro de los campos relacionados con el nombre, dirección y otros identificadores.

4. Cambios físicos y no suministro de datos: Se recomienda tomar controles para detectar casos en los que la descripción física de un cliente en sus documentos de identidad no coincida con otras imágenes previas del cliente. Además, es importante identificar a aquellos clientes que se nieguen a proporcionar documentos de identidad complementarios o que se demoren en exceso en el envío.

5. Accesos inusuales: Es importante prestar atención a los inicios de sesión de clientes que se realicen desde un solo dispositivo o dirección de Protocolo de Internet (IP) para acceder a varias cuentas aparentemente no relacionadas, a menudo en un corto período.

Adicionalmente, se sugiere revisar si la dirección IP asociada con los inicios de sesión no coincide con la dirección indicada por el cliente en su documentación.

Por otra parte, es aconsejable tomar medidas para identificar los inicios de sesión de clientes que se produzcan dentro de un patrón de alto tráfico de red con tasas de éxito de inicio de sesión disminuidas y tasas de restablecimiento de contraseña aumentadas.

6. Extraños comportamientos de clientes: Una señal de alerta que toda entidad financiera debería incluir en su sistema de prevención del fraude es la de clientes que se ponen en contacto para cambiar los métodos de autenticación y de comunicación de sus productos financieros, y luego intentan rápidamente realizar transacciones en una cuenta que nunca antes había recibido pagos de ese cliente.

Fuente: https://www.infolaft.com/fraude-como-reconocer-posibles-casos/

Beneficiarios finales: mejores prácticas para su conocimiento

La detección automática de cambios en la participación accionaria de empresas es uno de los controles más eficaces para detectar a los propietarios.

Una de las tareas más complejas de los oficiales de cumplimiento consiste en identificar a los beneficiarios finales de las personas jurídicas con las que tienen relación.

Esto debido a que muchos países, sobre todo de Latinoamérica, todavía carecen de la legislación y las herramientas tecnológicas que permitan dinamizar ese proceso.

En ese sentido, con el propósito de brindar mejores prácticas para fortalecer los sistemas de prevención del lavado de activos y la financiación del terrorismo del continente, el Grupo de Acción Financiera de Latinoamérica (GAFILAT) **publicó una versión traducida en español de una guía del Grupo de Acción Financiera Internacional (GAFI) sobre beneficiarios finales**.

Dentro del referido documento se comparten ejemplos de casos que permiten conocer las estrategias usadas por varios países europeos para develar quién o quiénes están detrás de las compañías.

El reporte, titulado *"Mejores prácticas sobre beneficiarios finales para personas jurídicas"*, también incluye algunas señales de alerta que pueden ser utilizadas por gobiernos y oficiales de cumplimiento de la región.

Registros de empresas, factor clave:

Según el referido reporte, los países y sujetos obligados deberían adoptar medidas de verificación cruzada para verificar o monitorear la información sobre el beneficiario final, aprovechando la disponibilidad de diferentes agentes de información.

A manera de ejemplo, se recomienda a las instituciones financieras y a las actividades y profesiones no financieras designadas (APNFD) verificar la información básica y del beneficiario final que les proporcionan las empresas con la información disponible en el registro que posee la empresa.

Además, sugiere a dichos sujetos obligados supervisar continuamente los cambios en los registros, incluidas las designaciones de empresas infractoras y consultar a sus clientes sobre posibles discrepancias. La manera sencilla de hacerlo, asegura el GAFILAT, es a través de interfaces automatizadas por computadora.

Cruces de información:

El GAFILAT señala que algunos países implementan controles de verificación cruzada automatizados entre las bases de datos mantenidas por diferentes instituciones públicas. Ello en base en a la interrelación de la información disponible y los procedimientos implementados por las autoridades gubernamentales. En ese sentido, en la guía se aconseja desarrollar un portal común para que la información del registro de empresas se pueda cruzar con otras bases gubernamentales, entre ellas los repositorios de sanciones y las fuentes de administración tributaria e inscripción de tierras.

Señales de alerta relacionadas con beneficiarios finales:

De acuerdo con lo señalado por el GAFILAT, algunos países establecen indicadores *"que sugieren actividades sospechosas"*. Tal es el caso de tarjetas de crédito o direcciones de correo electrónico que se utilizan para incorporar muchas empresas que, en apariencia, no están conectadas. Cuando esta señal de alerta es detectada, los registros de empresas de algunas jurisdicciones informan a las autoridades competentes sobre las presuntas actividades sospechosas.

De igual manera, algunos sujetos obligados suelen establecer indicadores sobre los ingresos de las empresas –ingresos en efectivo y nivel de activos– y estos datos se comparan con el promedio de la industria, por lo que los resultados posteriores anormales y/o significativos se consideran sospechosos y, por lo tanto, están sujetos a una evaluación adicional.

Asimismo, el GAFILAT señala que en algunos países, es tal el nivel de avance que los sistemas de registro están en capacidad de detectar cualquier variación en la información presentada por las empresas (es decir, aumento de acciones, transferencias de propiedad) y también comparar los indicadores relevantes con el promedio de la industria, por lo que cuando se identifican variaciones inusuales, los sistemas activan unas alertas y envían los respectivos reportes para una mayor investigación.

Fuente:https://www.infolaft.com/beneficiarios-finales-mejores-practicas-para-su-conocimiento/

El acceso al documento" Mejores prácticas sobre beneficiarios finales para personas jurídicas" puede ser obtenido a través del siguiente enlace: https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/buenas-practicas-18/3826-mejores-practicas-sobre-beneficiarios-finales-para-personas-juridicas/file

Actualidad

Próximos cambios en la recomendación 1 del GAFI

El GAFI hará ajustes en la recomendación 1 y recibirá opiniones y aportes de oficiales de cumplimiento de todo el mundo.

Cabe indicar que la recomendación 1 del GAFI solicita a los países identificar, evaluar y entender su exposición a los riesgos de lavado de activos y financiación del terrorismo.

Según el referido organismo, *"con base en esa evaluación, los países deben aplicar un enfoque basado en riesgo a fin de asegurar que las medidas para prevenir o mitigar el lavado de activos y el financiamiento del terrorismo sean proporcionales a los riesgos identificados"*.

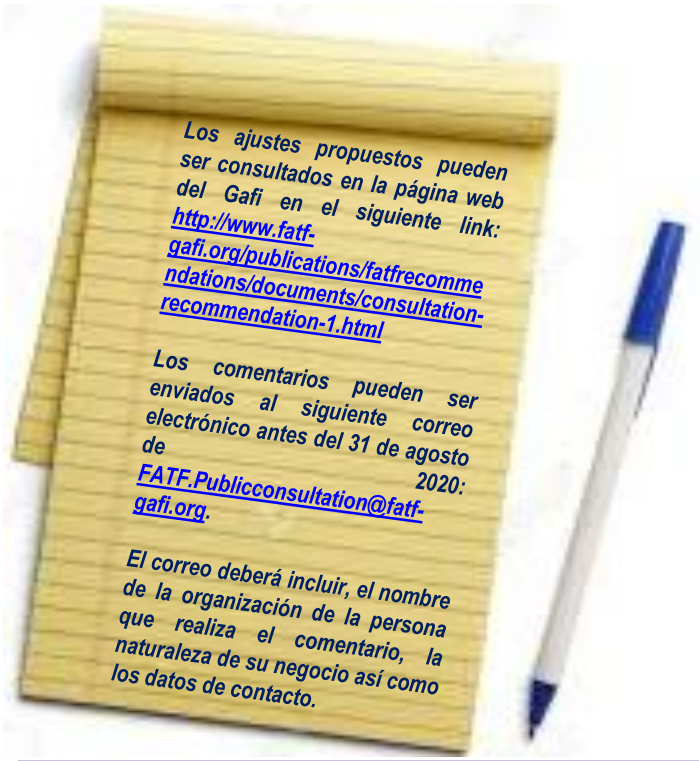
El citado estándar sería modificado en los próximos meses y para ello el GAFI anunció que está consultando a todas las partes interesadas afectadas antes de finalizar estas enmiendas.

Dentro de esas partes interesadas se encuentran, los oficiales y analistas de cumplimiento de toda clase de industrias obligadas a implementar sistemas de prevención del LA/FT, así como funcionarios de instituciones públicas nacionales.

Concretamente, los ajustes que propone el GAFI buscan reforzar la implementación de sanciones financieras específicas y se crearían las siguientes obligaciones para las entidades financieras y las APNFD:

- Evaluar los riesgos de incumplimiento, no implementación y evasión de sanciones financieras específicas relacionadas con el financiamiento de la proliferación.

- Tomar las medidas de mitigación apropiadas proporcionales al nivel de riesgos identificados.



Fuente: https://www.infolaft.com/habria-proximos-cambios-en-la-recomendacion-1-del-gafi/

Avisos Importantes

Inclusión de 01 persona en la Lista de Sanciones contra el EIIL (Daesh) y Al-Qaida del Consejo de Seguridad de las Naciones Unidas (CSNU)

El 16 de julio de 2020 el Comité del Consejo de Seguridad, establecido en virtud de las Resoluciones del CSNU 1267 (1999), 1989 (2011) y 2253 (2015), aprobó la inclusión de 1 persona a la Lista de Sanciones contra el EIIL (Daesh) y Al-Qaida.

La persona incluida en la referida lista es la siguiente:

QDi.427 **Nombre**: 1: Noor 2: Wali 3: Mehsud 4: na **Título:** Mufti **Designación:** na **DOB:** 26 Jun. 1978 **POB:** Gurguray, Pakistan **También conocido como:** Abu Mansoor Asim **Baja calidad alias:** na **Nacionalidad:** Pakistan **Pasaporte no.:** na **Identificación Nacional no.**: na. **Dirección:** na, **Incluido en la lista:** 16 de julio de 2020. **Otra Información:** Líder del movimiento denominado Tehrik-e Taliban Pakistan (TTP)(Qde.132)

Fuente:https://www.un.org/press/en/2020/sc14256.doc.htm