ICD
Instituto Costarricense sobre Drogas

GOBIERNO DE COSTA RICA

UNIDAD DE INTELIGENCIA FINANCIERA

GUÍA DE IDENTIFICACIÓN DE RIESGOS / EBR

PARA USO DEL SECTOR DE PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES (PSAV)

(V-1-2024)
Setiembre 2024

EXTRACTO RESUMEN

De la Guía dirigida al sector de APNFD, para la construcción de una matriz de riesgos en prevención del lavado de activos y financiamiento al terrorismo (LA/FT) del GAFILAT

ELEMENTOS MÍNIMOS PARA CONSIDERAR AL MOMENTO DE REALIZAR UNA EVALUACIÓN DE RIESGOS EN LOS SECTORES DE PSAVs.

1. DEFINICIÓN DEL RIESGO

De acuerdo con la Guía del GAFI (2013, p.7) el riesgo es definido como "una función que se encuentra determinada por la interacción de tres variables: Amenaza, Vulnerabilidad y Consecuencia o Impacto".

Amenaza:
Es una persona, un grupo de personas, elementos o actividades que pueden afectar a un Estado, una sociedad o una economía. En el contexto del Lavado de Activos y el Financiamiento al Terrorismo (LA/FT), se incluyen a los criminales y sus organizaciones; grupos terroristas, sus integrantes, sus fondos y futuras actividades delictivas.

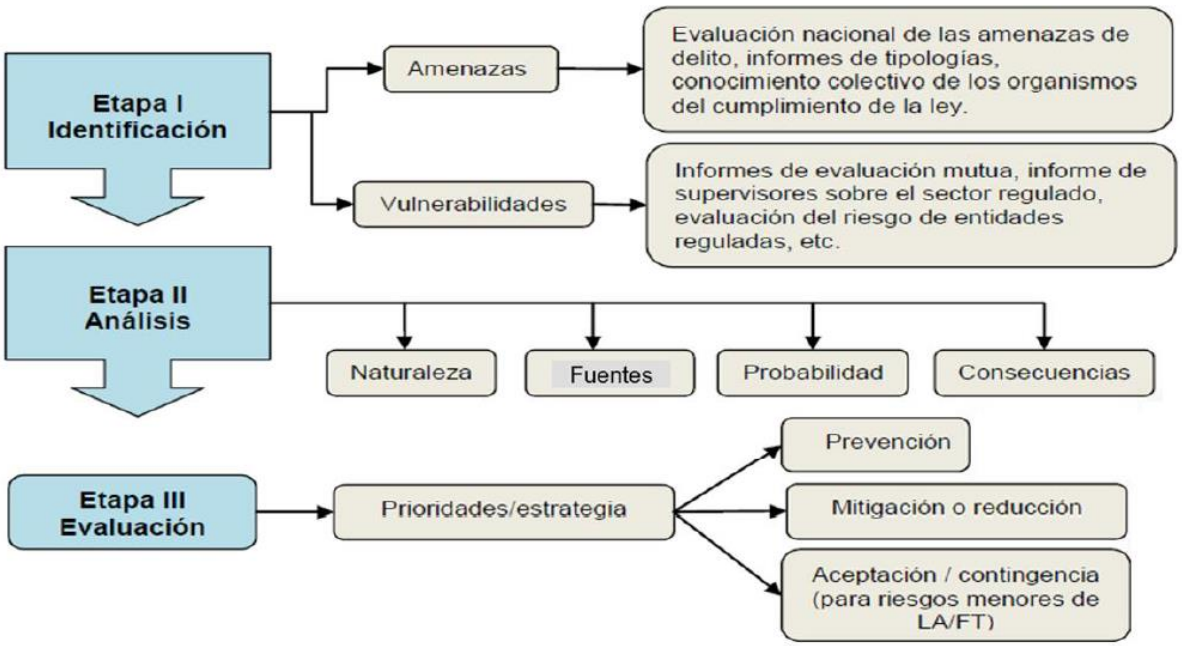
La evaluación de esta amenaza requiere del conocimiento del ambiente donde se desarrollan los delitos determinantes y cuáles serían los posibles ingresos generados por las actividades criminales.

Vulnerabilidades:
Comprende aquellas debilidades que pueden ser explotadas o aprovechadas por la amenaza o que pueden facilitar y/o permitir sus actividades. Se deben focalizar la atención en los factores que significan debilidades en el sistema Antilavado y contra el Financiamiento al Terrorismo (ALA/CFT) y en los controles estatales. Su valoración debe considerar las características específicas de su sector, productos y servicios que lo hagan atractivos a los fines de LA/FT.

Consecuencias:
Refiere al impacto o daño que el LA o el FT puede causar, esto incluye los efectos de la actividad criminal y terrorista en el sector así como en la economía y en toda la sociedad. Las consecuencias pueden ser a corto y a largo plazo y relacionarse con determinados intereses nacionales y regionales, reputación internacional, afectación a los sectores de negocios, comunidades, etc.

2. ETAPAS DEL PROCESO DE EVALUACIÓN DE RIESGOS DE ACUERDO CON EL GAFI

Se describen las etapas para el proceso de la evaluación de riesgos LA/FT.



3. OBJETIVO DE LA GESTIÓN DE RIESGOS

Al implementar la gestión de riesgos deben evitar ser utilizadas por los delincuentes para actividades ilícitas. Por esta razón, los objetivos deben estar acordes a establecer sus propias declaraciones de compromiso y prevención. Por esta razón, se debe cumplir con las disposiciones preventivas establecidas en la regulación nacional (Ley 7786 y sus reformas).

4. VALORACIÓN DEL RIESGO

Se deben considerar escalas de valoración del riesgo LA/FT, que definan un valor a cada uno de los componentes que forman parte de los factores de riesgo. Estos criterios de valoración del riesgo deben estar relacionados con la severidad del riesgo y el indicador de la severidad del evento de riesgo de LA/FT determina su nivel de prioridad para su tratamiento.

5. RELACIÓN ENTRE LOS CRITERIOS DE VALORACIÓN Y SEVERIDAD

Criterio de Valoración del Riesgo de LA/FT	Severidad del Riesgo de LA/FT
Bajo (1)	Aceptable
Medio (2)	Significativo [5]
Alto (3)	Moderado
Extremo (4)	Catastrófico

Referencia / fuente: elaboración propia sobre la base de lo planteado por Sintura, Francisco; Martínez Wilson; Quintana, 2014, página 329. De la Guía dirigida al sector de APNFD, para la construcción de una matriz de riesgos en prevención del lavado de activos y financiamiento al terrorismo (LA/FT) del GAFILAT

6. FACTORES DE RIESGO

Clientes/Usuarios: En su actividad profesional, debe gestionar los riesgos asociados con sus clientes "por su comportamiento, antecedentes, y actividad al inicio y durante toda la relación" (UAFE Ecuador, 2022).

Productos/Servicios: debe evaluar los riesgos de LA/FT en los productos y/o servicios que ofrecen, especialmente en relación con la vulnerabilidad que estos puedan presentar para el LA/FT.

Jurisdicción: Las áreas geográficas o jurisdicciones son las regiones o países en la que opera u operan sus clientes/usuarios se encuentran, es decir, donde ofrece sus servicios o tendrá sus efectos6.

Canales: Son todos los medios físicos y virtuales a través de los cuales ofrece sus productos o servicios.

7. ESTABLECER LOS EVENTOS DE RIESGO Y POSIBLES CAUSAS

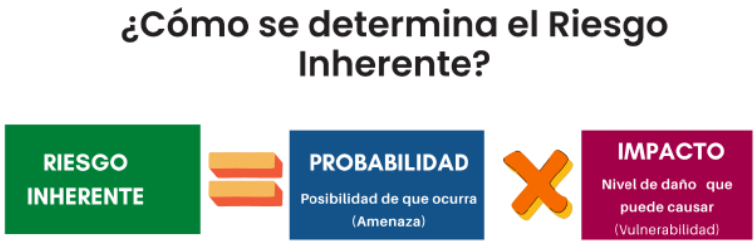
Es importante determinar los eventos de riesgo en torno a cada criterio definido para cada factor de riesgos.

Determinar **¿qué podría ocurrir?**: elaborar una lista de los posibles eventos de riesgo como posibles incidentes. Estos eventos de riesgo se deben realizar para cada uno de los factores de riesgo de LA/FT que se hayan definido.

Causas:
Para cada riesgo es necesario establecer las posibles causas porque permite identificar las situaciones que podrían favorecer la materialización de cada evento de riesgo.

8. MEDIR EL RIESGO

Esto corresponde a la determinación del riesgo inherente y se logra mediante la obtención de valoraciones de probabilidad de ocurrencia del evento de riesgo.



9. CLASIFICACIÓN NUMÉRICA DE LA PROBABILIDAD DE OCURRENCIA

Tabla: medición de la probabilidad de un evento de riesgo

Probabilidad de ocurrencia de un evento de riesgo				
Improbable	Raro	Posible	Probable	Casi Seguro
1	2	3	4	5

Ref: Sintura, Martínez y Quintana (2014, p.324)

10. IMPACTO

Escala de medición del impacto de un evento de riesgo de LA/FT

Insignificante: Sin perjuicios, baja pérdida financiera o daño reputacional. Puede incluir la amonestación escrita del supervisor de LA/FT de la APNFD (Riesgo Legal).

Leve: Puede ser susceptible de sanción moderada de índole económico. Genera pérdida de ingresos o incremento de gastos por pérdida de reputación. Puede implicar el involucramiento de clientes en actividades de LA/FT. Publicidad Negativa (Riesgo Reputacional) Sanciones administrativas y/o multas moderadas (Riesgo Legal).

Moderado: Pérdida o daño moderado. Susceptible de una amonestación de índole • Sanciones administrativas y/o multas (Riesgo económico. Puede haber disminución de ingresos por desprestigio, mala imagen o publicidad negativa. El riesgo de contagio está presente. Legal) Clientes se retiran por el desprestigio de la APNFD (Riesgo Operacional) Publicidad Negativa (Riesgo Reputacional).

Crítico: Pérdida o daño crítico. Susceptible de una amonestación de índole económica a la mayor cuantía posible. Pérdida de clientes, disminución de los ingresos por mala imagen o publicidad. Sanciones penales, administrativas y/o multas de la mayor cuantía posible. (Riesgo Legal) Desprestigio de la APNFD que afecta directamente los ingresos (Riesgo Reputacional) No se logran los objetivos de la APNFD en la participación en el mercado. (Riesgo Operacional).

Catastrófico: Pérdida o daño catastrófico, susceptible de cuantiosas amonestaciones económicas y estrictas sanciones de suspensión o inhabilitación permanente (incluyendo sanciones de carácter penal). Multas cuantiosas impuestas por el supervisor de la APNFD (Riesgo Legal) Indemnización por daños (Riesgo Legal) Retiro de licencia de operaciones de la APNFD (Riesgo Legal) Bloqueo financiero (Riesgo Reputacional)

11. DETERMINAR LA SEVERIDAD DE CADA RIESGO

Esto se obtiene multiplicando la calificación del nivel de probabilidad por la calificación dada al nivel de impacto respectivo. De esta forma y para este caso, se obtienen múltiplos que van desde 1 hasta 25, donde 1 es el más bajo nivel de severidad y, por tanto, de menor prioridad, mientras que 25 es el máximo valor.

Mapa con nivel de severidad del riesgo

IMPACTO							
	Catastrófico	5	Aceptable 5	Moderado 10	Crítico 15	Catastrófico 20	Catastrófico 25
	Crítico	4	Aceptable 4	Significativo 8	Moderado 12	Crítico 16	Catastrófico 20
	Moderado	3	Aceptable 3	Significativo 6	Significativo 9	Moderado 12	Crítico 15
	Leve	2	Aceptable 2	Aceptable 4	Significativo 6	Significativo 8	Moderado 10
	Insignificante	1	Aceptable 1	Aceptable 2	Aceptable 3	Aceptable 4	Aceptable 5
			1	2	3	4	5
			Improbable	Raro	Posible	Probable	Casi Seguro
			PROBABILIDAD				

Escala de severidad del Riesgo

Rango del valor de la severidad (probabilidad x impacto)	Calificación de la severidad del evento de riesgo	Escala
1-5	Aceptable	1
6-9	Significativo	2
10-12	Moderado	3
13-16	Crítico	4
17-25	Catastrófico	5

PLANTEAMIENTO BASE DE RIESGOS DE LA/FT EN EL SECTOR DE LOS PSAVs

Esta no es una lista exhaustiva de riesgos, por lo tanto, cada sujeto obligado debe identificar sus propios riesgos derivados del conocimiento del sector en que se desenvuelve, evaluarlos y establecer las propuestas de mitigación. Tome en consideración que adicionalmente, el incumplimiento de obligaciones ALA/CFT relacionadas con la implementación de controles, el reporte de operaciones sospechosas, el mantenimiento de registros, controles sobre PEPS, entre otras establecidas en la Ley 7786 constituye riesgos legales, reputacionales e incluso de posibles sanciones administrativas y penales.

Contexto

Los activos virtuales (AV) y los proveedores de servicios de activos virtuales (PSAV) se integran rápidamente en el sistema financiero mundial, es así como su posible uso indebido con fines delictivos y de financiación del terrorismo plantean un desafío importante y en evolución.

La materialización de casos específicos, perfiles y tipologías empleadas por entidades terroristas y otras actividades criminales para explotar los AV y los PSAV, dan cuenta que no hay un estado de inmunidad frente a esta amenaza.

Oportunidades de respuesta

- **Mejora regulatoria:** Es necesaria la implementación de mejora de los marcos jurídicos y reglamentarios alineando las leyes, regulaciones y prácticas con los estándares internacionales del GAFI.

- **Cooperación:** Las buenas prácticas apuntan a fomentar el fortalecimiento de la cooperación entre países de la región con el intercambio de casos exitosos e iniciativas que permitan mejorar las capacidades para responder a las amenazas con el uso indebido de los AV y PSAV.

- **Fomento de las asociaciones público-privadas:** las cuales desempeñan un papel crucial en la lucha contra la delincuencia organizada y el lavado de activos a través de los AV. En este sentido resulta relevante el diálogo y la colaboración permanente entre las agencias gubernamentales y el sector de los PSAV.

1. Riesgo: Anonimato

Descripción: Los activos virtuales pueden ser transferidos de manera anónima, lo que dificulta la identificación del origen y destino de los fondos. La naturaleza anónima y sin fronteras de las transacciones de los AV complica la capacidad de los Estados para identificar, rastrear e interceptar transacciones ilícitas utilizando VA/VASP

Acciones de mitigación:

a) Implementar medidas robustas de conocimiento del cliente (KYC) y debida diligencia (CDD) para verificar la identidad de los usuarios.
b) Limitar las transacciones anónimas o seudónimas y exigir verificaciones adicionales en estas situaciones.
c) Utilizar tecnología de análisis de blockchain para rastrear posibles transacciones sospechosas.
d) Reportar operaciones sospechosas a la UIF.

2. Riesgo: Transacciones Transfronterizas

Descripción: Las transacciones con activos virtuales suelen cruzar fronteras rápidamente en ambiente virtual, complicando la supervisión y rastreo por las autoridades.

Acciones de mitigación:

a) Establecer procedimientos para monitorear transacciones internacionales y reportar aquellas que sean sospechosas.
b) Cooperar con UIFs internacionales para compartir información sobre transacciones transfronterizas.
c) Implementar límites y alertas en las transacciones de alto valor o volumen significativo.
d) Aplicar medidas de DDC y evitar realizar operaciones desde o hacia jurisdicciones catalogadas de riesgo o donde no exista regulación ALA/CFT.

3. Riesgo: Uso de Plataformas Descentralizadas

Descripción: Las plataformas descentralizadas permiten transacciones directas entre pares, eludiendo intermediarios tradicionales y la supervisión regulatoria.

Acciones de mitigación:

a) Requerir a los PSAVs que implementen procedimientos para identificar y reportar transacciones realizadas en plataformas descentralizadas.
b) Establecer mecanismos para la identificación y bloqueo de fondos relacionados con actividades ilícitas.
c) Mantener una lista de entidades de alto riesgo relacionadas con plataformas descentralizadas.
d) Implementar la realización de reportar operaciones sospechosas.

4. Riesgo: Insuficiente Supervisión Regulatoria

Descripción: La regulación de los PSAVs puede ser inconsistente o débil en algunas jurisdicciones, lo que facilita el abuso del sistema.

Acciones de mitigación:

a) Promover la armonización regulatoria a nivel internacional para asegurar un marco regulatorio consistente y robusto.
b) Realizar evaluaciones regulares de los riesgos y cumplimiento de los PSAVs.
c) Fortalecer la cooperación y el intercambio de información entre reguladores internacionales.
d) Conocer aquellas jurisdicciones que no tienen ningún tipo de regulación.

5. Riesgo: Uso de Mixers y Tumblers

Descripción: Estas herramientas se utilizan para ofuscar la trazabilidad de los activos virtuales, dificultando la identificación de su origen. Son herramientas que buscan mejorar la privacidad de las transacciones mezclando transacciones de Bitcoin.

Acciones de mitigación:

a) Prohibir el uso de servicios de mezclado en las transacciones realizadas por PSAVs.
b) Implementar soluciones tecnológicas que puedan detectar y bloquear el uso de mixers o tumblers.
c) Monitorear y reportar transacciones que utilicen estas herramientas.
d) Reportar operaciones sospechosas a la UIF en situaciones de alto riesgo.

6. Riesgo: Participación de Entidades No Regulatorias

Descripción: Algunos PSAVs pueden operar sin estar sujetos a regulación o supervisión adecuada dentro del país, facilitando el lavado de dinero y el financiamiento del terrorismo.

Acciones de mitigación:

a) Requerir el registro o la licencia obligatoria de todos los PSAVs en las jurisdicciones donde operan y también a nivel local.
b) Implementar sanciones para aquellos PSAVs que operen sin las licencias o registros adecuados.
c) Promover la educación y concienciación en el sector sobre la importancia del cumplimiento regulatorio.

7. Riesgo: Uso de Activos Virtuales en la Dark Web

Descripción: Los activos virtuales son comúnmente utilizados para transacciones ilícitas en la Dark Web.

Acciones de mitigación:

a) Monitorear y analizar las transacciones que podrían estar relacionadas con actividades de la Dark Web.
b) Colaborar con agencias de investigación (MP/OIJ) y seguridad cibernética (MICIT y otras) para identificar y desmantelar actividades ilícitas en la Dark Web.
c) Implementar medidas tecnológicas que detecten patrones asociados con el uso de la Dark Web.

8. Riesgo: Ataques Cibernéticos

Descripción: Los PSAVs pueden ser vulnerables a ataques cibernéticos que comprometan la seguridad de los fondos y la información de los clientes.

Acciones de mitigación:

a) Implementar protocolos de ciberseguridad avanzados, incluyendo cifrado y autenticación de múltiples factores.
b) Realizar auditorías de seguridad regulares y pruebas de penetración.
c) Establecer un plan de respuesta a incidentes para mitigar rápidamente los efectos de un ataque.

9. Riesgo de ser un facilitador

Descripción: Un PSAV pueda ser puente para el pago de una extorción, secuestro u otro delito.

Acciones de mitigación:

a) Monitorear y analizar las transacciones que podrían estar relacionadas con actividades delictivas basadas en umbrales u otros parámetros referentes.
b) Colaborar con agencias de investigación.
c) Implementar medidas tecnológicas que detecten patrones asociados con delitos.

10. Riesgo: Omisión del Reporte de Operaciones Sospechosas

Descripción: El reportar operaciones sospechosas es una obligación por lo tanto, debe estar realizar el registro formal en la plataforma para disponer de la herramienta de comunicación segura y confidencial de las sospechas.

Mitigador: Registrarse en la plataforma gratuita (UIF Reportes) de la Unidad de Inteligencia Financiera en el siguiente enlace: https://apps.icd.go.cr/uifreportes/Autenticacion.aspx
Participar en eventos de capacitación y acercamiento. Informarse sobre la importancia y obligaciones relativas al reporte de operaciones sospechosas. Hacer curso de capacitación suministrado por la UIF para los sujetos obligados.

RESUMEN DE OBLIGACIONES DE ACUERDO CON EL GAFI

Los PSAV deben:

- Implementar las mismas medidas preventivas que las instituciones financieras, incluida la debida diligencia del cliente, el mantenimiento de registros y reporte de operaciones sospechosas.

- Obtener, mantener y transmitir de forma segura la información del originador y del beneficiario al realizar transferencias.

- Deben estar debidamente registrados o licenciados en una instancia de supervisión.

- Deben cumplir con los requisitos establecidos en las Recomendaciones 10 a 21 del GAFI

- Recomendación 10 – El umbral designado para transacciones ocasionales por encima del cual los VASP deben llevar a cabo DDC es de USD/EUR 1 000.

- Recomendación 16 – Para las transferencias de activos virtuales, los países deben asegurarse de que:
    - (i) los PSAV de origen obtengan y mantengan la información del originador y la información requerida del beneficiario.
    - (ii) los PSAV beneficiarios obtengan y mantengan la información requerida del originador y la información requerida y precisa de los beneficiarios;
    - (iii) otros requisitos de la R.16
    - (iv) las mismas obligaciones se aplican a las instituciones financieras al enviar o recibir transferencias de activos virtuales en nombre de un cliente.