Política y procedimientos para la prevención de lavado de dinero y financiamiento al Terrorismo.

International Mobile Services.

Fecha de emisión: 26 de marzo del 2026.

Versión 2.1.

Aprobado por Gerencial General.

1.) Objetivo.

Establecer directrices y procedimientos para prevenir el lavado de dinero y el financiamiento al terrorismo, garantizando el cumplimiento de las normativas nacionales e internacionales aplicables y protegiendo la integridad y reputación de la empresa.

2.) Alcance.

Esta política se aplica a todos los empleados, directivos, contratistas, socios comerciales, y cualquier otra persona que interactúe con la empresa o tenga acceso a recursos financieros y transacciones.

3.) Principios Rectores.

- Cumplimiento Legal y Regulatorio: La empresa se compromete a cumplir con todas las leyes locales e internacionales relativas a la prevención de lavado de dinero y financiamiento al terrorismo.
- Debida Diligencia: Implementar procedimientos adecuados para conocer a nuestros clientes, proveedores y socios, con el fin de prevenir el uso indebido de los servicios o productos de la empresa para actividades ilícitas.
- Transparencia y Ética: Fomentar una cultura de transparencia y ética empresarial, asegurando que todos los colaboradores actúen con responsabilidad y cumplan con los estándares de integridad.

4.) Definiciones.

- Lavado de Dinero: Proceso de ocultar o disfrazar el origen ilícito de fondos obtenidos a través de actividades criminales, con el fin de hacer que parezcan legítimos.
- Financiamiento al Terrorismo: Proceso de proporcionar fondos o recursos a organizaciones o personas involucradas en actividades terroristas.
- Debida Diligencia: Procedimientos que se aplican para verificar la identidad y el perfil de los clientes o socios comerciales, a fin de prevenir la participación en actividades ilícitas.

5.) Política de Prevención de Lavado de Dinero y Financiamiento al Terrorismo.

a.) Conozca a su Cliente (KYC)

IMS llevará a cabo procedimientos de Conozca a su Cliente (KYC, por sus siglas en inglés) para verificar la identidad de los clientes, proveedores, y socios comerciales.
Esta verificación incluirá la revisión de documentos oficiales de identificación, registros financieros y antecedentes legales, si corresponde.

b.) Monitoreo de Transacciones

Todas las transacciones financieras realizadas por los clientes, empleados y terceros serán monitoreadas para detectar actividades sospechosas o inusuales, que podrían indicar lavado de dinero o financiamiento al terrorismo.
Cualquier transacción que no coincida con el perfil del cliente será investigada más a fondo y se tomará una acción adecuada.

c.) Debida Diligencia Reforzada

En situaciones donde se identifiquen clientes de alto riesgo (por ejemplo, clientes provenientes de países con altos índices de corrupción o sancionados por organismos internacionales), se aplicarán procedimientos de debida diligencia más estrictos para verificar la fuente de los fondos y la legitimidad de las actividades.

d.) Capacitación y Sensibilización

Todos los empleados recibirán capacitación periódica sobre la prevención de lavado de dinero y financiamiento al terrorismo, incluyendo cómo identificar señales de alerta y qué hacer en caso de sospechas.

La capacitación también incluirá las políticas internas y los procedimientos a seguir en caso de detectar transacciones o actividades sospechosas.

6.) Prohibiciones sobre el Lavado de Dinero

La organización establece una política de cero tolerancia frente a cualquier conducta relacionada con el lavado de dinero o activos, así como con el financiamiento al terrorismo.

En consecuencia, queda estrictamente prohibido:

- Participar, directa o indirectamente, en cualquier actividad, operación o transacción que tenga como finalidad ocultar, encubrir, transformar o dar apariencia de legalidad a recursos de procedencia ilícita.
- Ocultar, encubrir, transferir, adquirir, administrar, custodiar o utilizar bienes o recursos cuando se tenga conocimiento, sospecha o indicios razonables de que provienen de actividades ilícitas.
- Facilitar, permitir o tolerar el uso de la organización, sus operaciones, productos o servicios como medio para el ingreso, manejo o circulación de recursos de origen ilícito.
- Realizar o continuar relaciones comerciales con personas físicas o jurídicas cuando existan indicios razonables de su vinculación con actividades ilícitas o cuando no sea posible verificar adecuadamente el origen de sus recursos.
- Fraccionar, estructurar o modificar operaciones con el propósito de evadir controles internos, umbrales regulatorios o mecanismos de reporte establecidos por la normativa aplicable.

- Proporcionar información falsa, incompleta o engañosa, o bien omitir información relevante con el fin de evitar la detección de operaciones inusuales o sospechosas.
- Ignorar señales de alerta, omitir reportes internos o incumplir con los procedimientos establecidos para la identificación y comunicación de operaciones inusuales.
- Participar, directa o indirectamente, en cualquier forma de financiamiento al terrorismo, incluyendo la provisión, recolección, canalización o administración de recursos con dicho propósito.
- Tomar represalias contra cualquier persona que, de buena fe, reporte actividades sospechosas o posibles incumplimientos a la presente política.

El incumplimiento de cualquiera de estas disposiciones será considerado una falta grave y dará lugar a la aplicación de medidas disciplinarias conforme a la normativa interna de la organización, sin perjuicio de las responsabilidades administrativas, civiles o penales que puedan derivarse conforme a la legislación aplicable.

7.) <u>Identificación de Actividades Vulnerables</u>

La organización llevará a cabo análisis periódicos, sistemáticos y documentados con el fin de identificar si alguna de sus operaciones, productos, servicios o relaciones comerciales puede ser considerada como una Actividad Vulnerable, de conformidad con la legislación aplicable en materia de prevención de lavado de dinero y financiamiento al terrorismo.

Dicho análisis deberá considerar, entre otros factores:

- La naturaleza de los productos o servicios ofrecidos.
- El tipo de clientes o contrapartes.
- Los montos, frecuencia y características de las operaciones.
- Las zonas geográficas en las que se opera.
- Los canales de distribución o comercialización utilizados.

Como resultado de este análisis, la organización clasificará sus actividades conforme a su nivel de exposición al riesgo y documentará las conclusiones en los instrumentos correspondientes (matriz de riesgo, dictamen, entre otros).

En caso de identificarse actividades vulnerables, la organización deberá implementar controles y medidas específicas, incluyendo, de manera enunciativa mas no limitativa:

- Identificación y Conocimiento del Cliente (KYC):
  Recopilación, verificación y actualización de la información y documentación de clientes, usuarios y beneficiarios finales.
- Integración y Resguardo de Expedientes:
  Conformación de expedientes completos, veraces y actualizados, asegurando su adecuada conservación y disponibilidad conforme a los plazos legales aplicables.
- Clasificación y Perfilamiento de Riesgo:
  Evaluación del nivel de riesgo de clientes y operaciones, aplicando medidas de debida diligencia acordes a dicho nivel.
- Monitoreo de Operaciones:
  Supervisión continua de las transacciones para detectar comportamientos inusuales o inconsistentes con el perfil del cliente.
- Identificación de Señales de Alerta:
  Implementación de mecanismos para detectar posibles operaciones inusuales o sospechosas.
- Presentación de Avisos a Autoridades:
  Cumplimiento oportuno de las obligaciones de reporte ante las autoridades competentes, cuando así lo establezca la normativa aplicable.
- Capacitación del Personal:
  Formación continua de los colaboradores involucrados en la ejecución de actividades vulnerables.

- Controles Internos Adicionales:
  Implementación de políticas, procedimientos y controles reforzados proporcionales al nivel de riesgo identificado.

La organización revisará y actualizará de manera periódica este análisis, o cuando ocurran cambios relevantes en sus operaciones, entorno regulatorio o perfil de riesgo, con el fin de asegurar su vigencia y efectividad.

8.) <u>Declaración de Cumplimiento Normativo</u>

La organización manifiesta su firme compromiso con el cumplimiento de todas las leyes, reglamentos y disposiciones aplicables en materia de prevención, detección y, en su caso, reporte y coadyuvancia en la persecución de los delitos de lavado de dinero o activos, así como del financiamiento al terrorismo.

En este sentido, la organización actuará en estricto apego a la normativa vigente en las jurisdicciones donde opera, implementando los controles, mecanismos y procedimientos necesarios para prevenir el uso de sus operaciones, productos o servicios con fines ilícitos.

Asimismo, se compromete a colaborar de manera oportuna, transparente y conforme a derecho con las autoridades competentes, atendiendo requerimientos de información, reportes regulatorios y cualquier obligación legal que derive de la materia.

Todos los colaboradores, directivos y terceros relacionados con la organización deberán cumplir con las disposiciones establecidas en esta política y en la legislación aplicable, siendo responsables de actuar con diligencia, integridad y apego a la legalidad.

El incumplimiento de estas obligaciones podrá dar lugar a sanciones internas, sin perjuicio de las responsabilidades administrativas, civiles o penales que correspondan conforme a la ley.

9.) Procedimientos para la prevención de lavado de Dinero y financiamiento al Terrorismo.

10.) Identificación de Riesgos.

a. La empresa realizará evaluaciones periódicas para identificar riesgos asociados con lavado de dinero y financiamiento al terrorismo. Este proceso incluirá la revisión de la naturaleza de las actividades comerciales, la localización geográfica de los clientes y proveedores, y el tipo de transacciones realizadas.

11.) Monitoreo Continuo.

a. Todas las transacciones financieras serán monitoreadas continuamente para identificar patrones inusuales. Se utilizarán herramientas automatizadas para la detección temprana de actividades sospechosas.

b. Los empleados serán entrenados para identificar indicadores de lavado de dinero o financiamiento al terrorismo, como transacciones de grandes sumas sin justificación o cambios repentinos en el comportamiento financiero de un cliente.

12.) **Reporte de Actividades Sospechosas.**

a. En caso de detectar una actividad sospechosa, los empleados deben reportarla inmediatamente.

b. Si se confirma que la actividad es sospechosa, se reportará a las autoridades pertinentes de acuerdo con las leyes locales.

13.) **Auditorías Internas.**

a. Se realizarán auditorías internas periódicas para evaluar la efectividad de los procedimientos de prevención de lavado de dinero y financiamiento al terrorismo. Las auditorías también verificarán el cumplimiento de las políticas y la implementación de acciones correctivas cuando sea necesario.

14.) **Colaboración con Autoridades.**

a. La empresa cooperará plenamente con las autoridades competentes en investigaciones relacionadas con lavado de dinero o financiamiento al terrorismo y proporcionará toda la información necesaria para cumplir con las regulaciones.

15.) **Confidencialidad y Protección.**

a. Se garantizará la confidencialidad de cualquier información obtenida durante el proceso de debida diligencia y el reporte de actividades sospechosas. No habrá represalias para aquellos que denuncien de buena fe posibles actividades ilícitas.

16.) <u>Análisis de Enfoque Basado en Riesgo</u>

La organización adoptará un enfoque basado en riesgo para la prevención del lavado de dinero y financiamiento al terrorismo, mediante la identificación, evaluación, mitigación y monitoreo continuo de los riesgos asociados a sus operaciones.

Para tal efecto, se desarrollarán y mantendrán actualizados, de manera enunciativa mas no limitativa, los siguientes instrumentos:

- Un Dictamen de Riesgo, que documente el nivel de exposición de la organización.
- Una Matriz de Riesgos, que permita evaluar y clasificar los factores de riesgo relevantes.
- Un Manual de Procedimientos, que establezca los controles y procesos operativos en la materia.
- Una Metodología de Evaluación, que defina los criterios y parámetros para la medición del riesgo.
- Esquemas de Debida Diligencia diferenciados conforme al nivel de riesgo identificado.

Los resultados del análisis de riesgo deberán ser revisados periódicamente y aprobados por la alta dirección, asegurando la implementación de controles proporcionales al nivel de exposición identificado.

17.) <u>Medidas Preventivas en materia de Lavado de Dinero y Financiamiento al Terrorismo</u>

La organización implementará medidas preventivas razonables, proporcionales y basadas en riesgo, con el objetivo de evitar que sus operaciones, productos o servicios sean utilizados para el lavado de dinero o el financiamiento al terrorismo.

Dichas medidas incluyen, de manera enunciativa mas no limitativa, las siguientes:

a.) Identificación y Conocimiento del Cliente (KYC)

- Recopilación y verificación de información y documentación de clientes, proveedores y terceros.
- Identificación del beneficiario final.
- Integración y resguardo de expedientes conforme a la normativa aplicable.

b.) Clasificación de Riesgo

- Evaluación y clasificación de clientes y operaciones en niveles de riesgo (bajo, medio, alto).
- Aplicación de controles diferenciados conforme al nivel de riesgo identificado.

c.) Debida Diligencia

- Aplicación de procesos de debida diligencia simplificada, estándar o reforzada, según corresponda.
- Validación de información mediante fuentes confiables.
- Revisión de antecedentes y reputación.

d.) Monitoreo de Operaciones

- Supervisión continua de las operaciones realizadas.
- Identificación de patrones inusuales o inconsistentes con el perfil del cliente.
- Generación de alertas internas para su análisis.

e.) Listas Restrictivas y Personas de Riesgo

- Verificación contra listas nacionales e internacionales de sanciones y personas bloqueadas.
- Identificación de Personas Políticamente Expuestas (PEP) y aplicación de controles reforzados.

f.) Reporte de Operaciones

- Establecimiento de mecanismos internos para el reporte de operaciones inusuales o sospechosas.
- Cumplimiento de las obligaciones de reporte ante las autoridades competentes, cuando aplique.

18.) Metodología de Implementación y Verificación de Cumplimiento

La organización establecerá una metodología estructurada para la implementación, seguimiento y verificación del cumplimiento de la presente política en materia de prevención de lavado de dinero y financiamiento al terrorismo.

a.) Implementación

La implementación de la política se llevará a cabo mediante:

- La elaboración y difusión de procedimientos internos alineados con esta política.
- La asignación de responsabilidades claras a las áreas y colaboradores involucrados.
- La integración de controles en los procesos operativos, comerciales y administrativos.
- La adopción de herramientas y mecanismos para la identificación, evaluación y monitoreo de riesgos.
- La capacitación inicial y periódica del personal en materia de prevención de lavado de dinero y financiamiento al terrorismo.

b.) Verificación de Cumplimiento

La organización realizará actividades de supervisión continua para asegurar el cumplimiento efectivo de la política, incluyendo:

- Revisiones periódicas de los procesos y controles establecidos.
- Evaluaciones del cumplimiento por parte de las áreas responsables.
- Monitoreo de indicadores clave relacionados con riesgos y cumplimiento.
- Validación del adecuado funcionamiento de los mecanismos de identificación, monitoreo y reporte.

c.) Auditoría y Evaluación Independiente

Cuando resulte aplicable, se llevarán a cabo auditorías internas o externas para evaluar la efectividad de los controles implementados y el grado de cumplimiento de la normativa aplicable.

Las observaciones derivadas de dichas auditorías deberán ser atendidas mediante planes de acción específicos.

d.) Gestión de Incumplimientos

Cualquier incumplimiento detectado deberá ser documentado, analizado y gestionado de manera oportuna, incluyendo:

- La implementación de medidas correctivas.
- El establecimiento de acciones preventivas para evitar su recurrencia.
- La aplicación de sanciones internas, cuando corresponda.

e.) Mejora Continua

La organización mantendrá un enfoque de mejora continua, revisando y actualizando periódicamente la política, los procedimientos y los controles, con el fin de adaptarlos a cambios regulatorios, operativos o de riesgo.

19.) Prohibición de Actividades Precedentes al Lavado de Dinero

La organización prohíbe de manera expresa cualquier conducta, acto u omisión que implique la participación directa o indirecta en actividades ilícitas que puedan constituir delitos precedentes al lavado de dinero, tales como fraude, corrupción, evasión fiscal, soborno, tráfico ilícito u otras actividades contrarias a la ley.

En consecuencia:

- Ningún colaborador, directivo o tercero podrá participar en operaciones que involucren recursos de procedencia ilícita o cuyo origen no pueda ser razonablemente justificado.
- Se prohíbe facilitar, encubrir o tolerar actividades que puedan dar origen a recursos ilícitos.
- La organización evitará establecer relaciones comerciales con personas físicas o jurídicas cuando existan indicios razonables de su vinculación con actividades ilícitas.

- Se deberán aplicar medidas de debida diligencia para prevenir la incorporación de recursos provenientes de actividades ilegales.

Cualquier incumplimiento a esta disposición será considerado una falta grave y podrá dar lugar a sanciones internas, así como a las acciones legales correspondientes ante las autoridades competentes.

20.) <u>Estructura de Prevención.</u>

La organización establecerá una estructura interna adecuada para la gestión y supervisión del cumplimiento en materia de prevención de lavado de dinero y financiamiento al terrorismo, basada en la asignación clara de responsabilidades y en la implementación de líneas de control efectivas.

Dicha estructura incluirá, de manera enunciativa mas no limitativa:

a.) Alta Dirección

- Aprobar la política y sus actualizaciones.
- Definir la estrategia y el nivel de tolerancia al riesgo.
- Asegurar la asignación de recursos necesarios para su implementación.

b. Responsable de Cumplimiento (Oficial o Área)

- Supervisar la correcta implementación de la política y procedimientos.
- Coordinar la identificación, evaluación y monitoreo de riesgos.
- Recibir y analizar reportes de operaciones inusuales o sospechosas.
- Fungir como enlace con autoridades, cuando corresponda.

c. Áreas Operativas

- Ejecutar los procesos de identificación, debida diligencia y monitoreo.
- Detectar y reportar señales de alerta.
- Cumplir con los procedimientos establecidos.

d. Auditoría Interna (cuando aplique)

- Evaluar la efectividad de los controles implementados.
- Verificar el cumplimiento de la política y la normativa aplicable.

- Emitir recomendaciones y dar seguimiento a planes de acción.

e. Todos los Colaboradores

- Cumplir con esta política y la normativa aplicable.
- Participar en las capacitaciones.
- Reportar cualquier actividad sospechosa o incumplimiento detectado.

La estructura de prevención deberá ser proporcional al tamaño, complejidad y nivel de riesgo de la organización, garantizando en todo momento la independencia, objetividad y eficacia de las funciones de control.

21.) Consecuencias por Incumplimiento.

El incumplimiento de esta política y procedimientos puede resultar en medidas disciplinarias, incluyendo la terminación del contrato de empleo, así como sanciones legales según las leyes locales e internacionales.

22.) Revisión y Actualización de la Política.

Esta política será revisada de manera regular y actualizada en función de los cambios legislativos, las mejores prácticas y los resultados de las auditorías internas. La política también se ajustará conforme a nuevas normativas o tendencias emergentes en la prevención de lavado de dinero y financiamiento al terrorismo.

23.) Capacitación y Difusión

La organización garantizará la adecuada difusión y comprensión de la presente política, así como de las obligaciones en materia de prevención de lavado de dinero y financiamiento al terrorismo.

Para ello:

- Se comunicará la política a todos los colaboradores, directivos y terceros relevantes, asegurando su disponibilidad permanente.
- Se impartirán programas de capacitación inicial y periódica, adaptados al nivel de responsabilidad y exposición al riesgo de cada puesto.
- Las capacitaciones incluirán, entre otros temas, la identificación de señales de alerta, procedimientos internos, obligaciones legales y consecuencias del incumplimiento.
- Se mantendrán registros de asistencia, evaluaciones y evidencias de las capacitaciones impartidas.
- Se promoverá una cultura organizacional basada en la ética, la legalidad y la prevención de riesgos.

24.) Régimen Sancionador

El incumplimiento de la presente política, de los procedimientos asociados o de la normativa aplicable en materia de prevención de lavado de dinero y financiamiento al terrorismo será considerado una falta grave.

- Se aplicarán medidas disciplinarias proporcionales a la gravedad de la falta, las cuales podrán incluir amonestaciones, suspensiones, terminación de la relación laboral o contractual, entre otras.
- Las sanciones se impondrán sin perjuicio de las responsabilidades administrativas, civiles o penales que pudieran derivarse conforme a la legislación aplicable.
- Se considerará como agravante el ocultamiento de información, la reincidencia o la participación intencional en conductas ilícitas.
- El proceso sancionador deberá garantizar criterios de objetividad, confidencialidad y debido proceso.

25.) Canal de Denuncia

La organización contará con mecanismos formales, accesibles y confidenciales para la recepción de denuncias relacionadas con posibles incumplimientos de esta política o con actividades sospechosas.

Dichos mecanismos deberán:

- Permitir el reporte anónimo o identificado de conductas indebidas.
- Garantizar la confidencialidad de la información y la protección de los datos del denunciante.
- Prohibir cualquier tipo de represalia contra las personas que reporten de buena fe.
- Establecer procedimientos claros para la recepción, análisis, investigación y seguimiento de las denuncias.
- Asegurar que las denuncias sean atendidas de manera oportuna y documentada.

Las denuncias se pueden realizar en el enlace: https://www.ims.do/denuncias/page.html

26.) Supervisión y Verificación.

La organización implementará mecanismos de supervisión y control con el fin de asegurar el cumplimiento efectivo de la presente política y la adecuada gestión de los riesgos asociados.

- Se realizarán revisiones periódicas de los procesos, controles y procedimientos establecidos.
- Se evaluará el cumplimiento por parte de las distintas áreas y colaboradores.
- Se monitorearán indicadores clave de riesgo y cumplimiento.
- Se podrán llevar a cabo auditorías internas y, en su caso, externas para verificar la efectividad del sistema de prevención.
- Se dará seguimiento a las observaciones, hallazgos y recomendaciones, mediante la implementación de planes de acción correctivos.

- La política y los controles asociados serán revisados y actualizados de manera periódica o cuando existan cambios relevantes en el entorno regulatorio o en el perfil de riesgo de la organización.

Este documento es aprobado por la Gerencial General de IMS.

CARLOS LUIS POLONIO LOBO (FIRMA)

Digitally signed by CARLOS LUIS POLONIO LOBO (FIRMA)
Date: 2026.04.08 17:20:39 -06'00'

Nombre: Carlos Luis Polonio Lobo.

Cargo: Gerente General

International Mobile Services

Fecha: 26 de marzo del 2026.