SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

República del Perú

Boletín informativo

Año 2024
Edición N° 142

Prevención de Lavado de Activos y Financiamiento del Terrorismo

Superintendencia Adjunta de Unidad de Inteligencia Financiera del Perú

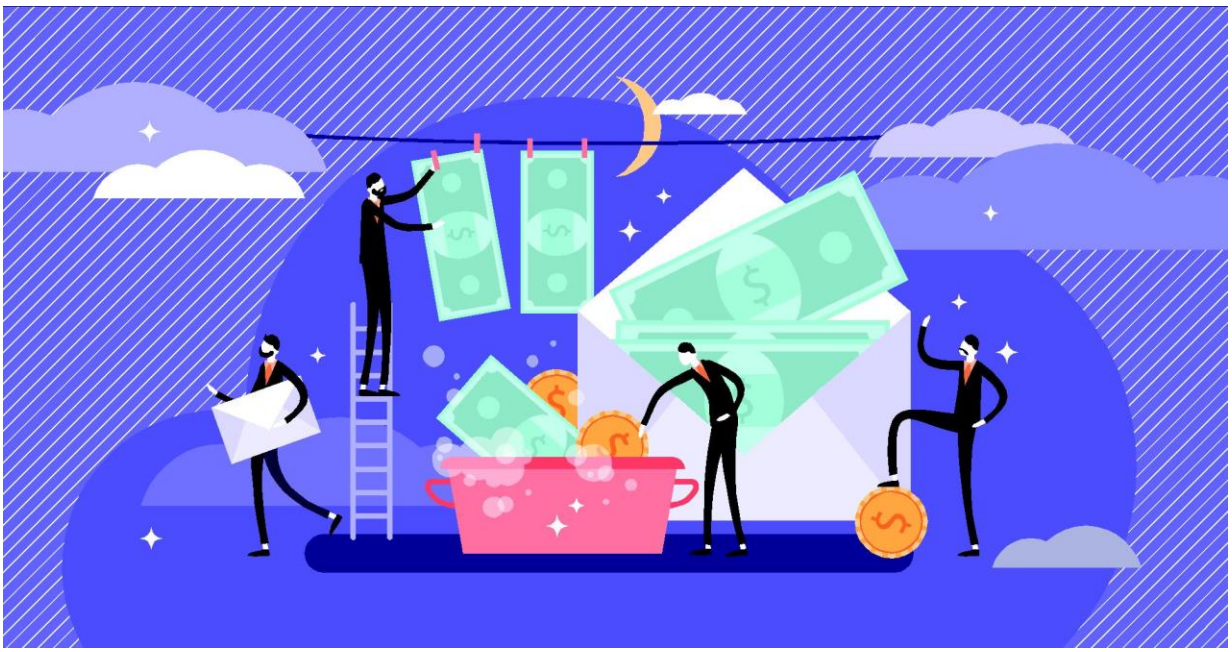
Contenido

Avisos importantes

Herramientas

Actualidad

1. Semana de Prevención del Lavado de Activos 2024



En el marco del día contra el lavado de activos, conmemorado cada 29 de octubre por la comunidad internacional, la Superintendencia de Banca, Seguros y AFP (SBS), con el apoyo de Cooperación Suiza a través de la Secretaría de Estado para Asuntos Económicos (SECO), ha organizado la Semana de Prevención del Lavado de Activos 2024. El objetivo del evento es fortalecer el intercambio de información y difundir estrategias para la prevención del lavado de activos frente a los delitos precedentes.

Entre el 28 y 31 de octubre, como parte de dicho evento, la SBS programó la realización de 15 charlas virtuales gratuitas a cargo de expertos nacionales e internacionales de Argentina, Paraguay y Colombia; así como de organismos internacionales como la Organización de Estados Americanos (OEA), Grupo de Acción Financiera de Latinoamérica (GAFILAT) y el Grupo Egmont.

Ir a contenido

Avisos importantes

A los participantes que se hayan conectado como mínimo a 5 charlas, se les hará llegar, a través del correo electrónico, una constancia de participación al finalizar el evento. La plataforma del evento estará disponible hasta el 08 de noviembre para quienes deseen ver las grabaciones de las charlas realizadas. Asimismo, las grabaciones estarán disponibles a través del canal de YouTube de la UIF.

Para acceder a la plataforma de la Semana de Prevención del Lavado de Activos, ingresar aquí.

Para acceder al canal de YouTube de la UIF, ingresar aquí.

1. Estudio sobre buenas prácticas y recomendaciones para el diseño y aplicación de un marco sancionatorio proporcional y disuasivo

Recientemente, el Grupo de Acción Financiera de Latinoamérica (GAFILAT) ha publicado el documento denominado "*Estudio sobre buenas prácticas y recomendaciones para el diseño y aplicación de un marco sancionatorio proporcional y disuasivo*". El estudio efectuado es

una herramienta para el diseño y la aplicación de un marco sancionatorio adecuado a los requisitos de la Recomendación N° 35 (R.35) del Grupo de Acción Financiera Internacional (GAFI), en el cual se analiza la situación actual de los países de la región y se formulan recomendaciones y buenas prácticas que permitan fortalecer el marco normativo y la aplicación de las sanciones.

La R.35 del GAFI señala que "*los países deben asegurar que exista una gama de sanciones eficaces, proporcionales y disuasivas, sean penales, civiles o administrativas, que estén disponibles para tratar a las personas naturales o jurídicas cubiertas en las Recomendaciones 6 y 8 a la 23, que incumplan con los requisitos antilavado de dinero y contra el financiamiento del terrorismo (ALA/CFT). Las sanciones deben ser aplicables no sólo a las instituciones financieras y a las actividades profesionales no financieras designadas (APNFD), sino también a sus directores y la alta gerencia*."

Dicha recomendación no solo busca disuadir a los infractores, sino también salvaguardar la integridad y estabilidad del sistema financiero global. Esta abarca varios aspectos, desde la imposición de multas y penas, hasta la disolución de entidades que incumplen las normativas ALA/CFT. Cabe señalar que todas las obligaciones que recaigan sobre los ciudadanos, en cualquier ámbito, deben ir acompañadas de medidas que tengan la finalidad de corregir el incumplimiento de aquellas.

Al respecto, es importante recordar que una de las claves para la mejora de los sistemas ALA/CFT de los países miembros del GAFILAT, de cara a la próxima Quinta Ronda de Evaluaciones Mutuas, es el desarrollo de acciones que promuevan marcos sancionatorios proporcionales y disuasivos para todos los tipos de sujetos obligados; y que estas permitan un mayor grado de cumplimiento a las exigencias de los estándares internacionales.

Herramientas

Como referencia, es preciso indicar que la normativa peruana incluye como delito la omisión de comunicación de operaciones sospechosas; asimismo incluye infracciones vinculadas al oficial de cumplimiento, al manual de prevención y gestión de riesgos de LA/FT, la capacitación, las auditorías, el Informe Anual del Oficial de Cumplimiento, entre otros; y contempla multas para los accionistas o socios, directores, gerentes y principales funcionarios de las personas jurídicas.

Para acceder al estudio, *ingresar aquí*.

2. Medidas de debida diligencia con relación a las personas expuestas políticamente (PEP)

Las personas expuestas políticamente (PEP) son personas naturales, nacionales o extranjeras, que cumplen, o que en los últimos cinco (5) años hayan cumplido, funciones públicas destacadas o funciones prominentes en una organización internacional, sea en el territorio nacional o extranjero, y cuyas circunstancias financieras puedan ser objeto de un interés público (Revisar la Resolución SBS N° 4349-2016).

Herramientas

Las normas en materia de prevención del lavado de activos y del financiamiento del terrorismo (LA/FT) establecen que las PEP están consideradas en los tipos de clientes a los que corresponde la aplicación de procedimientos reforzados de debida diligencia, debido a que podrían estar altamente expuestas a los riesgos de LA/FT y/o delitos precedentes. En consecuencia, los sujetos obligados deben recopilar y verificar mayor información respecto a dichos clientes, con el propósito de corroborar que sus perfiles guardan congruencia con las características de las operaciones que se disponen a realizar, o ya han realizado, y/o detectar la activación de señales de alerta.

De acuerdo con el artículo 16 de la Resolución SBS N° 789-2018, los sujetos obligados deberán solicitar a sus clientes bajo la categoría de PEP la siguiente información:

- el cargo y el nombre de la institución (organismo público u organización internacional);
- el nombre de sus parientes hasta el segundo grado de consanguinidad y segundo de afinidad, así como del cónyuge o conviviente; y,
- la relación de personas jurídicas o entes jurídicos en los que tenga la condición de beneficiario final, de conformidad con el artículo 4 del Decreto Legislativo N° 1372 y sus modificatorias.

Dicha información también deberá ser solicitada por el sujeto obligado cuando el cliente adquiera la condición de PEP, luego de haber iniciado relaciones comerciales. Además, si el beneficiario de la operación es un tercero (persona natural), el sujeto obligado deberá requerir, entre otros datos, información respecto a si esta es o ha sido PEP, precisando, de ser el caso, el cargo y el nombre de la institución (organismo público u organización internacional).

Herramientas

Asimismo, el sujeto obligado deberá:

- incrementar la frecuencia en la revisión de las operaciones que realiza la PEP (la periodicidad, los montos, el tipo de operaciones que realiza, entre otros), según corresponda;

- realizar mayores indagaciones y aplicar medidas adicionales de identificación y verificación de la información de la PEP, por ejemplo: (i) recolectar información de fuentes públicas o abiertas (Infogob, Contraloría, Registros Públicos, Agencias de Noticias, entre otros), (ii) solicitar documentación que acredite su centro laboral, (iii) verificar la identidad de la persona que realiza los pagos (a través de los datos de la transferencia, depósito u otros); (iv) u otras que el sujeto obligado considere pertinentes, a fin de contar con información más completa del cliente, que permita identificar posibles operaciones inusuales y/o sospechosas.

Para acceder a la lista de funciones y cargos ocupados por PEP, *ingresar aquí*.

3. Lanzamiento del Algoritmo para la Legalidad de Madera de la Amazonía (ALMA)

Considerando que entre el 2001 y el 2023, en el Perú se ha perdido un total de 3,053,354 hectáreas de bosque amazónico (según información de GEOBOSQUES), y que esta pérdida forestal amenaza a miles de especies de fauna y flora únicas, el 15 de agosto del presente año, Proética (Capítulo Peruano de *Transparency International*) en alianza con el *Center for International Environmental Law* (CIEL) y la *Environmental Investigation Agency* (EIA), lanzaron una herramienta denominada "Algoritmo para la Legalidad de Madera de la Amazonía" (ALMA).

Esta herramienta tiene como objetivo el análisis de riesgo sobre el posible origen ilegal de madera extraída en el Perú, a partir de información consignada en una guía de transporte forestal amparada en un plan de manejo forestal, el cual analiza y proyecta la probabilidad o el riesgo de que la madera extraída tenga un origen ilegal.

Herramientas

Es importante precisar que, este algoritmo identifica la probabilidad de la ilegalidad del producto maderable, posterior a ello, la autoridad deberá coordinar con las autoridades competentes para tener la certeza de que la madera tiene un origen ilegal.

Esta herramienta resultaría relevante para los sistemas de prevención de lavado de activos, dado que podría ser utilizada en los procesos de debida diligencia de sujetos obligados que cuenten con clientes vinculados de forma directa o indirecta con la actividad forestal.

