CCP CONSULTORES
Manual de Prevención de Riesgos LC/FT/FPADM

1) **Alcance y objetivo**

- **Alcance:** Este manual aplica a todas las operaciones comerciales y relaciones con clientes, proveedores y contrapartes que intervienen en ventas de propiedades, diseño y construcción, así como en servicios relacionados en CCP Consultores. Incluye procesos de identificación, verificación de identidad (KYC), evaluación de riesgos, aprobación formal, divulgación y desarrollo de controles permanentes.
- **Objetivo:** Prevenir, detectar y reportar operaciones de lavado de dinero, financiamiento del terrorismo y otras actividades ilícitas; asegurar el cumplimiento con la normativa aplicable (Ley Antilavado, normativas de conocimiento del cliente, reportes de operaciones sospechosas y demás disposiciones nacionales e internacionales pertinentes).

2) **Definiciones clave**

- **LC/FT/FPADM:** Normativas y controles para prevenir Lavado de Dinero (LD), Financiamiento del Terrorismo (FT) y otras actividades ilícitas en la administración de fondos y operaciones comerciales. Incluye Ley Antilavado, normas KYC/Conozca a su Cliente, KYC empresarial, reportes de operaciones sospechosas (ROS), procedimientos de debida diligencia y trazabilidad de fondos.
- **Cliente de alto riesgo (CAR):** Cliente o relación que presenta pruebas o circunstancias que aumentan el riesgo de LD/FT, por ejemplo, estructuras complejas, pagos en efectivo inusuales, jurisdicciones de alto riesgo, falta de información verificada.
- **Conozca a su Cliente (KYC):** Proceso de verificación de identidad, antecedentes, y evaluación de la adecuación de la relación comercial.
- **Conozca su negocio (KYC empresarial):** Debida diligencia sobre la naturaleza de la empresa cliente, su estructura, objetivo de negocio, fuente de fondos y control interno.
- **Existencia (Identidad y verificación):** Verificación de identidad de individuos y entidades, trazabilidad de fondos y origen de recursos.
- **Aprobación formal:** Aprobación documentada de operaciones y/o relaciones comerciales por la autoridad correspondiente dentro de la empresa (firma digital o física).
- **Divulgación:** Reporte y comunicación a autoridades/reguladores y archivos internos, conforme a plazos y criterios establecidos.

3) **Estructura de control: Existencia (Identidad y verificación)**

- Descripción general: Controles para asegurar que toda relación comercial u operación tenga identidad verificada y trazabilidad de fondos antes de avanzar. -Componentes clave:
    - Verificación de identidad (persona física o jurídica).

- Verificación de documentos y procedencia de fondos.
- Detección de alertas KYC/AML en terceros y contrapartes.
- Registro de datos de identificación y trazabilidad.

4) **Estructura de control: Aprobación formal**

4.1 Roles y responsabilidades

- **Responsable de cumplimiento (Compliance Officer):** Diseñar, implementar y supervisar el programa de LC/FT/FPADM; coordinar evaluaciones de riesgo; gestionar reportes y respuestas ante autoridades.
- **Gerente de ventas/Proyectos:** Supervisión de la relación comercial, revisión de perfiles de cliente y aprobación previa a operaciones relevantes.
- **Supervisor de obra/diseño:** Verificación de proyectos y contratos desde la perspectiva de riesgo; colaboración en la verificación de identidad y trazabilidad.
- **Equipo financiero:** Verificación de trazabilidad de fondos, monitoreo de transacciones y soporte en aprobaciones financieras.

4.2 **Proceso de aprobación**

- Paso 1: **Clasificación de riesgo del cliente/operación**. Determinar nivel (bajo, medio, alto) según perfil, jurisdicción, fuente de fondos y propósito de la operación.
- Paso 2: **Revisión de KYC y trazabilidad de fondos.** Verificar identidad, documentos, estructura societaria, origen de fondos y flujo de capitales.
- Paso 3: **Aprobación por autoridad competente dentro de la empresa** (firma digital o física). Resolver y registrar aprobación de la operación o apertura de relación.
- Paso 4: **Registro de la decisión y notas de justificación**. Archivo documental con criterios de clasificación, evidencia y razonamiento.

5. Estructura de control: Divulgación

5.1 **Reporte de operaciones sospechosas (ROS)**

- **Criterios para determinar una operación sospechosa:**
  - Transacciones inusuales o inconsistentes con el perfil del cliente (volumen, frecuencia, cambios abruptos).
  - Estructuras complejas o uso de terceros para ocultar la información de beneficial ownership.
  - Originación de fondos fuera de la actividad declarada o sin fuente verificable.
  - Pagos en efectivo inusuales o repetidos que exceden umbrales establecidos.
  - Violación de procedimientos KYC/EDD, o intento de evadir controles.
  - Relación con jurisdicciones de alto riesgo o sancionadas.
  - Modificaciones repetidas en contratos o de fecha límite que dificultan trazabilidad.
- **Canales internos para reportar:**
  - Equipo de Compliance (oficina de cumplimiento).

        - Línea Directa de denuncia o buzón seguro.
        - Supervisor de ventas/proyectos cuando identifique indicios en relación comercial.
    - **Plazos de reporte a las autoridades competentes:**
        - ROS inmediato o “a la brevedad razonable” tras la detección de indicios.
        - Informe formal a la autoridad competente dentro de los plazos legales aplicables en Costa Rica (según normativa local, típicamente dentro de 24–72 horas desde la detección, según la regulación vigente).
        - Si aplica, notificación adicional y envío de documentación de respaldo dentro del plazo establecido por la autoridad.

5.2 **Comunicación con autoridades**

- **Procedimiento de notificación:**
    - Notificar al órgano competente correspondiente (por ejemplo, unidad de lavado de dinero, superintendencia, o autoridad designada en Costa Rica) conforme a requisitos legales y reglamentarios.
    - Adjuntar evidencia relevante de identificación, antecedentes de la operación, y la evaluación de riesgo.
    - Mantener registro de la fecha, hora y canal de la notificación, así como el número de expediente asignado.
- **Confidencialidad y protección de denuncias:**
    - Garantizar confidencialidad de la identidad del denunciante y de la información sensible.
    - Evitar represalias y asegurar protección de datos conforme a normativa de protección de datos personales y de confidencialidad interna.

5.3 **Divulgación externa y terceros**

- **Obligaciones de notificación a clientes o terceros cuando aplique:**
    - Informar a clientes/terceros cuando exista obligación legal de divulgar información o cuando la propia operación así lo requiera (por ejemplo, cambios en condiciones, necesidad de proveer documentos).
    - Resguardar confidencialidad de datos y minimizar exposición innecesaria de terceros.
- **Gestión de confidencialidad y protección de datos:**
    - Aplicar políticas de protección de datos (acceso restringido, cifrado de documentos sensibles, almacenamiento seguro).
    - Limitar divulgaciones a lo estrictamente necesario y conforme a consentimientos o bases legales.

5.4 **Registro y seguimiento**

- **Registro de eventos reportados, respuestas de autoridades y acciones tomadas:**
    - Mantener expediente de ROS con fecha, tipo de operación, perfil de cliente, evidencia, decisiones y medidas correctivas.
    - Registrar respuestas de autoridades, plazos cumplidos y acciones de remediación.
    - Archivar correspondencia, documentos de soporte y resultados de investigaciones.
- **Indicadores de desempeño para el proceso de divulgación:**
    - Tiempo medio desde detección hasta reporte.

- Porcentaje de ROS aceptados por la autoridad y cerrados en tiempo.
- Nº de ROS abiertos por tipo de operación/cliente.
- Cumplimiento de plazos de notificación y respuesta.

6. Medidas organizativas y técnicas

6.1 Políticas y manuales de cumplimiento LC/FT/FPADM

- Establecer, revisar y aprobar políticas de LC/FT/FPADM (KYC, PEP, DGA, trazabilidad de fondos, monitoreo de transacciones, divulgación).
- Manuales y procedimientos operativos estándar (SOPs) para cada proceso (captación de clientes, KYC, aprobaciones, divulgación).
- Definición de roles y responsabilidades, estructura de control y canales de reporte.

6.2 Comité de Cumplimiento y Supervisión

- Crear un Comité de Cumplimiento (o equivalente) integrado por:
- Responsable de cumplimiento (Compliance Officer).
- Gerente de ventas/Proyectos.
- Supervisor de obra/diseño.
- Representante del área financiera.
- Responsable de Tecnologías de la Información (TI) para controles técnicos.
- Funciones del Comité:
- Aprobar políticas, estándares y cambios en el programa LC/FT/FPADM.
- Monitorear riesgos, indicadores clave y tendencias; revisar indicadores de desempeño (KPI/KRI).
- Garantizar la adecuación de controles ante cambios regulatorios o estructurales de la empresa.
- Revisar y aprobar casos complejos de clasificación de riesgo y excepciones.
- Asegurar la capacitación continua, pruebas de controles y auditorías internas.
- Reuniones y seguimiento: mínimo una vez al trimestre, con actas y seguimiento de decisiones.

6.3 Controles tecnológicos y de información

- Gestión de identidades y accesos (IAM): acceso basado en roles para sistemas de KYC, CRM, ERP y divulgación.
- Registro y trazabilidad: grandes sistemas deben registrar eventos de cumplimiento (creación de cliente, aprobaciones, ROS, comunicaciones).
- Seguridad de datos: cifrado, copias de seguridad, protección de datos personales y cumplimiento de NDPR/lei de protección de datos local.
- Monitoreo de transacciones: herramientas de detección de anomalías, alertas y escalamiento automático según umbrales.
- Auditoría y pruebas: pruebas de penetración, revisiones de controles y evaluaciones de riesgo regulares.

6.4 Formación y cultura de cumplimiento

- Plan de capacitación anual para todo el personal (KYC, ROS, boletines de riesgos).
- Evaluaciones de competencia y certificaciones necesarias para roles críticos.
- