asociación
de agregadores
de medios
de pago a.c.

GUÍA DE MEJORES PRÁCTICAS

AGREGADORES DE MEDIOS DE PAGO

PREVENCIÓN DE LAVADO DE DINERO Y FINANCIAMIENTO AL TERRORISMO

ÍNDICE

PRÓLOGO

El ecosistema de pagos en México atraviesa una etapa de transformación profunda, marcada por una rápida digitalización, una expansión acelerada del modelo de agregadores y un entorno internacional donde la integridad financiera ha adquirido un nivel de escrutinio sin precedentes. En los últimos años, los agregadores se han consolidado como actores esenciales para la inclusión financiera, facilitando millones de transacciones diarias y habilitando que comercios de todos los tamaños se integren a la economía digital. Sin embargo, esta centralidad también los ha expuesto a riesgos operativos, reputacionales y regulatorios cada vez más complejos.

El contexto internacional reciente ha elevado significativamente los estándares de cumplimiento para todas las empresas que participan en la cadena de pagos. En 2025, el Departamento de Estado de Estados Unidos designó a seis grupos de narcotraficantes mexicanos como organizaciones terroristas trasnacionales[1]. Como consecuencia de esta medida, el gobierno de Estados Unidos a través de la Red de Control de Delitos Financieros (FinCEN) emitió acciones sin precedentes contra instituciones financieras mexicanas y, posteriormente, contra establecimientos de sectores no financieros como casinos, identificándolos como vehículos para facilitar flujos vinculados al crimen organizado. Estas medidas, sustentadas en facultades extraterritoriales y fundamentadas en información no pública, evidenciaron la disposición de las autoridades internacionales para imponer restricciones severas cuando consideran que existen riesgos sustanciales de lavado de dinero o financiamiento al terrorismo.

Dichos eventos confirmaron que los riesgos para agregadores no se limitan al ámbito operativo, sino que pueden escalar a sanciones que afecten la continuidad del negocio, la relación con adquirentes, las corresponsalías internacionales y la reputación del sector. Para los participantes del sistema financiero mexicano —incluyendo bancos, agregadores, fintechs y otros— esto implica la necesidad de reforzar controles de listas negras, monitoreo transaccional, trazabilidad y debida diligencia ampliada.

Frente a este panorama, la ASAMEP que agrupa a más de 30 agregadores responsables de más del 90% de las transacciones procesadas bajo este modelo ha adoptado una estrategia gremial basada en la autorregulación, la colaboración institucional y la convergencia con estándares internacionales (UIF, GAFI, OFAC, CNBV, SAT, SHCP, Banxico, y lineamientos de marcas). Esta Guía de Mejores Prácticas busca ser un pilar central de dicha estrategia.

El propósito de este documento es ofrecer un marco de referencia común que permita elevar el estándar colectivo del sector, fortaleciendo la capacidad de los agregadores para prevenir el lavado de dinero y el financiamiento al terrorismo mediante prácticas consistentes, actualizadas y alineadas con la evolución del riesgo global. Esta guía no sustituye obligaciones normativas, ni pretende imponer requisitos operativos específicos; sino que busca fomentar una cultura de cumplimiento proactivo que privilegie la transparencia, la corresponsabilidad y la integridad como bases para un ecosistema de pagos seguro y sostenible.

La adopción de mejores prácticas gremiales es un elemento clave para enfrentar los riesgos emergentes, mitigar vulnerabilidades y enviar un mensaje claro a clientes o comercios y autoridades nacionales e internacionales: los agregadores en México están comprometidos con operar bajo estándares globales de seguridad, reducir el riesgo sistémico y blindar al sector frente a amenazas que pueden comprometer la estabilidad financiera, la confianza del público y la viabilidad de la innovación en pagos.

A través de esta guía, los agregadores representados en ASAMEP reafirman su liderazgo como un gremio que entiende que la prevención no es solo una obligación moral y operativa, sino una condición indispensable para sostener la expansión del ecosistema, garantizar relaciones confiables con adquirentes y marcas, proteger a los comercios y usuarios, y asegurar que México continúe avanzando hacia una economía digital segura e incluyente.

MYRIAM COSÍO ROBLES
PRESIDENTE
ASOCIACIÓN DE AGREGADORES DE MEDIOS DE PAGO

CARLOS ROJERO CASILLAS
DIRECTOR GENERAL
ASOCIACIÓN DE AGREGADORES DE MEDIOS DE PAGO

1.- Departamento de Estado de los EE. UU. (2021, Diciembre) Designación de cárteles internacionales. U.S. Department of State. https://www.state.gov/translations/spanish/designacion-de-carteles- internacionales

AGRADECIMIENTOS

ASAMEP agradece la participación de sus agremiados, autoridades, especialistas y aliados estratégicos que colaboraron en la elaboración de este documento. Su compromiso y visión compartida hicieron posible consolidar una guía que refleja la madurez y responsabilidad del gremio frente a los retos del ecosistema de pagos.

Expresamos un reconocimiento especial por el apoyo brindado por la Comisión Nacional Bancaria y de Valores (CNBV) y del Banco de México (Banxico) que, mediante sus ponencias nos ayudaron a definir las mejores prácticas para la presente guía, e inspiraron a la ASAMEP en el fortalecimiento e integridad en beneficio del ecosistema de pagos en México.

Agradecemos también al despacho Y&G Consultores S.C. (YG), por su acompañamiento técnico y su aportación en el desarrollo de los contenidos de esta guía. Su experiencia en materia de cumplimiento, regulación financiera y prevención de operaciones ilícitas fue clave para garantizar el rigor y la claridad del presente trabajo.

Esta Guía es el resultado del trabajo conjunto entre nuestros agremiados, las autoridades y los especialistas, reafirmando nuestra convicción de que la prevención es una tarea compartida que fortalece la confianza y la transparencia en toda la industria de pagos.

INTRODUCCIÓN

El fortalecimiento del ecosistema de pagos en México requiere que los agregadores adopten estándares de prevención acordes con los riesgos crecientes del entorno económico, tecnológico, geopolítico y normativo. En un contexto marcado por la expansión acelerada de los modelos digitales, un escrutinio internacional cada vez más riguroso y la intervención activa de autoridades nacionales y extranjeras, la integridad financiera se ha convertido en un prerrequisito indispensable para garantizar la continuidad operativa, la confianza de los adquirentes y la estabilidad de la red de pagos en su conjunto.

Bajo esta premisa, ASAMEP determinó la necesidad de construir un documento gremial que ofreciera un marco metodológico común, basado en estándares globales y en riesgos reales observados en el mercado mexicano. Esta guía se diseñó como un instrumento educativo y práctico, orientado tanto a reforzar la cultura de cumplimiento como a habilitar decisiones operativas más informadas.

En este sentido, los objetivos centrales de este documento son:

- Fomentar una visión compartida de cumplimiento, donde todos los agregadores adopten prácticas alineadas con los más altos estándares nacionales e internacionales.
- Mitigar los riesgos de uso indebido de los servicios, mediante la implementación de controles que eviten relaciones comerciales con actores de riesgo y favorezcan la detección temprana de operaciones inusuales.
- Fortalecer la toma de decisiones basadas en datos, promoviendo el uso de información completa, actualizada y relevante sobre los clientes o comercios, derivada del monitoreo continuo de transacciones y del conocimiento integral del ecosistema.
- Impulsar la madurez del sector, incentivando que los agregadores integren la gestión de riesgos como un componente estratégico de su modelo de negocio, contribuyendo así a la sostenibilidad y competitividad de la industria.
- Consolidar al gremio como un aliado estratégico de las autoridades, de los clientes o comercios y la sociedad, comprometido con el desarrollo responsable, transparente y seguro del ecosistema de pagos en México.

En conjunto, estos objetivos se ven plasmados en la Guía que busca funcionar como un instrumento académico, gremial y operativo que eleve el estándar colectivo, fortalezca la resiliencia del ecosistema de pagos y refuerce la posición de ASAMEP como un actor responsable y estratégico en el cumplimiento y la integridad financiera del país.

Al elevar la atención en las prácticas de PLD/FT entre los agregadores, se reduce la probabilidad de que los clientes o comercios de alto riesgo utilicen estas plataformas como vehículos para operaciones ilícitas, protegiendo así la integridad de la red de pagos y garantizando que la innovación tecnológica se desarrolle en un entorno seguro, confiable y sostenible.

La estructura del documento responde a un enfoque integral: inicia con el proceso de identificar a los clientes o comercios (KYC) como insumo primario, continúa con la verificación en listas negras como filtro esencial, incorpora la metodología de enfoque basado en riesgo, detalla los criterios para crear perfiles transaccionales y ejecutar monitoreo transaccional, promueve la capacitación continua y culmina con tipologías basadas en casos reales para cerrar el ciclo de prevención.

La implementación de los principios delimitados en esta guía ayudará a fortalecer los procesos internos de PLD/FT de los agregadores, mitigando significativamente el riesgo de ser utilizados por el crimen organizado y evitando incurrir en graves sanciones y daños reputacionales, asegurando así un desarrollo seguro y sostenible de la red de medios de disposición.

LAVADO DE DINERO Y FINANCIAMIENTO AL TERRORISMO

Iniciemos por definir el lavado de dinero como el proceso por virtud del cual, los bienes de origen ilícito se integran al sistema financiero con la apariencia de haber sido obtenidos de forma legal. Este fenómeno no ocurre en un solo acto, sino que opera a través de un ciclo diseñado para borrar el rastro delictivo[2].

Dicho ciclo comienza con la Colocación, fase en la que el lavador introduce los fondos ilegales en el sistema financiero. Le sigue la Estratificación, que consiste en separar esos fondos de su fuente original mediante capas complejas de transacciones cuyo fin es desdibujar el rastro y disimular su origen. Finalmente, el proceso culmina con la Integración, etapa donde el capital reingresa a la economía formal mediante transacciones comerciales o personales que aparentan ser normales, otorgando a la riqueza ilícita una apariencia de legitimidad difícil de distinguir[3].

Asimismo, definimos el financiamiento al terrorismo como la aportación, financiación o recaudación de recursos o fondos económicos que tengan como fin provocar alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad para que tome una determinación.

Las mejores prácticas presentadas en esta Guía buscan ofrecer a los agregadores un marco operativo claro, consistente y alineado con los estándares nacionales e internacionales para la prevención de ambos fenómenos.

2.- Comisión Nacional Bancaria y de Valores (2019, Junio) Conocimientos básicos en PLD/FT. [Diapositiva de PowerPoint 3]. Comisión Nacional Bancaria y de Valores. https://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/1-1_Conceptos_basicos.pdf
3.- Idem. [Diapositivas de PowerPoint 3, 13, 15, 16 y 17]
4.- Idem

MARCO NORMATIVO

El ecosistema de pagos opera en un entorno cada vez más interconectado, donde la confianza y la transparencia son fundamentales. Aunque los agregadores de pago no están sujetos al mismo marco regulatorio que las instituciones financieras tradicionales, su papel dentro del sistema los convierte en actores estratégicos para la PLD/FT.

Esta guía se basa en los principios y estándares nacionales e internacionales que han demostrado ser efectivos para fortalecer la integridad financiera. Entre los más relevantes destacan:

- **Recomendaciones emitidas por el Grupo de Acción Financiera Internacional (GAFI):** organismo del cual México es parte, que establece las 40 Recomendaciones globales sobre PLD/FT, adoptadas por la mayoría de los países del mundo[5].

- **Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI)[6], Reglamento de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (Reglamento)[7] y Reglas de Carácter General a que se refiere la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (Reglas)[8]:** marco legal mexicano de PLD/FT que sienta las bases de prevención fuera del sistema financiero y que sirven como modelo de buenas prácticas para el sector de agregadores.

- **Disposiciones de la Secretaría de Hacienda y Crédito Público (SHCP) y la CNBV**: referentes nacionales que definen las obligaciones formales para las entidades financieras[9].

- **Tipologías y Guías de Referencia:** Análisis de casos reales publicados por autoridades nacionales e internacionales que describen los modus operandi delictivos. Para los ejemplos prácticos de esta guía, se han seleccionado directamente las tipologías emitidas por:

- **Unidad de Inteligencia Financiera (UIF) y SAT:** Fuentes nacionales base para identificar esquemas como “Personas Políticamente Expuestas (PEP)”, “El Licenciado”, “Testaferros”, “Empresas Fantasma versión PEMEX” y “Uso de Identidad”.

- **FinCEN (Tesoro de EE.UU.):** Referencias técnicas clave para esquemas operativos específicos como la “Estructuración” (Pitufeo).

- **GAFI (FATF)**: Referente global para los indicadores de riesgo en el uso de profesionistas y estructuras corporativas.

- Adicionalmente, el marco de prevención de esta guía se nutre de los criterios generales y estudios de organismos como la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y el Grupo Egmont, cuyas directrices sobre delincuencia organizada y cooperación financiera fortalecen la visión global del sector.

- Listas y estándares internacionales, como las emitidas por la Oficina de Control de Activos Extranjeros (OFAC), la ONU y la OCDE, que promueven la transparencia y la integridad en los flujos financieros globales.

La ASAMEP promueve la adopción de estos lineamientos como parte de un compromiso voluntario del gremio. Las recomendaciones enunciadas a continuación se basan en estas fuentes para guiar a los agregadores en la implementación de sus lineamientos de PLD/FT. El objetivo es elevar el nivel de profesionalismo y confianza del sector, alineándose con las mejores prácticas internacionales.

5.- Grupo de Acción Financiera Internacional (GAFI). (2012) Estándares Internacionales Sobre la Lucha Contra el Lavado de Activos y el Financiamiento del Terrorismo y la Proliferación. Comisión Nacional Bancaria y de Valores. https://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/RecomiendacionesGAFI2012.pdf
6.- Cámara de Diputados. (2025, Julio) Ley Federal para la Prevención e Identificación de Operaciones de Recursos de Procedencia Ilícita. Cámara de Diputados. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI.pdf
7.- Cámara de Diputados. (2013) Reglamento de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita. Cámara de Diputados. https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPIORPI.pdf
8.- Cámara de Diputados. (2014, Julio) Acuerdo 02/2013 por el que se emiten las Reglas de Carácter General a que se refiere la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita. Secretaria de Hacienda y Crédito Público. https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/compilado_rcg_reforma2014.pdf
9.- Unidad de Inteligencia Financiera. (2024, Agosto) Disposiciones de Carácter General en materia de prevención, operaciones posiblemente vinculadas con los delitos de Operaciones con Recursos de Procedencia Ilícita, de financiamiento al terrorismo. Gobierno de México. https://www.gob.mx/uif/documentos/uif-marco-juridico-disposiciones-de-caracter-general-337829

IDENTIFICACIÓN DE CLIENTES O COMERCIOS (KYC): LA BASE DE LA PREVENCIÓN

A diferencia de las instituciones financieras, los agregadores no cuentan con un marco normativo de obligaciones específicas en materia de PLD/FT. Sin embargo, su posición estratégica en la red de medios de disposición, como intermediarios entre clientes o comercios, adquirentes, emisores de tarjetas y titulares de marca, implica una responsabilidad operativa de facto. Contar con procesos de debida diligencia siguiendo los estándares nacionales e internacionales, no solo protege al agregador, sino que mitiga riesgos para los participantes del ecosistema de pagos en su conjunto.

Implementar un proceso robusto de KYC permite conocer la naturaleza, el origen y la legitimidad de los clientes o comercios, reduciendo significativamente el riesgo de que los agregadores sean utilizados para fines ilícitos.

El principio de “Conoce a tu Cliente” (KYC, por sus siglas en inglés) es la parte más importante de cualquier estrategia de prevención. **Identificar a los clientes o comercios con quienes se realizan actividades comerciales, recabar su información y documentación** ya sea digital o física y verificar su identidad basada en la documentación oficial, es conocer quién está detrás de cada cliente o comercio, operación o flujo transaccional.

En un entorno donde la afiliación es rápida y digital, aplicar un proceso de identificación adecuado marca la diferencia entre operar con confianza o exponerse a riesgos reputacionales y legales.

En este contexto, un KYC efectivo no consiste únicamente en recabar documentos, sino verificarlos a fin de generar un entendimiento integral del cliente o comercio, su actividad económica y la coherencia entre lo que declara como giro del cliente o comercio y lo que realmente transacciona.

Por lo anterior, el agregador no debería establecer relaciones comerciales o celebrar contratos con personas anónimas, bajo nombres ficticios, seudónimos o en las que no sea posible identificar plenamente a la persona física o moral que actúa como cliente o comercio.

Para los agregadores, un enfoque sólido de KYC implica:

Verificar la identidad de sus clientes o comercios a fin de **conocer a la persona o personas** a las que se le ofrecen servicios y si es que conlleva algún riesgo.

Promover relaciones comerciales **transparentes y responsables,** fundadas en la confianza mutua y la validación oportuna de información.

Construir y mantener una base de información precisa y confiable, **que sirva de soporte** para los procesos de monitoreo y evaluación continua de riesgos.

La identificación del cliente o comercio se inicia con el proceso de alta, pero es un proceso continuo. Las mejores prácticas exigen la actualización anual de los expedientes de clientes o comercios. Esta tarea es esencial a lo largo de toda la relación comercial. La revisión periódica de la información, la validación de documentos y la actualización de datos relevantes son acciones clave que fortalecen la seguridad del ecosistema y permiten la detección oportuna de cualquier desviación o irregularidad.

También el agregador puede implementar mecanismos de actualización de algunos expedientes en específico antes del plazo anual si existen cambios relevantes del cliente o comercio, por ejemplo: cuando se detecte variación sustancial en la transaccionalidad, cambio de accionistas por adquisición o compra (cuando sea del dominio público) o cambio del giro del comercio.

Dado que los agregadores se encargan de traer nuevos comercios a la red de medios de disposición, contar con una identificación sólida es fundamental. Esto asegura que los flujos transaccionales y los procesos de liquidación que circulan por la infraestructura —en la que participan adquirentes, cámaras de compensación, emisores, titulares de marca y empresas especializadas— se gestionen con clientes debidamente verificados, reduciendo riesgos y preservando la integridad del ecosistema.

10.- Cámara de Diputados. (2014, Julio) Acuerdo 02/2013 por el que se emiten las Reglas de Carácter General a que se refiere la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita. Página 9. Cámara de Diputados. https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/compilado_rcg_reforma2014.pdf

EXPEDIENTES Y VERIFICACIÓN

Para cada cliente o comercio al que se le provea servicios, se tiene que llevar a cabo la creación de expedientes consistentes y verificados. Para formar un expediente efectivo es necesario ejecutar 4 acciones:

Recabar documentación e información

Validar o verificar la documentación

Actualizar la documentación e información

Conservar la documentación e información

El proceso de verificación de la documentación, se refiere a tener la certeza de que la información proporcionada es verídica, vigente y auténtica. La incorporación de una identificación en el expediente carece de valor si el documento es apócrifo o si la entidad declarada no existe jurídicamente. Por ello, los agregadores deben establecer mecanismos, ya sea mediante equipos internos especializados o a través de alianzas con proveedores tecnológicos, para verificar la autenticidad de los datos contra fuentes oficiales (como el SAT, RENAPO, INE, etc.).

Para ello, los agregadores deben asegurarse de que el mecanismo elegido —interno o externo— cumpla al menos con los siguientes principios operativos:

- **Conectividad directa con el INE (no tercerizada):** evitando procesos manuales o intermediados que incrementen riesgo.
- **Tiempo de Respuesta:** las consultas deben resolverse en milisegundos para no afectar la experiencia del cliente o comercio durante el proceso de alta.
- **Manejo de Datos Personales:** Debe cumplir con la normativa de protección de datos aplicable en México, garantizando que el tratamiento de los datos consultados o almacenados se haga de forma legal y segura.
- **Integración (API):** en caso de ser un proveedor externo, debe ofrecer una API robusta y fácil de integrar con los sistemas de alta de clientes o comercios (onboarding) del agregador.
- **Continuidad de Negocio:** El proveedor debe contar con un Plan de Continuidad de Negocio para garantizar que el servicio de consulta no se interrumpa.
- **Seguridad de la Información:** garantizar la integridad, confidencialidad y disponibilidad de los datos.
  a. Contar con certificaciones en materia de seguridad de la información (por ejemplo, ISO 27001).
  b. Contar con protocolos definidos de seguridad en el procesamiento y transmisión de la información.

Los expedientes que los agregadores conforman para cada cliente o comercio constituyen el primer insumo para construir un perfil transaccional inicial, del cual se hablará con mayor detalle más adelante. A partir de esta información se puede estimar un riesgo preliminar, identificar alertas tempranas y determinar qué acciones de verificación, validación o seguimiento deben aplicarse desde el inicio de la relación comercial.

Además, los agregadores deben adoptar diferentes esquemas de KYC, como el régimen simplificado de identificación cuando un cliente o comercio es catalogado como de bajo riesgo, o la debida diligencia reforzada cuando el nivel de riesgo aumenta o cuando, desde el inicio, se trate de clientes o comercios clasificados como de alto riesgo.

Adicionalmente, se debe garantizar la conservación de los expedientes conforme a los plazos mínimos legales, que son de 10 años[11]. Para tal efecto, los agregadores, deben contar con sistemas de resguardo adecuados, ya sean digitales o en espacios físicos que se adapten a las necesidades operativas de cada agregador, cuidando en todo momento que la misma cuente con la protección necesaria para garantizar su integridad, disponibilidad y confidencialidad, evitando cualquier alteración, destrucción, pérdida o acceso no autorizado durante dicho periodo.

Al recabar, verificar, actualizar y conservar la documentación e información de sus clientes o comercios, el agregador cierra el círculo de seguridad, asegurándose de que cada cliente o comercio afiliado es quien dice ser, estableciendo así un entorno de negocios más seguro y confiable.

11.- Cámara de Diputados. (2025, Julio) Ley Federal para la Prevención e Identificación de Operaciones de Recursos de Procedencia Ilícita. Página 16. Cámara de Diputados. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI.pdf

INFORMACIÓN A REQUERIR EN EL KYC

Aunque el universo de clientes o comercios es vasto, la experiencia del sector nos permite identificar y categorizar los perfiles de clientes o comercios más usuales con los que interactúa un agregador:

- Personas Físicas de Nacionalidad Mexicana: Emprendedores y profesionistas locales.
- Personas Físicas Extranjeras: Residentes con estancia legal en territorio nacional.
- Personas Morales Nacionales: Empresas constituidas bajo leyes mexicanas (S.A., S.C., S.A.P.I., etc.).
- Personas Morales Extranjeras: Empresas internacionales con operaciones en México.
- Entidades Gubernamentales: En ocasiones, dependencias que requieren servicios de recaudación.

Para garantizar una identificación plena, las mejores prácticas del sector sugieren recabar, como mínimo, un conjunto de datos y documentos que acrediten la existencia y legalidad del cliente o comercio. Por lo que de manera enunciativa más no limitativa, entre los elementos clave se incluyen:

1. Información Básica
Datos fundamentales como:

- Nombre completo o Razón Social.
- Domicilio fiscal y operativo.
- Teléfono.
- Correo electrónico.
- Datos del Representante Legal.

2. Documentación Soporte:

- **Identificación Oficial Vigente:** (INE o Pasaporte) del titular o representante legal. Es crucial validar su vigencia y autenticidad.
- **Claves de Identificación Fiscal y Poblacional:** El RFC (Registro Federal de Contribuyentes) para validar la situación fiscal y actividad económica, y la CURP en el caso de personas físicas (validable ante RENAPO).
- **Comprobante de Domicilio:** Reciente, para asegurar la ubicación física del negocio.
- **Documentos Corporativos (Personas Morales):** El Acta Constitutiva para acreditar la existencia legal de la empresa y los Poderes Notariales para verificar que quien firma tiene la facultad jurídica para hacerlo.

De igual manera y como parte fundamental de la validación documental, el agregador debe cotejar que la actividad económica declarada por el cliente o comercio no se encuentre dentro de las categorías prohibidas o restringidas por la normativa del sector[12], por ejemplo, las actividades prohibidas, las cuales implican la afiliación de clientes o comercios relacionados con actividades ilícitas como pornografía infantil, o cualquier actividad de contenido para adultos prohibida por las leyes nacionales, venta de sustancias ilegales o controladas sin los permisos correspondientes, etc.

12.- Mandatos de los titulares de marca (VISA y Mastercard)

CONSULTA EN LISTAS NEGRAS: EL ABC DE LAS MEJORES PRÁCTICAS

Verificar con quién se establecen relaciones comerciales (clientes o comercios), a quién se contrata como proveedor clave (manejo de datos sensibles, gateway de pagos, liquidadores, servicios de cloud, entre otros), personal del agregador (staff ejecutivo, personal del área comercial, el oficial de cumplimiento, entre otros) es un paso esencial para garantizar la integridad del agregador. El insumo obtenido en el KYC (en el caso de clientes y comercios) y el due dilligence (para proveedores y persona) nos permite revisar si los perfiles que interactúan con los agregadores han sido señalados anteriormente como riesgosos o delictivos. En este contexto, la consulta en listas negras, se convierte en una herramienta indispensable de PLD/FT.

Las listas negras o restrictivas incluyen individuos, entidades y organizaciones que han sido sancionados o se encuentran bajo restricciones legales, regulatorias o normativas. Estas listas son fundamentales para evitar transacciones con partes que representan un alto riesgo de actividades ilícitas, es decir, son bases de datos que ayudan a mitigar los riesgos de con quién realizan actividades comerciales los agregadores.

Incorporar la consulta en listas dentro de los procedimientos de afiliación de nuevos clientes o comercios demuestra el compromiso del gremio con la transparencia y la prevención. Más allá del cumplimiento, esta práctica refuerza la confianza de los clientes o comercios o socios financieros, previene la exposición a riesgos reputacionales, promueve la cooperación con autoridades nacionales y mitiga el riesgo de que un agregador pueda ser utilizado para PLD/FT.

Sin embargo, la consulta en listas no debe verse únicamente como un filtro inicial. Las condiciones de riesgo cambian constantemente, un cliente o comercio, o un socio estratégico que antes no representaba una amenaza, podría aparecer posteriormente en alguna lista negra, por lo que se recomienda que la validación de listas se aplique de forma continua a toda la base de datos de sus clientes o comercios al menos cada trimestre, lo anterior con base en las mejores prácticas del sector financiero. Por ello, los agregadores que implementan verificaciones periódicas o automatizadas demuestran una cultura de cumplimiento más sólida y una verdadera gestión preventiva del riesgo.

En este sentido, para llevar a cabo estas consultas de manera eficiente, **en México existen diversos proveedores especializados que ofrecen herramientas para automatizar dicho proceso.** El uso de estas plataformas permite consultar múltiples bases de datos y realizar búsquedas masivas y eficaces, reduciendo la carga operativa manual.

Alcance y Calidad de la Información
La calidad de la lista es más importante que la cantidad de registros.

- Fuentes de la Información: Preguntar qué tipo de fuentes utilizan.
- Cobertura Geográfica: Debe cubrir las jurisdicciones de los clientes o comercios a los que se les da servicio.
- Actualización y Frecuencia: La base de datos debe ser actualizada diariamente (o en tiempo real) y el proveedor debe garantizar la frecuencia con la que integran nuevas listas.

Capacidad Técnica y Tecnología[13]
La tecnología debe garantizar la eficiencia de tu proceso de Due Diligence.

- Motor de Búsqueda y Coincidencias (Fuzzy Logic): El sistema debe utilizar algoritmos avanzados (fuzzy logic) para manejar homónimos, errores de escritura, transliteraciones de nombres y variaciones. Una simple coincidencia exacta no es suficiente y genera falsos positivos o, peor aún, falsos negativos.
- Integración (API): Debe ofrecer una API robusta y fácil de integrar con los sistemas de alta de clientes o comercios (onboarding) y monitoreo transaccional.
- Tiempo de Respuesta: Las consultas deben resolverse en milisegundos para no afectar la experiencia del cliente o comercio durante el proceso de alta.
- Evidencia de Consulta: El sistema debe generar un registro auditable (bitácora o audit trail) que demuestre que se consultó la identidad del cliente o comercio en una fecha y hora específica, y con qué resultado.

Seguridad
Al igual que en el KYC, el tratamiento y manejo de datos para consultar listas negras debe seguir ciertos estándares de seguridad.

- Seguridad de la Información: Deben garantizar la integridad, confidencialidad y disponibilidad de los datos.
- Pregunta sobre sus certificaciones (por ejemplo, ISO 27001).
- Deben contar con protocolos de seguridad en el procesamiento y transmisión de la información.
- Manejo de Datos Personales: Debe cumplir con la normativa de protección de datos aplicable en México, garantizando que el tratamiento de los datos consultados o almacenados se haga de forma legal y segura.
- Continuidad de Negocio: El proveedor debe contar con un Plan de Continuidad de Negocio para garantizar que el servicio de consulta no se interrumpa.
- Para que el blindaje sea efectivo, la consulta no debe limitarse únicamente al nombre comercial del negocio. Las mejores prácticas dictan que la verificación en listas debe abarcar a todos los actores clave involucrados en la relación comercial:

Si es Persona Física: Al titular de la cuenta.
Si es Persona Moral: A la Razón Social, a los Representantes Legales y a los Accionistas.

13.- Criterios tecnológicos basados en el “Marco para el Cumplimiento de Sanciones” de la OFAC (Departamento del Tesoro de EE.UU.) y la “Guía sobre el Filtrado de Sanciones” del Grupo Wolfsberg, así como en los requerimientos de auditabilidad de sistemas automatizados

TIPOS DE LISTAS SUGERIDAS

El universo de listas es amplio, pero para efectos de prevención en el sector de agregadores, se recomienda consultar las siguientes categorías:

1. Categoría por naturaleza del riesgo: Es la clasificación general asignada a una lista en función del riesgo que representa.

a. PEPs (Personas Expuestas Políticamente): Esta categoría incluye personas que, a través de su posición destacada o influyente en el gobierno, son más susceptibles a estar involucradas en soborno o cometer actos de corrupción[14]. Utiliza como fuente bases de datos de organismos internacionales y nóminas gubernamentales.
b. Law Enforcement (Fuerzas del Orden): Listas emitidas por agencias de seguridad e inteligencia que contienen información sobre individuos buscados, investigados o condenados por la comisión de delitos graves. Estas listas no se refieren a los miembros de las fuerzas del orden, sino a los objetivos de sus investigaciones.
c. Regulatory Enforcement (Cumplimiento Regulatorio): Listas que contienen información sobre individuos o entidades que han violado regulaciones específicas y están sujetos a acciones regulatorias. Utilizando fuentes de organismos supervisores.
d. Sanctions (Sanciones): Listas que contienen personas o empresas que han sido sancionadas por diversas autoridades, tanto nacionales como internacionales por actividades ilícitas o incumplimiento regulatorio.
e. Gatekeepers (Guardianes): Esta categoría agrupa a profesionales y entidades no financieras que, por la naturaleza de su actividad, pueden ser utilizados como puerta de entrada para recursos ilícitos. Las listas permiten identificar si un cliente o comercio desempeña alguna de estas Actividades Vulnerables para aplicar una debida diligencia reforzada. Utiliza como fuentes registros gremiales.
f. Adverse Information (Información Adversa): Listas que contienen información adversa y valiosa para las políticas internas de una entidad. Utiliza como fuente el monitoreo de medios de comunicación abiertos, tales como noticias, reportajes o menciones públicas disponibles en la prensa, sitios web, blogs, redes sociales, y bases de datos de dominio público.
g. Blocked (Bloqueados): Esta categoría contiene registros de personas o entidades que han sido oficialmente bloqueadas por autoridades financieras o gubernamentales. Utiliza fuentes directas de autoridades gubernamentales.

2. Categoría por ámbito de origen: Dichas categorías de riesgo se distribuyen en 4 tipos de listas según su alcance geográfico:

LISTAS GLOBALES

OFAC - Specially Designated Nationals (SDN)[15]

OFACN - Non-Specially Designated Nationals List (Non-SDN)[16]

ONU - Organización de las Naciones Unidas (Consejo de Seguridad 1267 y 1373)[17]

PEPINT - Persona Políticamente Expuesta Internacional (CIA)[18]

LISTAS NACIONALES[19]

Personas Políticamente Expuestas (PEPs) nacionales[20]

SAT69B - Servicio de Administración Tributaria Art. 69-B CFF[21]

SAT69B-BIS - Servicio de Administración Tributaria Art. 69B-BIS CFF[22]

Lista de Servidores Públicos Sancionados por la PGR - Procuraduría General de la República de México (ahora Fiscalía General de la República)[23]

Registro Nacional de Detenciones[24]

LISTAS INFORMATIVAS

CORR - Gatekeepers “Corredores”[25]

DONA - Gatekeepers “Donatarios”[26]

NOTA - Gatekeepers “Notarios”[27]

SIND - Gatekeepers “Sindicatos”[28]

LISTAS INTERNAS[29]

Aquellas generadas por el propio Agregador o el gremio para identificar comercios con antecedentes de fraude o comportamiento irregular.

21.- Listado publicado por el Servicio de Administración Tributaria (SAT) sobre las personas que se ubican en el supuesto de Empresas que Facturan Operaciones Simuladas (EFOS) presunto, https://www.sat.gob.mx/portal/public/tramites/articulo-69-del-cff
22.- Listado publicado por el Servicio de Administración Tributaria (SAT) sobre las personas que se ubican en el supuesto de hacer una transmisión indebida del derecho de disminuir pérdidas fiscales, https://www.sat.gob.mx/portal/public/tramites/articulo-69-del-cff
23.- La Secretaría de la Función Pública y los Órganos Internos de Control de cada institución, incluyendo la FGR, tienen registros de funcionarios que han sido inhabilitados o sancionados por faltas administrativas o hechos de corrupción. Estos registros son públicos y pueden consultarse en el Sistema del Registro de Servidores Públicos Sancionados. https://compras.buengobierno.gob.mx/ConsultaPublicaDGRSP/ -Registros de Detenciones: Puedes consultar el Registro Nacional de Detenciones para verificar si una persona está actualmente detenida y puesta a disposición de las autoridades.
24.- Se puede consultar para verificar si una persona está actualmente detenida y puesta a disposición de las autoridades, incluyendo en vinculación con algún delito relacionado a finanzas ilícitas o en colaboración con una agrupación terrorista designada. https://consultasdetenciones.sspc.gob.mx/
25.- El Directorio de Corredores Públicos del Colegio Nacional de Correduría Pública, pone a disposición la lista con la finalidad de verificar la existencia y el registro legal de estos profesionales, y así prevenir que dichos intermediarios sean utilizados indebidamente como vehículos para la canalización de recursos ilícitos.
26.- El Directorio de Donatarios Públicos Autorizados pone a disposición la lista con la finalidad de verificar la existencia y el estatus legal de las Organizaciones de la Sociedad Civil. La consulta a esta lista permite confirmar la legitimidad de las donaciones y prevenir que las organizaciones no lucrativas sean utilizadas para la canalización de recursos de procedencia ilícita, un riesgo potencial que debe ser gestionado por los participantes del sistema financiero.
27.- El Directorio de Notarios Públicos del Colegio Nacional del Notariado Mexicano pone a disposición del público, las listas con la finalidad de verificar la identidad de los representantes legales, la existencia legal de las empresas, y, crucialmente, la validez y el alcance de los poderes notariales,incluyendo facultades como pleitos y cobranzas.
28.- El Directorio de Sindicatos y Asociaciones del STPS (Secretaría del Trabajo y Previsión Social) pone a disposición la lista para verificar la existencia y el registro legal de estas organizaciones, con la finalidad de prevenir que dichas estructuras sean utilizadas indebidamente como vehículos para la canalización de recursos ilícitos.
29.- Para efectos de consulta, es importante señalar que algunas de las listas mencionadas no son de acceso público directo. En estos casos, su consulta requiere contar con los servicios de un proveedor especializado que otorgue acceso autorizado a dichas bases de datos.

¿QUÉ HACER EN CASO DE IDENTIFICAR A UN CLIENTE EN LISTAS NEGRAS?

Como se mencionó, las listas son fundamentales para evitar transacciones con clientes o comercios que representan un alto riesgo de actividades ilícitas.

Sin embargo, es importante tener presente la posible aparición de falsos positivos derivados de homónimos (personas o empresas con el mismo nombre, pero distinta identidad). Para evitar afectar a clientes o comercios legítimos, los agregadores pueden apoyarse en empresas tecnológicas que ofrecen servicios de validación avanzada para descartar estas coincidencias automáticamente, o bien, diseñar políticas internas de validación cruzada (cotejando RFC, CURP o fecha de nacimiento) para minimizar este riesgo operativo.

Si durante el proceso del KYC con un prospecto de un cliente o comercio, o durante la validación del 100% de los clientes o comercios actuales de los agregadores se obtiene una coincidencia positiva, se sugiere actuar bajo los siguientes lineamientos generales:

En el Proceso de Alta (KYC)

Si en el proceso de enrolamiento y afiliación de un prospecto se detecta una coincidencia en listas negras, se deberán seguir los siguientes pasos:

- **Suspensión del proceso de afiliación:** Se deberá posponer inmediatamente el enrolamiento y la afiliación del prospecto. No se podrá continuar con el trámite hasta obtener el visto bueno del área de cumplimiento.

- **Verificación y Análisis:** El caso será turnado a las áreas de cumplimiento para que realicen una investigación exhaustiva, la cual deberá determinar: En qué lista específica surgió la coincidencia. Si la identidad del prospecto coincide plenamente con la persona listada o si existen discrepancias que sugieran un homónimo.

- **Dictamen y Resolución:** Con base en la investigación, se tomará una de las siguientes acciones definitivas:

  - Si es un Falso Positivo u Homónimo: Se notificará la aclaración al prospecto y se levantará la suspensión para continuar con el proceso de enrolamiento y afiliación de manera regular.

  - Si es una Coincidencia Real (Positivo Confirmado): En caso de verificar que el sujeto efectivamente se encuentra en las listas de personas bloqueadas o sancionadas, se denegará definitivamente la contratación del servicio.

En Clientes o Comercios Activos (Transaccionado):

- **Suspensión Preventiva:** Si la coincidencia se da en clientes o comercios que ya están operando, se debe detener cualquier transacción con estos de manera inmediata para mitigar riesgos.

- **Verificación y Análisis:** El caso será turnado a las áreas de cumplimiento para que realicen una investigación exhaustiva, la cual deberá determinar:

  - En qué lista específica surgió la coincidencia.

  - Si la identidad del prospecto coincide plenamente con la persona listada o si existen discrepancias que sugieran un homónimo.

- **Dictamen y Resolución:** Con base en la investigación, se tomará una de las siguientes acciones definitivas:

  - Si es un Falso Positivo u Homónimo: Se notificará la aclaración al prospecto y se levantará la suspensión para continuar con el proceso de enrolamiento y afiliación de manera regular.

  - Si es una Coincidencia Real (Positivo Confirmado): En caso de verificar que el sujeto efectivamente se encuentra en las listas de personas bloqueadas o sancionadas, se procederá a suspender de manera definitiva el servicio al comercio.

EL ENFOQUE BASADO EN RIESGOS (EBR): LA ESTRATEGIA INTELIGENTE DE PREVENCIÓN

El EBR es el diseño e implementación de una metodología para llevar a cabo una evaluación de los riesgos a los que se encuentran expuestos los agregadores, derivado de los productos, servicios, clientes o comercios, países o áreas geográficas, transacciones y canales de envío o distribución vinculados con sus operaciones y con sus clientes o comercios.

De acuerdo a la "Guía para un enfoque basado en riesgo" emitida por el Grupo de Acción Financiera (GAFI) en octubre de 2014[30], el EBR es el deber por parte de los países, autoridades competentes e instituciones financieras de identificar, evaluar y entender los riesgos a los que están expuestos y adoptar medidas adecuadas para mitigar de manera efectiva dichos riesgos.

Además, el EBR adquire cada día más relevancia en normativas nacionales e internacionales. En el contexto nacional, la reforma del 16 de julio de 2025 a la LFPIORPI consolidó la adopción del Enfoque Basado en Riesgos como un requisito indispensable. Al armonizarse con estándares de gestión como la ISO 31000 —norma internacional que establece principios y directrices para un manejo integral y sistemático del riesgo— esta metodología se convierte en un pilar central para el cumplimiento legal y operativo.

Específicamente para el caso de los agregadores, el EBR debe permitirles entender cómo y hasta qué punto son vulnerables a los riesgos, lo cual le permitirá asignar eficientemente sus recursos y aplicar procesos de gestión de dichos riesgos adecuados a sus características propias. Es importante que los agregadores identifiquen la diferencia entre los riesgos financieros del agregador y los riesgos de PLD/FT.

El Enfoque Basado en Riesgos permite identificar perfiles y características que, por su naturaleza, implican una mayor probabilidad de exposición a actividades ilícitas.
Al detectarlos, los agregadores pueden aplicar una gestión diferenciada y prioritaria, orientada a mitigar de manera efectiva los riesgos específicos de PLD/FT asociados a cada caso.

El Modelo de Evaluación de Riesgos (MER) por su parte, es aquel que establece y describe todos los procesos que se llevarán a cabo para la identificación, medición y mitigación de los riesgos de sus clientes o comercios, presentándolos de una manera clara, concisa y organizada.

En su conjunto el EBR y MER son los mecanismos mediante los cuales se define la exposición al riesgo de los agregadores. Por tanto, su desarrollo conlleva necesariamente considerar diversos indicadores, tales como la frecuencia, el volumen de las operaciones, el carácter de las relaciones y el modo de interactuar con el cliente o comercio.

Considerando lo anterior, los indicadores varían de un agregador a otro. El diseño del EBR y MER de cada agregador debe establecer los procesos particulares que se llevarán a cabo para la identificación, medición y mitigación de sus riesgos de acuerdo a las características del modelo de negocio de cada agregador.

Por ejemplo, el EBR y MER de un agregador enfocado exclusivamente en comercio electrónico (e-commerce) deberá ponderar con mayor severidad los riesgos de fraude cibernético y transacciones no presenciales; mientras que la de un agregador dedicado a terminales físicas para pequeños comercios (mPOS) priorizará riesgos distintos, como la ubicación geográfica de los dispositivos o la validación de identidad presencial. En consecuencia, el EBR y MER establecerán los procesos de identificación, medición y mitigación alineados estrictamente a las características, modelo de negocio y tipos de clientes o comercios de cada agregador.

30.- GAFI (2014, Octubre) Guía del GAFI sobre el enfoque basado en el riesgo para combatir el lavado de dinero y la financiación del terrorismo: Principios y procedimientos de alto nivel. FATF-GAFI. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfguidanceontherisk- basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html

El desarrollo del MER comprende 3 fases:

1. Diseño: Busca identificar todos los elementos de riesgo y medirlos con indicadores, para que sobre cada uno de ellos se determinen mitigantes, se evalúe el riesgo y la efectividad de las mitigantes definidas para determinar el riesgo residual.
Una vez identificados estos factores, la medición debe basarse en herramientas visuales como los "Mapas de Calor". Estos permiten cruzar la probabilidad de que un evento ocurra contra la magnitud de su impacto, otorgando un nivel de severidad claro (Muy Bajo, Bajo, Medio, Alto y Muy Alto).

Niveles de riesgo

Muy Alto	Bajo	**Medio**	**Alto**	**Muy Alto**	**Muy Alto**
Alto	Bajo	**Medio**	**Medio**	**Alto**	**Muy Alto**
Medio	Bajo	**Medio**	**Medio**	**Medio**	**Alto**
Bajo	Bajo	Bajo	Bajo	Medio	Medio
Muy bajo	Muy Bajo	Bajo	Bajo	Bajo	Bajo
	Muy Poco Probable	**Poco Probable**	**Probable**	**Altamente Probable**	**Seguro**

Probabilidad

Fuente: GAFILAT, diciembre de 2022, p. 39.

Con lo anterior, el agregador puede decidir el tratamiento adecuado para cada riesgo. Existen cuatro estrategias posibles:

I. Mitigar: Aplicar controles para reducir el riesgo.
Además, requiere de forma continua programas de capacitación robustos para el personal y un compromiso de mejora continua en los procesos internos para adaptarse a las nuevas tipologías de riesgo.

II. Transferir: Pasar el riesgo a un tercero.
Implica trasladar el riesgo económico mediante la contratación de seguros contra el fraude o subcontratando a una empresa especializada para el scoring de riesgo, aunque la responsabilidad final ante la autoridad sigue siendo del agregador.

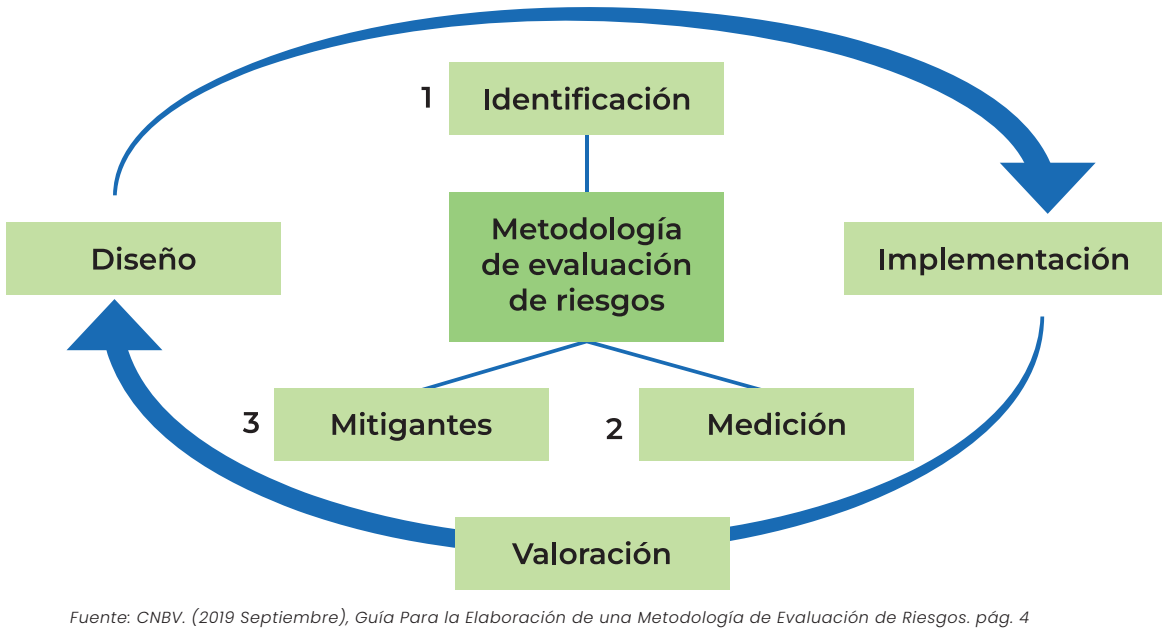
III. Aceptar: Asumir el riesgo cuando es bajo y el costo del control es excesivo.
Es la decisión consciente de asumir el riesgo residual cuando este se clasifica como Bajo o Aceptable.

IV. Rechazar: Decidir no operar ese producto, cliente o comercio o canal por ser demasiado riesgoso. Implica la negativa a iniciar una relación comercial, terminar una relación con un cliente existente, o decidir no operar con productos, giros o jurisdicciones específicas que se consideren incompatibles con la política interna de PLD/FT.

2. Implementación: Busca llevar a cabo el funcionamiento de la metodología en las operaciones del agregador, para prevenir la colocación, estratificación e integración de los recursos de procedencia ilícita y la adquisición, integración, transmisión y conversión para apoyar al financiamiento al terrorismo.

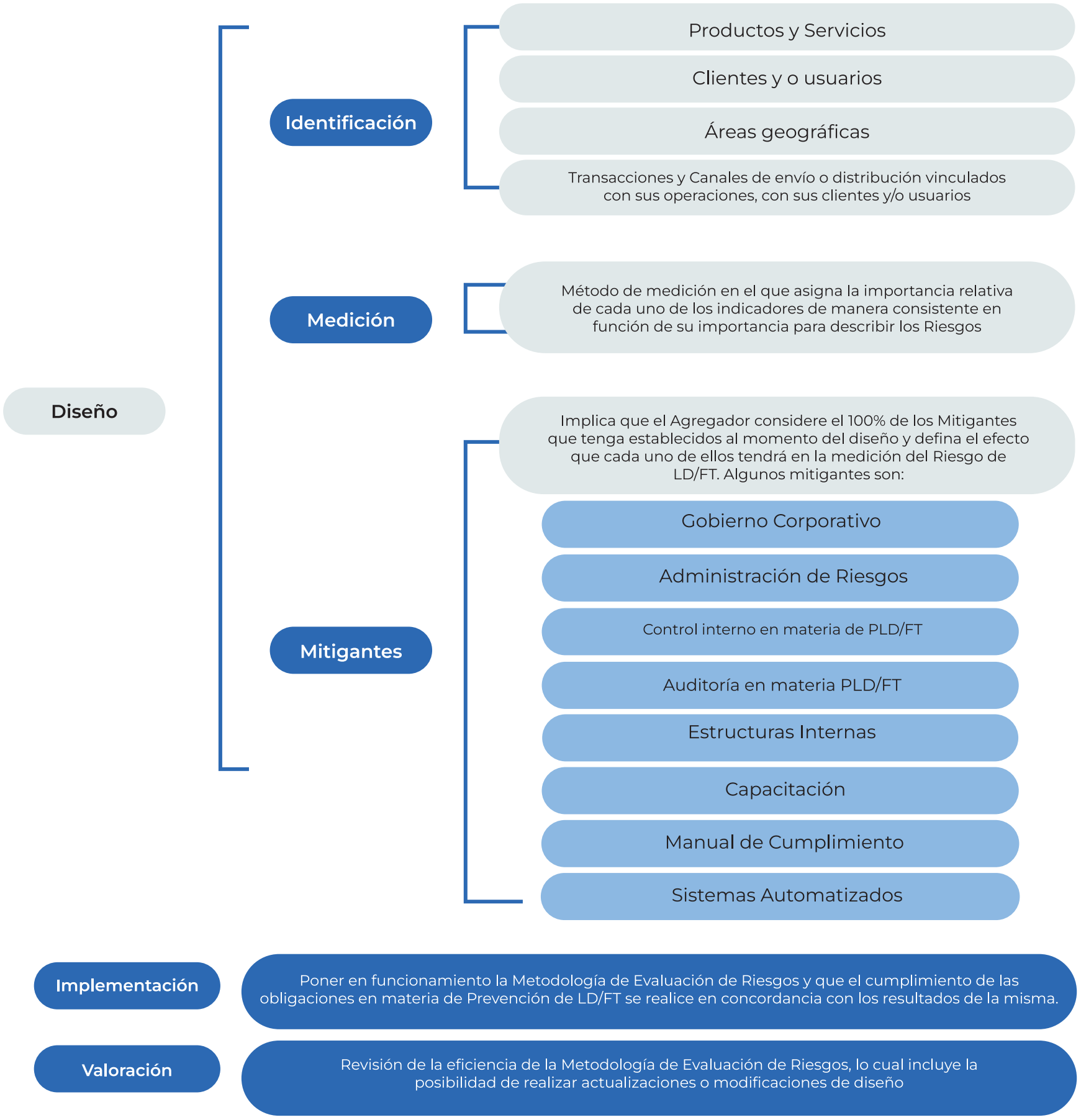
3. Valoración: Busca evaluar la eficiencia y eficacia de la metodología para su actualización y mejora.

Contexto o entorno del sujeto supervisado



Fuente: CNBV. (2019 Septiembre), Guía Para la Elaboración de una Metodología de Evaluación de Riesgos. pág. 4

Las fases de la metodología se detallan en la figura siguiente:



Fuente: CNBV. (2019 Septiembre), Guía Para la Elaboración de una Metodología de Evaluación de Riesgos. Gobierno de México.

PERFILAMIENTO CON EBR

El EBR permite a los agregadores generar perfiles de riesgo de sus clientes y comercios. Esto además sirve para optimizar recursos y concentrar los esfuerzos de prevención donde realmente se generan los mayores riesgos. En lugar de aplicar controles uniformes a todos los clientes o comercios, los agregadores pueden ajustar sus medidas según el tipo de operación, el historial del cliente o comercio, la zona geográfica en la cual se localiza el cliente o comercio, entre otros factores.

La zona geográfica y el giro comercial son dos de los factores más relevantes a contemplar al perfilar con EBR a un cliente o comercio, ya que impacta directamente en el grado de riesgo asociado, por ejemplo:

Actividades de Alto Riesgo: De acuerdo con los lineamientos internacionales emitidos por los Titulares de Marca y con base en recomendaciones del GAFI, existen actividades económicas consideradas de alto riesgo operativo, reputacional o legal. Estas actividades requieren una afiliación individualizada, controles reforzados y monitoreo continuo, y no deben ser incorporadas como subafiliados genéricos, debido a su vulnerabilidad a esquemas de lavado, fraude o evasión.

Estos giros incluyen, entre otros:

Juegos y Apuestas: Casinos, casas de juego, loterías y apuestas (MCC 7995).

Farmacias y Droguerías: Venta de medicamentos controlados o prescripción médica vía Internet (MCC 5912).

Telemarketing y Ventas Directas: Clientes o Comercios que realizan ventas por teléfono (Inbound/Outbound) o ventas de puerta en puerta (MCC 5960-5969).

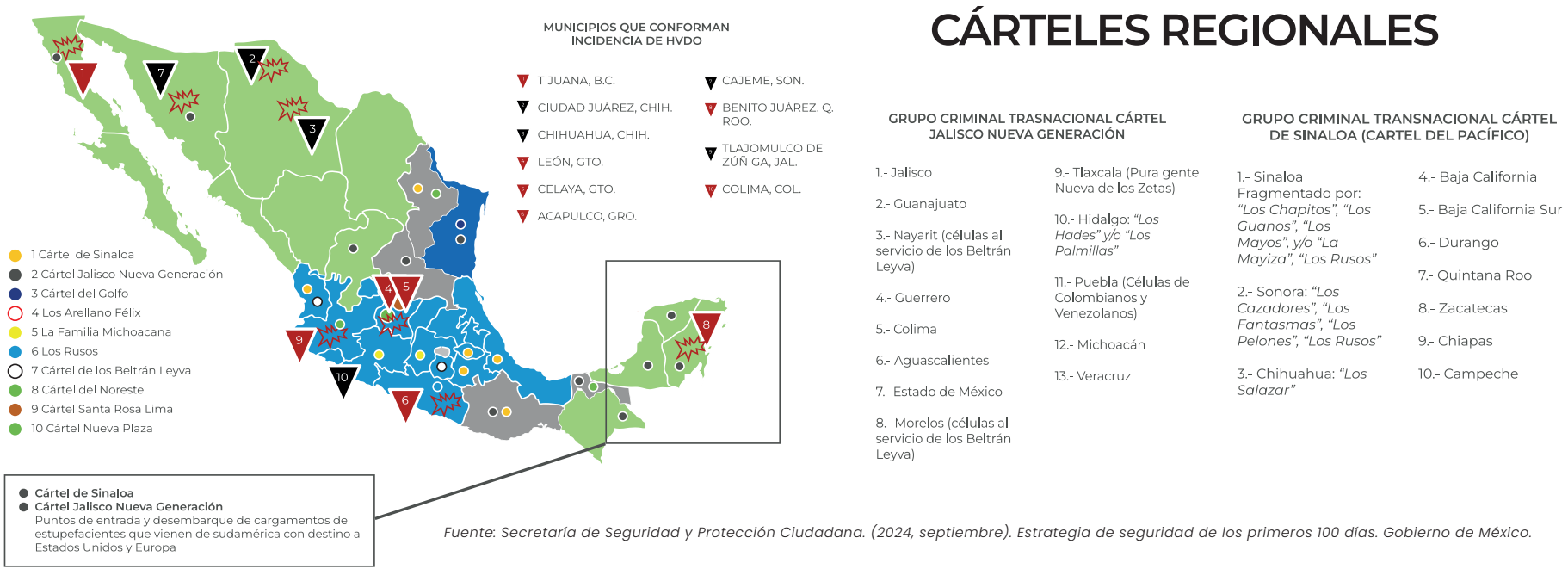
Tabaco: Tabaquerías y producción de tabaco (MCC 5993).

Servicios de Telecomunicación: Llamadas locales, larga distancia y servicios de información por computadora (MCC 4814, 4816).

Clubes de Mayoristas: Clubes de membresía (MCC 5300).

Burós de Crédito: Protección de crédito o contra robo de identidad (MCC 7321).

Zona Geográfica: se debe considerar la ubicación de cada cliente o comercio tomando como referencia los mapas que se muestran a continuación, los cuales ilustran la presencia de grupos delictivos y cárteles regionales, sirviendo como indicadores clave del nivel de riesgo en cada zona.



Fuente: Secretaría de Seguridad y Protección Ciudadana. (2024, septiembre). Estrategia de seguridad de los primeros 100 días. Gobierno de México.

Una vez analizados estos factores, el agregador puede clasificar a sus clientes o comercios (usualmente en niveles Muy Bajo, Bajo, Medio, Alto y Muy Alto) y aplicar medidas diferenciadas, como a continuación se detalla:

- **Riesgo Bajo (Régimen simplificado):** Para clientes o comercios debidamente identificados, que no cuenten con giros riesgosos o no estén en zonas geográficas de alto riesgo, el proceso de alta puede ser ágil, solicitando los requisitos mínimos indispensables.

- **Riesgo Alto (Debida diligencia reforzada):** Para clientes o comercios que, por su naturaleza o ubicación, presentan mayores riesgos, se aplica una debida diligencia intensificada. Esto no significa negar el servicio, sino solicitar mayor información, actualizar documentación en períodos más recurrentes, posiblemente hacer visitas de inspección para conocer al cliente o comercio y aplicar un monitoreo transaccional más estricto.

A modo de ejemplo, para asignar un grado de riesgo inicial a los clientes o comercios, es posible utilizar como referencia la Evaluación Nacional de Riesgos 2023. En la tabla siguiente se muestra cómo varía el nivel de riesgo dependiendo del giro del comercio:

SECTOR	2020	2023
OBRAS DE ARTE	ALTO	ALTO
METALES PRECIOSOS, PIEDRAS PRECIOSAS, JOYAS Y RELOJES	ALTO	ALTO
MONEDEROS Y CERTIFICADOS DE DEVOLUCIONES O RECOMPENSAS	MEDIO	ALTO
TARJETAS PREPAGADAS, VALES O CUPONES	MEDIO	MEDIO
VEHÍCULOS AÉREOS, MARÍTIMOS O TERRESTRES	ALTO	MEDIO
SERVIDORES PÚBLICOS	-	MEDIO
FE PÚBLICA	MEDIO	MEDIO
MUTUO, PRÉSTAMOS O CRÉDITOS	MEDIO	MEDIO
SERVICIOS DE BLINDAJE	ALTO	MEDIO-BAJO
TARJETAS DE SERVICIOS O DE CRÉDITO	MEDIO-BAJO	MEDIO-BAJO
JUEGOS CON APUESTA, CONCURSOS O SORTEOS	MEDIO-BAJO	MEDIO-BAJO
TRANSMISIÓN DE DERECHOS SOBRE BIENES INMUEBLES	MEDIO-BAJO	MEDIO-BAJO
RECEPCIÓN DE DONATIVOS	MEDIO-BAJO	MEDIO-BAJO
DERECHOS PERSONALES DE USO O GOCE DE INMUEBLES	MEDIO	MEDIO-BAJO
DESARROLLO INMOBILIARIO	-	MEDIO-BAJO
ACTIVOS VIRTUALES	-	MEDIO-BAJO
SERVICIOS PROFESIONALES	MEDIO-BAJO	MEDIO-BAJO
TRASLADO O CUSTODIA DE DINERO O VALES	MEDIO-BAJO	MEDIO-BAJO

Fuente:Secretaría de Hacienda y Crédito Público. (2023). Evaluación Nacional de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo. Gobierno de México.

RESPONSABILIDAD COMPARTIDA EN LA SEGURIDAD DEL ECOSISTEMA

Es fundamental destacar que la gestión de riesgos de un agregador no termina con sus propias evaluaciones internas. Como participantes de la red de pagos, los agregadores operan bajo lineamientos de seguridad compartida que impactan directamente su perfil de riesgo.

Aunque la relación contractual principal se establece con el adquirente que procesa las transacciones del agregador, las obligaciones estipuladas en la normativa del sector transfieren responsabilidades críticas que el agregador debe integrar en su EBR.

Implementar una visión basada en riesgos también contribuye a construir confianza institucional. Las autoridades, los adquirentes y los socios comerciales percibirán a los agregadores que aplican esta metodología como actores maduros, capaces de entender la complejidad del sistema financiero y de autorregularse de manera efectiva.

A través de esta práctica, los agregadores reafirman su papel como aliados estratégicos del desarrollo financiero, demostrando que prevenir riesgos también es una forma de impulsar el crecimiento sostenible.

1. Monitoreo de Puntos de Compromiso: Si se detecta que un cliente o comercio afiliado es el punto de origen de un fraude, el agregador debe actuar de inmediato (bloqueo o investigación), ya que esto eleva el riesgo de toda la red.

2. Atención al Sistema Nacional de Alertas: Los reportes sobre clientes o comercios con comportamientos irregulares (por ejemplo, exceso de contracargos, fraudes, etc.) emitidos por otros participantes deben ser incorporados como un factor de riesgo alto inmediato para la toma de decisiones.

3. Cumplimiento de Estándares de Seguridad (PCI-DSS): La vulnerabilidad tecnológica de un cliente o comercio es un riesgo de lavado de dinero y fraude. Asegurar que los sistemas cumplan con la normativa de protección de datos es parte esencial de la mitigación de riesgos.

EL MONITOREO TRANSACCIONAL: CONOCER AL CLIENTE O COMERCIO EN ACCIÓN

El conocimiento del cliente o comercio no termina cuando se aprueba su afiliación. Con el paso del tiempo, un comercio que en principio fue legítimo, o no señalaba ser riesgoso, puede empezar a comportarse de una manera que lo hace sospechoso de alguna actividad vinculada con las finanzas ilícitas.

El monitoreo transaccional es la práctica que permite observar, entender y analizar el comportamiento conductual, operativo y transaccional de los clientes o comercios en tiempo real, tomando como base el comportamiento histórico del cliente o comercio a lo largo del tiempo. Este conocimiento conductual permite determinar cuándo un cliente o comercio sale de su perfil transaccional habitual, identificando así irregularidades que podrían indicar un riesgo.

En el ecosistema de pagos, donde millones de transacciones ocurren cada día, este proceso se vuelve una herramienta clave para mantener la integridad y la seguridad de la red de medios de pagos. El monitoreo representa una forma de acompañamiento que ayuda a los agregadores a detectar comportamientos anómalos, prevenir fraudes y proteger a los clientes o comercios.

Un esquema de monitoreo efectivo se apoya en tres pilares fundamentales:

Identificar desviaciones o patrones inusuales que puedan sugerir un riesgo.

Análisis constante

Responder con medidas proporcionales, de acuerdo con el nivel de exposición o sospecha detectada.

Acción responsable

Conocer el comportamiento conductual de operación de cada cliente o comercio a fin de establecer parámetros operativos. Se pueden esperar ciertos comportamientos a partir del perfilamiento obtenido del EBR, así como la propia transaccionalidad que haya tenido cada comercio durante su tiempo usando activamente los servicios del agregador. **El agregador debe validar que el giro de estos coincida con su operación transaccional y no utilizar códigos de giro genéricos.**

Información constante

El monitoreo transaccional también impulsa la mejora continua. Cada alerta, revisión o hallazgo se convierte en un insumo para refinar los parámetros que detonan una revisión. Las observaciones derivadas del análisis transaccional ayudan a perfeccionar los procesos internos, actualizar criterios y fortalecer los mecanismos de identificación temprana de riesgos.

Para identificar cualquier anomalía, es indispensable establecer primero los parámetros de una operación normal de cada cliente o comercio, según sus particularidades. Este es el propósito del perfil transaccional.

Este perfil funge como la referencia operativa de cada cliente o comercio. Se construye mediante la integración de la información declarada por el cliente o comercio durante su afiliación (KYC) con el comportamiento histórico de sus ventas. Algunos de los elementos que deben contemplarse en la formulación del perfil transaccional de un cliente o comercio, y que pueden inferirse de su giro, tamaño y ubicación, son:

Volumen Transaccional: El monto promedio por venta (ticket promedio) y la facturación mensual estimada.

Frecuencia Operativa: El número de operaciones esperadas por hora, día o por semana.

Patrones Temporales: La correspondencia entre los horarios de las transacciones y el horario comercial lógico del negocio.

Origen Geográfico: La procedencia de los fondos, distinguiendo entre tarjetas nacionales e internacionales.

INDICADORES DE RIESGO Y SEÑALES DE ALERTA

El monitoreo no es una vigilancia indiscriminada, sino una detección inteligente de discrepancias. Para ejecutar esta labor de manera efectiva, los agregadores tienen la flexibilidad de apoyarse en proveedores tecnológicos especializados en la materia o, en su defecto, implementar sistemas automatizados desarrollados por sus propios equipos internos.

Los sistemas de monitoreo están configurados para identificar señales de alerta o desviaciones que requieren un análisis especializado. Entre las más relevantes se encuentran:

- **Inconsistencia de Giro:** Casos donde la actividad transaccional (por ejemplo, montos muy elevados en un giro de baja transaccionalidad) no corresponde con la naturaleza económica o el sector del comercio declarado (por ejemplo, una cafetería pequeña que transacciona cientos de miles de pesos diariamente).

- **Discrepancias Geográficas:** Clientes o comercios con operación física local que comienzan a procesar un volumen inusual de pagos provenientes de jurisdicciones de alto riesgo o sin relación comercial lógica.

- **Operaciones Estructuradas:** La detección de múltiples transacciones por montos idénticos o muy similares en lapsos cortos, un patrón comúnmente asociado a intentos de evasión de controles.

- **Operatividad en Horarios Atípicos:** El registro de actividad transaccional significativa en horarios inusuales (por ejemplo, en la madrugada) que no se justifican por el tipo de servicio ofrecido.

GESTIÓN DE ALERTAS Y RESPUESTA

La activación de una alerta no implica necesariamente la existencia de una actividad ilícita, pero sí detona la responsabilidad del agregador de ejecutar una revisión. El monitoreo se vincula directamente con la gestión dinámica del riesgo.

Ante comportamientos atípicos, el protocolo estándar sugiere la reclasificación del nivel de riesgo del cliente o comercio (por ejemplo, de Bajo a Alto) y la solicitud de documentación soporte (como facturas o contratos) que acredite la legitimidad de las operaciones. Este mecanismo protege la integridad de la red de pagos y resguarda al propio cliente o comercio frente a posibles fraudes o usos indebidos de su afiliación.

A medida que la tecnología avanza, los agregadores pueden apoyarse en herramientas de análisis de datos, inteligencia artificial y automatización para detectar patrones complejos que antes podían pasar inadvertidos. Estas innovaciones no reemplazan el juicio humano, sino que lo complementan, ofreciendo mayor precisión y velocidad para proteger la integridad del sistema.

Para la ejecución efectiva del monitoreo transaccional, el agregador debe disponer de una infraestructura tecnológica robusta que permita el análisis de operaciones en tiempo real o cuasi-real. Esta infraestructura debe integrar herramientas de detección avanzadas, tales como motores de reglas (rule-based engines), modelos estadísticos para la identificación de valores atípicos (outliers) y algoritmos de machine learning supervisado, facilitando la gestión de riesgos a través de tableros de control (dashboards) operativos y la generación de alertas automáticas.

Adicionalmente, dicha infraestructura debe garantizar la trazabilidad y gobernanza del dato, asegurando el registro inalterable (logs) de cada transacción y la conservación del historial de decisiones tomadas por los analistas. Es indispensable mantener la evidencia documental de cada alerta gestionada, desde su detección hasta su dictamen final, para fines de auditoría y control interno.

El monitoreo no es una acción aislada, sino un proceso integral que implica conservar y actualizar de manera constante los datos del expediente de identificación de cada cliente o comercio para asegurar su vigencia. Esta labor conlleva la capacidad de clasificar las operaciones y productos con base en criterios de riesgo propios, permitiendo así detectar y agrupar todas las transacciones realizadas por un mismo cliente o comercio en una base consolidada que facilite su seguimiento integral. Todo este proceso debe operar bajo esquemas de seguridad que garanticen la integridad, disponibilidad, auditabilidad y confidencialidad de la información procesada.

CAPACITACIÓN INTERNA: CREANDO UNA CULTURA DE PREVENCIÓN

En el modelo de agregadores, la tecnología, los controles y los procesos estandarizados son indispensables, pero solo pueden funcionar con la correcta preparación de las personas que los operan. La integridad del ecosistema depende de colaboradores informados, competentes y conscientes del rol que desempeñan en la gestión de riesgos. Por ello, la capacitación interna es un pilar estratégico para garantizar una cultura de cumplimiento sólida, transversal y sostenible.

Los miembros de una organización responsable entienden que la prevención de PLD/FT no es responsabilidad exclusiva del área de cumplimiento, sino una función compartida entre todas las áreas que intervienen en el ciclo de vida del cliente o comercio: afiliación, ventas, atención al cliente o comercio, operaciones, monitoreo, auditoría, tecnología y alta dirección. Cada colaborador es un punto de control y una línea de defensa.

Invertir en capacitación continua significa fortalecer las capacidades técnicas de la organización, profesionalizar al equipo y demostrar responsabilidad institucional frente a adquirentes, marcas, socios financieros, autoridades y el propio sector. De esta manera, la prevención deja de ser un requisito formal y se convierte en un elemento central de la cultura organizacional.

Una cultura de prevención efectiva se construye a través de programas que:

- Sensibilizan al personal sobre la importancia de actuar con diligencia y detectar posibles riesgos.
- Homologan criterios entre áreas operativas, comerciales y directivas, para que todos hablen el mismo lenguaje de cumplimiento.
- Fomentan la participación activa, donde cada colaborador se sienta parte de la solución y no un simple ejecutor de normas.
- Concientizan sobre las posibles consecuencias y penalizaciones a las que está sujeto cada miembro de la organización en caso de no cumplir con sus responsabilidades definidas en PLD/FT.

Además, la capacitación continua ayuda a mantenerse actualizado frente a los cambios regulatorios y los desafíos digitales. Esto resulta fundamental para la mitigación de riesgos, pues a través de programas estructurados, el personal adquiere los conocimientos necesarios para identificar y gestionar las vulnerabilidades a las que se exponen los agregadores, lo cual optimiza la eficiencia del modelo de prevención.

CONTENIDO ESENCIAL: DE LA TEORÍA A LA PRÁCTICA

La capacitación debe impartirse en tres momentos clave, durante la inducción, de forma anual como proceso de actualización certificada y también de manera extraordinaria cuando surjan nuevos riesgos, incidentes internos o cambios normativos u operativos relevantes. Cada sesión debe documentarse adecuadamente para garantizar trazabilidad y mejora continua.

Un programa de capacitación robusto debe ser práctico y relevante para la operación diaria. Los temas fundamentales que se sugiere incluir son:

- **Contexto General:** Entender qué es PLD/FT y cómo los agregadores pueden ser utilizados involuntariamente para fines ilícitos.
- **Marco Regulatorio:** Revisión concisa y clara de las principales leyes y disposiciones aplicables que rigen la prevención.
- **Roles y Responsabilidades:** Delimitación clara de las funciones de cada área, asegurando que cada colaborador comprenda cuál es su nivel de responsabilidad y actuación dentro de la estructura de defensa.
- **Políticas Internas:** Un repaso de las reglas propias del agregador: cómo se hace el KYC, la revisión en listas, el EBR y el monitoreo transaccional; cuáles son los límites y por qué existen.
- **Actualización Tecnológica y Herramientas:** Entrenamiento específico (especialmente para los equipos de cumplimiento) en el uso de las plataformas de monitoreo, sistemas de validación de identidad y las nuevas herramientas tecnológicas disponibles para la detección y gestión de riesgos.
- **Identificación de Señales de Alerta:** Ejemplos reales y prácticos (tipologías) de lo que constituye una operación sospechosa en el día a día.
- **Canales de Reporte:** Instrucciones claras sobre qué hacer y a quién avisar si se detecta algo inusual, fomentando la comunicación interna sin miedo.

CAPACITACIÓN DIFERENCIADA POR ROLES Y ACTUALIZACIÓN

La capacitación interna debe adaptarse a la responsabilidad y exposición de cada rol dentro del agregador. Mientras todo el personal requiere nociones generales sobre riesgo, señales básicas de alerta, políticas internas y cultura de reporte, las áreas operativas necesitan un entendimiento más profundo de tipologías, validación documental, errores comunes y casos reales del ecosistema.

Los equipos especializados en cumplimiento, monitoreo y análisis de riesgo requieren capacitación avanzada en patrones transaccionales complejos, análisis de riesgo residual, gestión de alertas, interpretación de datos y evaluación de metodologías EBR. **A su vez, la alta dirección y los comités de riesgo deben dominar temas de apetito de riesgo, gobierno corporativo, indicadores clave y obligaciones frente a adquirentes y titulares de marca**.

Esta diferenciación permite que cada área cuente con las herramientas necesarias para cumplir con su función dentro del sistema de prevención. Asimismo, estos espacios de formación son clave para sensibilizar sobre las consecuencias tangibles del incumplimiento, reforzando el conocimiento de las posibles penalizaciones contractuales y operativas que pueden derivar de fallas en los procesos de PLD/FT.

La efectividad del programa depende de su capacidad para medir, actualizar y reforzar el conocimiento de manera continua. Para ello, es fundamental integrar evaluaciones periódicas, simulaciones, análisis de incidentes detectados por el personal y monitoreo de errores operativos recurrentes como parte del sistema de control interno.

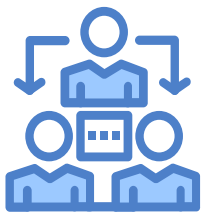
Al invertir en formación sostenida, los agregadores fortalecen su resiliencia, reducen el riesgo residual, profesionalizan a su personal y se posicionan como socios confiables dentro del ecosistema de pagos. Una cultura de prevención sólida convierte la capacitación en un activo estratégico que permea en cada decisión, proceso y transacción, consolidando al capital humano como la principal línea de defensa del modelo.

TIPOLOGÍAS: APRENDIENDO DE CASOS REALES

En el ámbito de los pagos, las tipologías son patrones comunes de comportamiento observados en casos reales de lavado de dinero o fraude. Las tipologías sirven como herramientas valiosas para reconocer señales de alerta antes de que se materialicen los riesgos. Conocer estas tipologías permite a los agregadores anticiparse a posibles vulnerabilidades y fortalecer sus mecanismos de detección.

Las tipologías ayudan a comprender cómo operan los riesgos en la práctica. Analizar casos reales, nacionales o internacionales, ofrece una perspectiva concreta sobre las estrategias que los actores ilícitos pueden intentar usar dentro de las plataformas. Este conocimiento permite identificar señales de alerta como operaciones inusuales, uso reiterado de ciertos canales, discrepancias entre el giro declarado y los movimientos reales o transacciones en zonas geográficas de riesgo.

Los agregadores deben aprovechar la existencia de las tipologías para integrarla en la creación y el ajuste de sus controles de monitoreo de afiliados. En ese sentido, las siguientes tipologías son las más representativas para el sector de agregadores, dado que exponen riesgos clave en la interacción con clientes o comercios, intermediarios y la infraestructura de pagos:



Tipología de Personas Políticamente Expuestas (PEP) UIF / GAFI[31]

- **Descripción:** Se refiere al riesgo de que funcionarios públicos, familiares o socios cercanos utilicen su influencia para desviar fondos públicos o recibir sobornos.

- **Señal de Alerta**: Una PEP (o un familiar) que opera un cliente o comercio con un volumen transaccional que no concuerda con su declaración patrimonial o con el giro del negocio, o que recibe transferencias de empresas contratistas del gobierno.

Tipología El Licenciado UIF / GAFI[32]

- **Descripción:** Involucra a abogados, contadores o consultores que actúan como intermediarios para constituir empresas o administrar cuentas, ocultando al verdadero beneficiario de los recursos.

- **Señal de Alerta:** Un despacho o consultoría que recibe fondos de múltiples orígenes inconexos y los redistribuye inmediatamente, actuando como una caja de paso sin una justificación comercial clara.

Tipología de Pitufeo o Estructuración UIF / FinCEN / UNODC / GAFI[33]

- **Descripción:** Es la técnica de dividir una gran suma de dinero ilícito en múltiples transacciones pequeñas (por debajo de los umbrales de reporte o alerta) para evitar la detección de los sistemas de monitoreo.

- **Señal de Alerta:** Un cliente o comercio que registra múltiples ventas o transferencias por montos idénticos o muy similares (por ejemplo $9,000 MXN cada 10 minutos) en un corto periodo de tiempo, utilizando diferentes tarjetas o cuentas emisoras.

Tipología de Estafa maestra versión PEMEX SAT / UIF[34]

- **Descripción:** Empresas legalmente constituidas (tienen RFC y Acta), pero que carecen de activos, personal o infraestructura real. Son utilizadas para simular operaciones comerciales y justificar el movimiento de dinero ilícito (facturación simulada).

- **Señal de Alerta:** Clientes o comercios que presentan una facturación millonaria a pocos meses de su creación, pero que no tienen sitio web, referencias comerciales visibles, ni gastos operativos (nómina, luz, agua) acordes a su volumen de ventas.

Tipología de Testaferros o Prestanombres UIF / GAFI[35]

- **Descripción:** Personas que prestan su identidad para aparecer como titulares de un negocio o cuenta, ocultando al verdadero dueño de los recursos.

- **Señal de Alerta:** Una discrepancia evidente entre el perfil socioeconómico del titular (ejemplo, un estudiante de 19 años o una persona de la tercera edad sin historial empresarial) y el alto volumen de recursos que transaccionan su cliente o comercio.

Tipología de Uso de Identidad UIF[36]

- **Descripción:** Consiste en la obtención, robo o suplantación de datos de identificación de una persona física o moral (sin su conocimiento o consentimiento) para abrir cuentas o vehículos de pago. El objetivo es crear una identidad falsa para cometer fraudes, mover recursos ilícitos de manera anónima o desviar la responsabilidad a la víctima.

- **Señal de Alerta:** El cliente (persona física o moral) inicia un proceso de alta de manera inusual o realiza una gran cantidad de transacciones a distancia. Se detectan inconsistencias en la documentación de identificación proporcionada, como el uso de documentos falsos, robados o apócrifos, o una discrepancia evidente entre el perfil socioeconómico y el volumen transaccional del cliente o comercio asociado.

En conjunto, las tipologías permiten a los agregadores alinear sus políticas internas con los estándares internacionales y adoptar una visión preventiva y proactiva, en la que el conocimiento de patrones delictivos conocidos se traduzca en mejores controles internos, detección temprana de operaciones inusuales y comunicación efectiva con las autoridades competentes.

31.- Secretaría de Hacienda y Crédito Público. (2022). Tipología PEPS. Gobierno de México. https://www.gob.mx/cms/uploads/attachment/file/873339/Tipologia_PEPS.pdf
32.- Secretaría de Hacienda y Crédito Público. (2021). Tipología: Licenciado. Gobierno de México. Gobierno de México. https://www.gob.mx/cms/uploads/attachment/file/708610/tipologia_licenciado.pdf
33.- Financial Action Task Force on Money Laundering FATF. (1998). Fatf-Ix Report on Money Laundering Typologies. Financial Crimes Enforcement Network. https://www.fincen.gov/financial- action-task-force-money-laundering-fatf
34.- Secretaría de Hacienda y Crédito Público. (2020). Estafa Maestra – Informe Pemex. Gobierno de México. https://www.gob.mx/cms/uploads/attachment/file/708601/EstafaMaestra_Pemex.pdf
35.- Grupo de Acción Financiera de Latinoamérica. (2024). Informe de tipologías regionales de LA/FT 2019-2020. Biblioteca GAFILAT. https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Informe-de- Tipologias-Regionales-de-LA-2019-2020-GAFILAT.pdf
36.- Secretaría de Hacienda y Crédito Público. (2009). Tipologías UIF México. Gobierno de México. https://www.gob.mx/cms/uploads/attachment/file/194184/Tipologias_UIF_Mexico.pdf

CONCLUSIÓN: LIDERAZGO Y RESPONSABILIDAD EN LA NUEVA ERA DE PAGOS

El crecimiento del ecosistema de pagos en México demanda que los agregadores ejerzan un liderazgo responsable en la gestión de riesgos y en la prevención de PLD/FT. La innovación solo puede prosperar cuando está acompañada de integridad operativa, disciplina técnica y controles proporcionales. Esta guía sintetiza el compromiso del gremio por adoptar estándares internacionales, fortalecer la autorregulación y consolidar una cultura institucional que privilegie la transparencia, la diligencia y la protección del sistema financiero. Al profesionalizar los procesos de identificación, revisión en listas negras, evaluación de riesgos, monitoreo transaccional y capacitación, los agregadores se posicionan no solo como actores tecnológicos, sino como instituciones clave en la estabilidad del ecosistema.

El futuro del sector dependerá de la capacidad colectiva de mantener este equilibrio entre eficiencia e integridad. Cada agregador que adopta y ejecuta estas mejores prácticas contribuye a reducir riesgos sistémicos, fortalece la confianza entre adquirentes, titulares de marca, clientes o comercios y autoridades, y consolida un entorno más seguro e inclusivo. La ASAMEP reafirma su liderazgo como articuladora de esta visión y como promotora de un desarrollo responsable del sector, impulsando un ecosistema de pagos donde la innovación y la prevención avanzan juntas para construir un mercado sostenible y confiable.

asociación
de agregadores
de medios
de pago a.c.

Guía de Mejores Prácticas de Agregadores en la Prevención de Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT) 2025