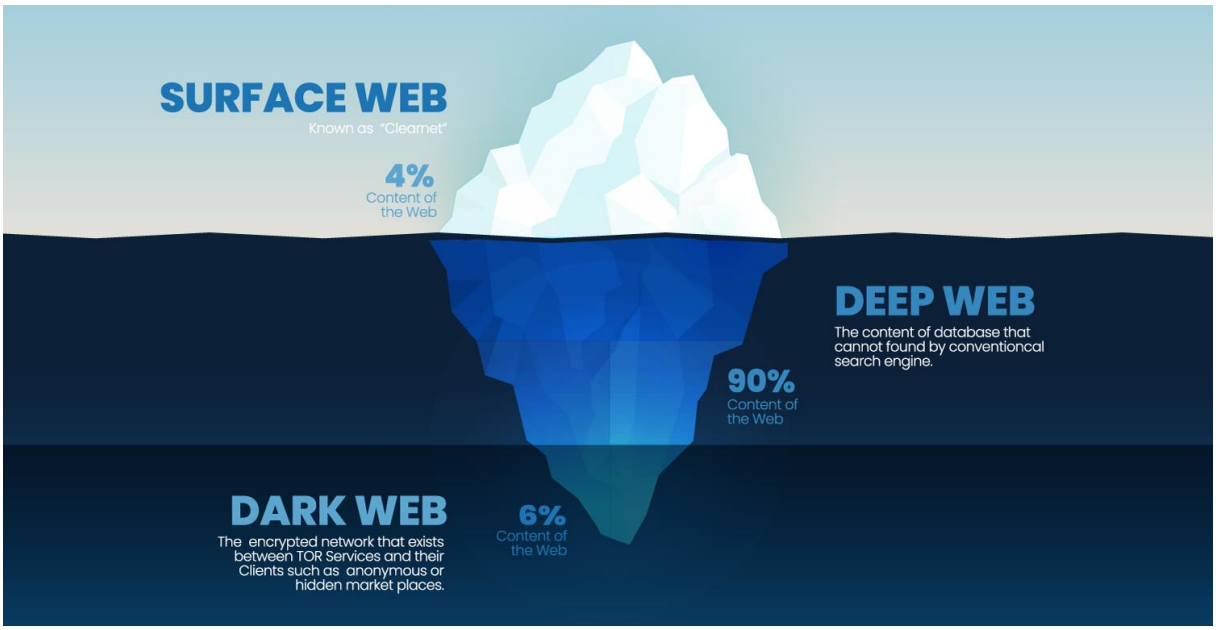
Para acceder a la herramienta ALMA, ingresar aquí.
Para acceder a GEOBOSQUES, ingresar aquí.

4. El Comité de CSNU añade dos entradas a su lista de sanciones

El 27 de setiembre de 2024, el Comité del Consejo de Seguridad de las Naciones Unidas (CSNU), establecido en virtud de la Resolución N° 2653 (2022) aprobó la adición de dos entradas en su Lista de sanciones de personas y entidades sujetas a las medidas impuestas por el CSNU y adoptadas en virtud del Capítulo VII de la Carta de las Naciones Unidas.

Para acceder al artículo, ingresar aquí.

1. La web oscura y su relación con el LA/FT/FP



Con el objetivo de entender que es la web oscura o *Dark web*, como es más conocida por su denominación en inglés, debemos pensar en un iceberg. Un iceberg es una gran masa de hielo que flota en el mar dejando ver solo una parte de su masa, mientras el resto se mantiene sumergida. Por ese motivo se volvió tan conocida la frase "es solo la punta del iceberg" para referirnos a que solo se conoce un aspecto pequeño de un todo, por ejemplo, cuando se descubre la comisión de un delito, pero aún no se ha logrado detectar toda la red criminal detrás de dicho delito, que sigue manteniéndose en las sombras.

En el caso de la web (*World Wide Web*) sucede lo mismo, existen millones de páginas web, bases de datos y servidores que funcionan las 24 horas del día. Sin embargo, la internet abierta o superficial, a la cual podemos acceder a través de motores de búsqueda como *Google* o *Internet Explorer*, solo es la punta del iceberg (alrededor del

4% del contenido de la web). Los sitios web se suelen identificar con operadores de registro como “.com” u “.org” y es posible localizarlos porque los motores de búsqueda pueden recorrer la web a través de enlaces visibles. Pensemos en los motores de búsqueda como barcos de pesca que solo pueden “capturar” sitios web cerca de la superficie. Todo lo demás, desde revistas académicas hasta bases de datos privadas, o inclusive contenido ilícito, está fuera de alcance.

Por debajo de la superficie se encuentra la web profunda o *Deep web* (alrededor del 90% del contenido de la web). Esta sería la parte de un iceberg debajo del agua, mucho más grande que la web superficial. De hecho, la web profunda es tan grande que es imposible determinar con precisión cuántas páginas o sitios web están activos en un momento determinado.

Gran parte del contenido en la web profunda es perfectamente legal y seguro. La web profunda incluye bases de datos protegidas, de carácter público o privado, de acceso restringido a través de sitios web específicos. Asimismo, incluye *intranets* de empresas, gobiernos o instituciones educativas, utilizadas para comunicar o controlar aspectos privados dentro de las propias organizaciones. Dichos sitios web pueden ocultarse detrás de contraseñas o solicitando a los motores de búsqueda que no rastreen su ubicación en la web. Sin perjuicio de ello, aún es posible acceder a dichos sitios en la web profunda haciendo uso de navegadores de Internet convencionales.

Por otro lado, la web oscura o *dark web* se suele asociar a mercados que ofrecen una amplia gama de bienes y servicios ilegales, por ejemplo: datos robados, drogas, armas, herramientas de piratería, *malware* y moneda falsificada. Considerando la analogía del iceberg, la web oscura sería la punta inferior del iceberg sumergido. No obstante, las partes legales también han hecho uso de esta web para aprovechar los beneficios que otorga respecto al anonimato y rastreo

de sitios web. Sin perjuicio de ello, la web oscura se mantiene en una zona gris, dado que utilizarla suele significar que se está intentando realizar una actividad que, de otro modo, no podría llevarse a cabo a la vista del público. El acceso a la web oscura solo es posible a través de un navegador web especializado, la forma más rápida de acceder es haciendo uso del navegador TOR (proyecto "*The Onion Routing*").

La investigación de actividades ilícitas en la web oscura siempre ha representado un reto para las agencias gubernamentales encargadas de detectar y perseguir delitos como el lavado de dinero, el financiamiento del terrorismo, el financiamiento de la proliferación de armas de destrucción masiva (LA/FT/FP) y otros delitos precedentes. Dicho reto se intensificó a partir de las medidas de distanciamiento social adoptadas por los países para combatir la pandemia causada por la COVID-19. Dado que la única forma viable de comunicarse o coordinar el envío de cosas era a través de la web, empezó a surgir información nueva sobre actividad sospechosa en la web oscura (incremento de la actividad ilegal).

Asimismo, el uso de activos virtuales en la web oscura también plantea importantes retos en la lucha contra el LA/FT/FP. Las criptomonedas son especialmente populares entre los vendedores de artículos tales como drogas ilegales, armas y otros bienes restringidos que podrían estar directamente relacionados al LA/FT/FP.

2. Ataque terrorista ocurrido en Karachi (Pakistán)

La noche del domingo 6 de octubre, un convoy que transportaba a trabajadores de nacionalidad china de la compañía eléctrica Port Qasim Limited fue atacado cerca del Aeropuerto Internacional de Jinnah, en Karachi, al sur de Pakistán. En el siniestro murieron dos ciudadanos chinos y un ciudadano pakistaní y resultaron heridos varios ciudadanos chinos y pakistaníes.

