SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

República del Perú

Boletín informativo

Año 2023
Edición N° 121

Prevención de Lavado de Activos y Financiamiento del Terrorismo

Superintendencia Adjunta de Unidad de Inteligencia Financiera del Perú

Contenido

Avisos importantes

Herramientas

Actualidad

1. Tutorial para comunicar la designación del OC a través del SISDEL

La comunicación de la designación del Oficial de Cumplimiento (OC), se realiza a través del Sistema de Designación en Línea del Oficial de Cumplimiento (SISDEL), siendo para ello necesario la creación de una cuenta de usuario.

Avisos importantes

A continuación, se muestran los enlaces en los cuales se muestran cómo realizar paso a paso, la creación de una cuenta de usuario y la comunicación de la designación del OC:

https://plaft.sbs.gob.pe/sisdel/

https://www.youtube.com/watch?v=8lZqVQEL0u0

https://www.youtube.com/watch?v=onMPWfoEIRo

2. Remisión del IAOC correspondiente al año 2022

Se recuerda a los sujetos obligados que se encuentran bajo el amparo de la Resolución SBS N° 5709-2012, Resolución SBS N° 789-2018 y Resolución SBS N° 5060-2018 (COOPAC Nivel 1) que tienen la obligación de remitir el Informe Anual del Oficial de Cumplimiento (IAOC) correspondiente al año 2022 a la Unidad de Inteligencia Financiera (UIF) hasta el 15 de febrero del 2023 a través del Portal de Prevención del Lavado de Activos y Financiamiento del Terrorismo (plaft.sbs.gob.pe).

Cabe señalar que en caso los sujetos obligados no remitan su IAOC correspondiente al año 2022, estarían incurriendo en una infracción grave, siendo pasibles de que se le imponga una sanción de acuerdo a lo establecido en la Resolución SBS N° 8930-2012 y la Resolución SBS N° 2755-2018, según corresponda.

El detalle del contenido mínimo se encuentra en el boletín informativo N° 20. Para acceder a dicho boletín ingresar aquí

2. Riesgo de Lavado de Activos proveniente de Minería Ilegal

En la Evaluación Nacional de Riesgos 2021, se señala que como resultado de la etapa de análisis y valoración de amenazas y vulnerabilidades, se obtuvo como riesgos de Lavado de Activos (LA) a la minería ilegal.

Avisos importantes

Al respecto, se indica que el nivel de riesgo asociado con el LA, proveniente de la minería ilegal en el Perú, es muy alto.

Sobre el particular, según la información estadística disponible, el dinero ilícito proveniente de esta actividad afecta, principalmente, a los sectores de bancos, agentes de aduanas y cajas municipales de ahorro y crédito.

Más de 50% de los Reportes de Operaciones Sospechosas y de los Informes de Inteligencia Financiera, relacionados con este delito, tienen un alcance internacional, involucrando principalmente a los países de India, Emiratos Árabes Unidos, Hong Kong, Suiza y Estados Unidos.

En el ámbito nacional, se aprecia que los mayores montos acumulados corresponden a operaciones sospechosas llevadas a cabo en las regiones de Lima, Puno, Callao y Madre de Dios; y que los principales tipos de productos utilizados son las cuentas de ahorros, exportaciones/ importaciones, y cuentas corrientes.

Avisos importantes

Asimismo, se reporta que el dinero trata de ser lavado por personas naturales de nacionalidad peruana, de profesión independiente-empresario, domiciliadas en Lima o Puno, y con un rango de edad entre 25 y 55 años; así como, personas jurídicas del tipo Empresa Individual de Responsabilidad Limitada y Sociedad Anónima Cerrada, del sector de Explotación de minas y canteras, domiciliadas en Puno, Lima o Madre de Dios, y con una antigüedad de creación menor a 1 año.

Por otro lado, las tipologías más utilizadas para lavar el dinero proveniente de esta actividad ilegal son:

- El uso de recursos ilícitos o no justificados destinados u obtenidos de la inversión en el sector minero (oro ilegal y otros minerales).

- Transferencias remitidas o recibidas al/del exterior producto de exportaciones o importaciones ficticia de bienes, no concordantes o relacionadas con mercancías sobrevaloradas o subvaluadas.

- Depósitos y/o transferencias fraccionadas de dinero ilícito o no justificado.

< Accede al informe completo aquí

Preguntas y respuestas relacionadas al IAOC

1 ¿Quién debe aprobar el Informe Anual del Oficial de Cumplimiento (IAOC) en caso el sujeto obligado no cuente con un directorio?

Puede ser aprobado por el gerente general, gerente, el titular gerente o administrador según sea el caso.

Herramientas

2 ¿En caso de un grupo económico, el oficial de cumplimiento corporativo (OCC) puede presentar un solo IAOC por todo el grupo?

En los casos de un OCC, este debe presentar un IAOC por cada uno de los sujetos obligados que formen parte del grupo económico, a más tardar el 15.02.2023.

3 ¿Si no se han detectado operaciones sospechosas, es obligatorio remitir el IAOC a la UIF?

Es obligatorio que se remita el IAOC a la UIF, dado que la información sobre las operaciones sospechosas reportadas a la UIF solo constituye una parte de la información mínima que contiene el IAOC.

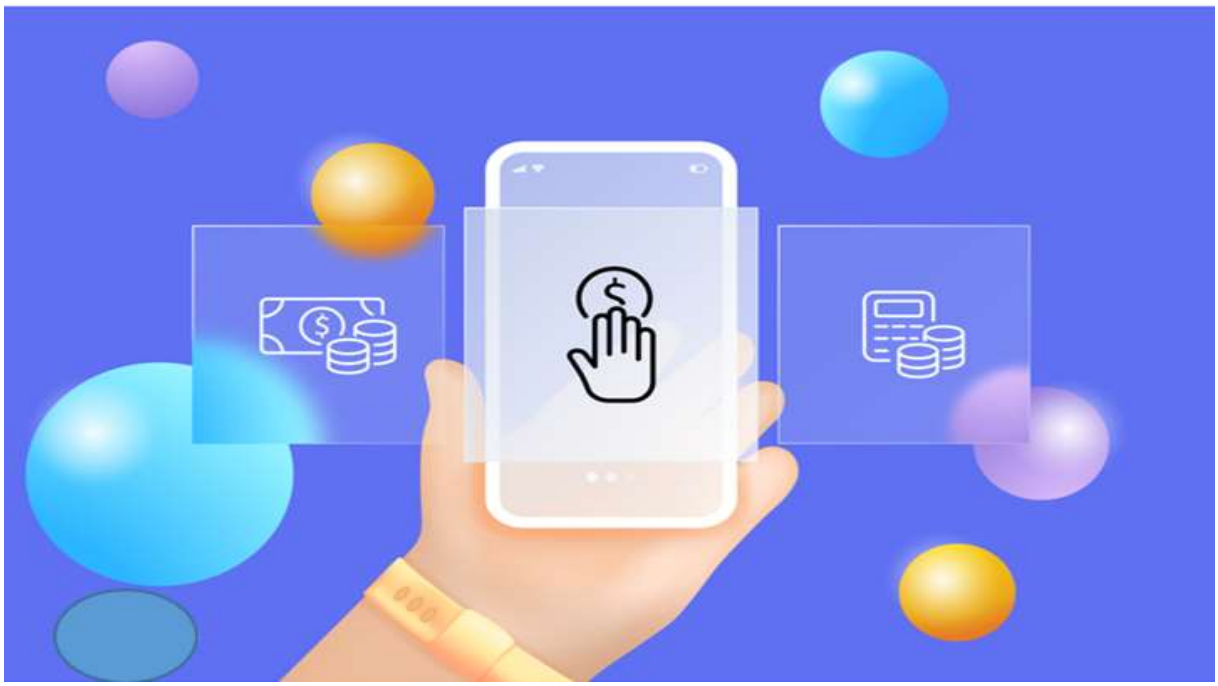
4 ¿Se puede remitir el IAOC después de su fecha de vencimiento?

Los sujetos obligados, pueden remitir el IAOC después de su vencimiento, a través del Portal PLAFT. No obstante ello, la UIF podría iniciar un procedimiento administrativo sancionador.

BUZÓN DE PREGUNTAS

Si tuviera alguna pregunta relacionada a temas de prevención del lavado de activos y del financiamiento del terrorismo, puede remitirla al siguiente correo: boletin_uif@sbs.gob.pe
Entre las preguntas enviadas, se elegirán algunas, las cuales serán absueltas en nuestro próximo boletín.
Importante: El presente buzón de preguntas no reemplaza a los canales oficiales de consulta con los que cuenta la UIF.

1. SBS advierte sobre esquemas de préstamos informales mediante aplicativos (App)



La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS), ante diversas consultas y en salvaguarda de los intereses de los ciudadanos, advierte que vienen operando en el país aplicativos (App) de préstamos de dinero que no están inscritos en el Registro de Empresas y Personas que efectúan Operaciones Financieras o de Cambio de Moneda, a cargo de la SBS.

Se han detectado los siguientes aplicativos (App) o plataformas virtuales a través de los cuales se ofrecen y desembolsan préstamos de dinero, sea a solicitud del usuario o, incluso, sin que el usuario los haya solicitado.

Cabe precisar que cuando el usuario descarga estos aplicativos (App) en su teléfono celular, le exigen brindar información personal y acceso al directorio de sus contactos, así como recopilar y monitorear información de su celular.

Asimismo, al momento de requerir a los usuarios el pago de los préstamos, estos aplicativos (App) incluyen cargos e intereses elevados, y amenazan a los usuarios con informar a todos sus contactos su supuesta condición de deudor, así como la atribución de hechos o situaciones agraviantes, que vulneran su honor y les infunde temor. Por tanto, se recomienda no consultar ni descargar estos aplicativos (App) o similares:

- ALPACASH
- C PLATINKA
- CARTERAPRÉSTAMO / CARTERA PRÉSTAMO
- CRECY / CRECI
- CREDI PERÚ / CREDIT PERU / CREDITO PERU
- CUYCASH
- EKEKO
- HICASH / HI CASH
- HOLA CASH / HOLACASH
- HUAY MONEY / HUAYMONEY / FINANCIERA HUAY MONEY / FINANCIERA HUAYMONEY
- IKORI / KORI / KOIRI
- ISOLEZ
- KOLQUE / KOLKE
- MISOLES / MISOLES PERÚ
- PERÚ CRÉDITO
- PERÚ LOAN / PERÚLOAN / LOAN
- PRESTASOLE / PRESTASOLES / PRESTA SOL / PRESTA SOLES
- SOL CASH / SOLCASH
- VAMOCASH

- YEP CRÉDITO / YEPCRÉDITOS

Se recuerda que, conforme al Decreto Legislativo N° 1106 y la Resolución SBS N° 6338-2012 y sus modificatorias, las personas o empresas que pretendan realizar actividades de préstamo deben estar inscritas en el Registro de Empresas y Personas que efectúan Operaciones Financieras o de Cambio de Moneda, lo cual faculta a la SBS a supervisarlas en materia de prevención del lavado de activos y financiamiento del terrorismo.

Se invoca a la población a informarse adecuadamente y tomar las previsiones del caso, cuando deba decidir dónde requerir un servicio financiero de cualquier tipo.

Cualquier consulta o denuncia relacionada con personas o empresas que presten servicios financieros, sin autorización de la SBS o sin encontrarse registrados, puede ser presentada a esta entidad, a los teléfonos 0-800-10840 (línea gratuita a nivel nacional) o 01-200-1930, o al correo electrónico informalidad@sbs.gob.pe. También pueden visitar la página de la SBS: www.sbs.gob.pe/informalidad.

> Para acceder al artículo, ingresar aquí

2. UAF de Panamá, Perú y Ecuador firman acuerdo para combatir la corrupción

La Unidad de Análisis Financiero (UAF) de Panamá, la Unidad de Análisis Financiero y Económico del Ecuador (UAFE) y la Unidad de Inteligencia Financiera de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones del Perú (SBS), unen esfuerzos suscribiendo un acuerdo de cooperación para implementar herramientas eficientes en la lucha contra el blanqueo de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

A través de este acuerdo se pondrá en marcha un programa de pasantías para un personal seleccionado de cada Unidad de Inteligencia Financiera (UIF), el cual les permitirá visitar las instalaciones de las otras unidades,

a fin de conocer y promover el intercambio de mejores prácticas en materia de análisis estratégico dentro del ciclo de inteligencia financiera y consolidar los vínculos interinstitucionales de las UIF de la región.

Según Isabel Pérez Henríquez, Directora de la UAF de Panamá, el Programa de Pasantías, es un proyecto que impulsa el CIEP (Combatting Illicit Economies Programme) del gobierno del Reino Unido, como aporte al plan de trabajo del Grupo de Acción Financiera de Latinoamérica (GAFILAT) 2022 y que se extiende hasta el año 2025.

Además de la directora Isabel Pérez Henríquez, la firma del memorándum de entendimiento contó con la participación de Carla Mera Proaño, Directora General de la UAFE y Presidenta Pro-tempore de GAFILAT, Sergio Espinosa, Superintendente Adjunto por la SBS y representantes del CIEP del gobierno del Reino Unido.

> Para acceder al artículo, ingresar aquí

3. FINCEN advierte un aumento del ransomware

La UIF de Estados Unidos (FINCEN en inglés) lanzó la alerta a través de su informe de análisis de tendencias financieras.

El ransomware, también conocido como el secuestro de datos, es un tipo de programa informático dañino que restringe el acceso a determinadas partes o archivos de un sistema operativo infectado.

Una vez instalado en un equipo, los cibercriminales responsables de su diseño suelen pedir el pago de un rescate a cambio de quitar esta restricción.

Durante la presentación de la Ley de Secreto Bancario (BSA), el director de FINCEN, Himamauli Das, indicó que el ransomware continúa representando una amenaza significativa para los sectores de infraestructura crítica, empresas y el público.

El valor total de actividad sospechosa reportada relacionadas con ransomware durante los primeros seis meses de 2021 fue un total de $590 millones de dólares, que supera el valor reportado para todo el 2020 ($416 millones de dólares).

Principales hallazgos

Fueron varios los hallazgos revelados por FINCEN y que pueden dar luces acerca de la dimensión del fenómeno del ransomware:

- Los incidentes relacionados con ransomware informados han aumentado sustancialmente desde 2020.

- Las presentaciones de BSA relacionadas con ransomware en 2021 se acercaron a $ 1.2 mil millones de dólares.

- Aproximadamente el 75% de los incidentes relacionados con ransomware informados a FINCEN durante la segunda mitad de 2021 se referían a variantes de ransomware relacionadas con Rusia.

Desde FINCEN confirmaron que continúan recopilando información para mejorar la transparencia y combatir las constantes amenazas de los actores cibernéticos ilícitos.

Así mismo, desde la FINCEN insistieron en que las instituciones financieras desempeñan un papel fundamental para ayudar a proteger a los Estados Unidos de las amenazas relacionadas con el ransomware, "simplemente cumpliendo con las obligaciones de la BSA".

Finalmente, FINCEN invitó a los oficiales de cumplimiento a revisar el sitio Stop Ransomware de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) para obtener más información y recursos sobre ransomware.

> Para acceder al artículo, ingresar aquí

4. GAFI alerta que están usando su nombre con fines de fraude

El Grupo de Acción Financiera Internacional (GAFI) expuso las modalidades que estarían utilizando los delincuentes para cometer estafas.

Los oficiales de cumplimiento deberán estar atentos para evitar caer en una nueva modalidad de fraude que se aprovecha del GAFI.

Según una alerta emitida por el propio organismo internacional, hay delincuentes que solicitan a sus víctimas un pago por la supuesta verificación del GAFI del origen de fondos en transacciones internacionales.

Además, en los documentos usados en estas estafas aparecen membretes con el logotipo del GAFI y las supuestas firmas de sus altos funcionarios.

Incluso, en ocasiones los delincuentes suelen incluir direcciones de sitios web legítimos para dar una apariencia de credibilidad a la estafa.

En otros casos, asegura el GAFI, se han detectado estafadores que aparentemente usan tecnología para hacer que el correo electrónico del remitente o el identificador de llamadas parezcan idénticos al correo electrónico o número de teléfono oficial del GAFI.

Por todo lo anterior, el máximo organismo internacional de lucha contra el LA/FT aclara que no proporciona ninguno de los servicios que se describen en las comunicaciones fraudulentas.

Vale la pena recordar que el GAFI es una agencia intergubernamental que no tiene facultades para comunicarse con el público ni para autorizar o negar transacciones financieras específicas.

Tampoco puede solicitar el pago de tarifas por supuestos servicios ni tiene la capacidad de bloquear ninguna cuenta.

Finalmente, desde el GAFI solicitan a las personas que han recibido estas comunicaciones cortar el contacto con los estafadores y no desembolsar ninguna suma de dinero.

> Para acceder al artículo, ingresar aquí

Ir a portada

Boletín informativo

Año 2023
Edición N° 121

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú