Manual de Prevención de Lavado de Activos, Financiamiento del Terrorismo y de la Proliferación

CryptoSwap SpA

Inscripción CMF N° · UAF N°
Versión: 2026-05-06 · Próxima revisión: cada 24 meses

1. Marco normativo aplicable

El presente Manual da cumplimiento a la normativa chilena vigente en materia de prevención de lavado de activos (LA), financiamiento del terrorismo (FT) y financiamiento de la proliferación de armas de destrucción masiva (FP):

• Ley N° 19.913 — Ley que crea la Unidad de Análisis Financiero (UAF) y tipifica el delito de lavado de activos.

• Ley N° 21.521 (Ley Fintech) — Incorpora a los prestadores de servicios financieros como sujetos obligados.

• NCG N° 502 (CMF, 2024) — Norma de carácter general sobre registro, autorización y gobierno corporativo.

• Circular N° 62 (UAF, 2025) — Instrucciones generales de prevención LA/FT/FP. Reemplaza la Circular 49/2012.

2. Política institucional

El Operador adopta una política de tolerancia cero ante la utilización de sus servicios para actividades ilícitas. Esta política incluye:

• Conocimiento exhaustivo del cliente (KYC y KYB) antes de iniciar la relación comercial.

• Aplicación del Enfoque Basado en Riesgo (EBR) sobre cada cliente y operación.

• Monitoreo continuo de operaciones con detección automática de patrones sospechosos.

• Capacitación anual obligatoria del personal con acceso a clientes y operaciones.

• Designación de un Oficial de Cumplimiento de alta dirección con acceso a todos los registros.

3. Designación del Oficial de Cumplimiento

Se designa como Oficial de Cumplimiento a:

El Oficial de Cumplimiento tiene acceso completo a operaciones, registros y sistemas, depende directamente del directorio o gerencia general, y reporta de forma autónoma a la UAF.

4. Enfoque Basado en Riesgo (EBR)

Conforme al Capítulo III de la Circular 62, el Operador implementa un EBR que evalúa cuatro factores:

Factor Cliente: tipo de persona (natural/jurídica), actividad económica, origen de fondos, condición PEP, coherencia perfil/volumen, complejidad societaria.

Factor Producto/Servicio: criptoactivos (riesgo inherente elevado por pseudo-anonimato).

Factor Canal: operaciones 100% digitales no presenciales (riesgo medio-alto).

Factor Geográfico: jurisdicción del cliente y contraparte según listas GAFI.

5. Conocimiento del cliente — KYC personal

Previo a habilitar al cliente para operar, se recopilan y verifican:

• Identificación: nombre completo, RUT, fecha de nacimiento, nacionalidad, documento de identidad (cédula o pasaporte).

• Verificación biométrica: prueba de vida (selfie con gestos) y comparación con foto del documento.

• Declaración de Persona Expuesta Políticamente (PEP), incluyendo familiares hasta 2° grado y asociados cercanos.

• Declaración de origen lícito de fondos y propósito de la relación comercial.

• Confirmación de no ser ciudadano(a) ni residente fiscal de los Estados Unidos.

• Aceptación expresa de Términos, Política de Privacidad y declaración AML/CFT.

6. Conocimiento de la empresa — KYB

Para empresas, se aplica un proceso de verificación en seis etapas:

1. Información básica: razón social, RUT, tipo de sociedad, fecha de constitución, actividad tributaria.

2. Documentos de verificación: escritura de constitución, certificado de vigencia, e-RUT SII, poder.

3. Dirección: estructura completa con comuna y región.

4. Prueba de dirección: comprobante de no más de 3 meses (servicios, bancario, notarial).

5. Beneficiarios finales: personas naturales con ≥10% de participación o control efectivo (Circular 62).

6. Perfil transaccional: volumen, frecuencia, monto promedio, países contraparte, propósito.

7. Niveles de Debida Diligencia

Simplificada — Riesgo bajo: identificación básica + monitoreo estándar.

Estándar — Riesgo medio: identificación completa, verificación documental, declaraciones, beneficiario final.

Reforzada (EDD) — Riesgo alto (PEP, GAFI, estructuras complejas): verificación intensificada, documentación de origen de fondos, aprobación expresa de gerencia, monitoreo continuo con umbrales reducidos.

8. Umbrales y obligaciones de reporte

≥ **USD 1,000** — Travel Rule: identificación de ordenante y beneficiario en transferencias de criptoactivos.

≥ **USD 3,000** — DDC completa + identificación de beneficiario final en operaciones ocasionales.

≥ **USD 10,000** — Reporte de Operación en Efectivo (ROE) a la UAF.

Sin umbral — Reporte de Operación Sospechosa (ROS) ante cualquier patrón inusual.

9. Monitoreo transaccional automatizado

El sistema genera alertas automáticas ante:

• Fraccionamiento (pitufeo): múltiples operaciones pequeñas en plazo corto.

• Inconsistencia de perfil: volumen real que excede 1.5x el declarado.

• Picos de volumen: operación que supera 3x el promedio histórico.

• Wallets compartidas: misma dirección de destino en distintos clientes.

• Jurisdicciones de alto riesgo: operaciones desde/hacia listas GAFI.

10. Screening contra listas de sanciones

Antes de aprobar a un cliente y al detectar alertas, se realiza screening automático contra:

• OFAC (Office of Foreign Assets Control, EE.UU.)

• Listas de sanciones de la ONU (Consejo de Seguridad)

• Listas de sanciones de la Unión Europea

• Lista negra y gris GAFI/FATF

Coincidencias confirmadas resultan en rechazo automático y bloqueo de la cuenta.

11. Conservación de registros (5 años)

Todos los registros relacionados con identificación de clientes, operaciones, reportes internos y alertas de compliance se conservan por un mínimo de 5 años desde la fecha de la última operación o cierre de la relación comercial. Se mantienen los siguientes registros permanentes:

• Registro de Operaciones en Efectivo (ROE).

• Registro de Operaciones Sospechosas (ROS).

• Registro de Debida Diligencia de Clientes (DDC).

• Registro de Personas Expuestas Políticamente (PEP).

• Registro de Transferencias Electrónicas (Travel Rule).

12. Capacitación

Todo el personal con acceso a datos de clientes y operaciones recibe capacitación anual obligatoria sobre:

• Tipologías de LA/FT/FP relevantes para criptoactivos.

• Detección de operaciones sospechosas.

• Obligaciones de reporte (ROE, ROS) y uso del Portal de Entidades Reportantes UAF.

• Actualización normativa (Circular 62, NCG 502, Ley 21.521).

Los registros de capacitación se conservan por 5 años.

13. Canales de denuncia

El Operador mantiene un canal confidencial y anónimo de denuncias, accesible desde el portal web. Cualquier persona —cliente, empleado, tercero— puede reportar sospechas de operaciones ilícitas, conflictos de interés, abuso de autoridad, fraude o incumplimiento normativo. Las denuncias son revisadas por el Oficial de Cumplimiento y, en caso de involucrar LA/FT/FP, elevadas como ROS a la UAF.

14. Revisión y aprobación

Este Manual debe ser revisado y aprobado al menos cada 24 meses por el directorio o gerencia general. Cualquier modificación regulatoria que afecte la operación obliga a su actualización inmediata.

Aprobado por: (Oficial de Cumplimiento)

Fecha de emisión: 06-05-2026

Documento generado automáticamente por el sistema de compliance de CryptoSwap SpA. Disponible para inspección de UAF y CMF.