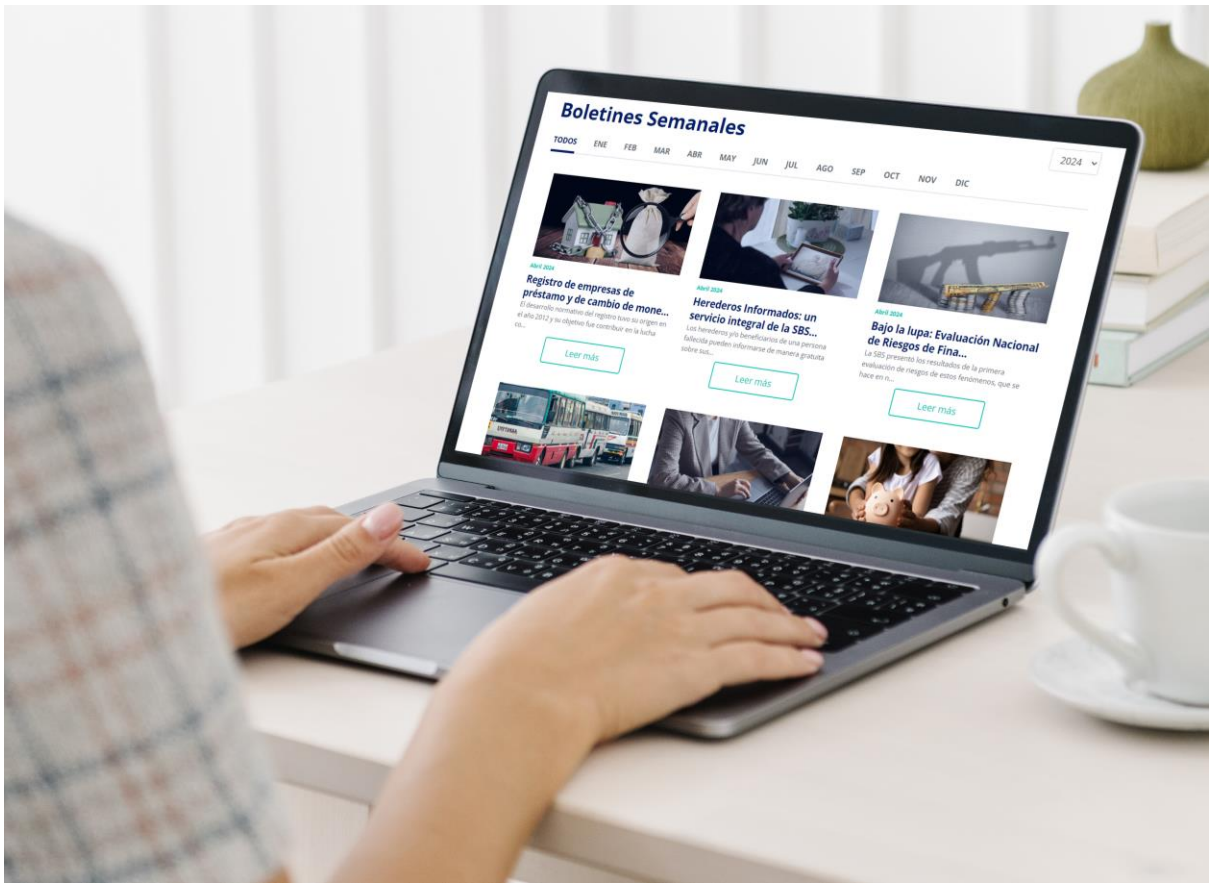
El Ejército de Liberación Baluchistán (BLA) afirmó que el ataque fue perpetrado por su Brigada Majeed. Este grupo armado opera principalmente en la provincia vecina de Baluchistán, y en los últimos años ha protagonizado varios ataques contra ingenieros chinos, que

en su mayoría son destinados a Pakistán para trabajar en el multimillonario Corredor Económico China-Pakistán (CPEC).

Este no es el único atentado terrorista ocurrido en Pakistán en el año 2024, en marzo, al menos seis personas murieron cuando un atacante suicida detonó su carga explosiva contra un convoy de ingenieros chinos en el distrito de Shangla, en la provincia norteña de Khyber Pakhtunkhwa, matando a cinco trabajadores chinos y a un paquistaní.

Ataques terroristas como los acontecidos en Pakistán reafirman la importancia de que los países establezcan medidas para combatir el financiamiento del terrorismo.

3. Boletines semanales de la SBS



La SBS publica semanalmente boletines informativos sobre temas de actualidad relacionados a sus funciones como regulador y supervisor de los sistemas financiero, de seguros, privado de pensiones, cooperativo de ahorro y crédito, y de prevención de LA/FT/FP.

Los invitamos a leer los boletines publicados. Entre los artículos más recientes se encuentra el relacionado a las principales funciones y responsabilidades de los notarios y del Órgano Centralizado de Prevención (OCP).

> Para acceder a los boletines semanales de la SBS, ingresar aquí.

Encuesta Boletín

Tu opinión es importante, por lo que te agradeceremos llenar la encuesta a fin de conocer cómo fue tu experiencia con el contenido del Boletín UIF, y qué temas te gustaría que incluyamos en las próximas ediciones.

> Para acceder a la encuesta, ingresar aquí

Ir a contenido

Boletín informativo

Año 2024
Edición N° 142

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú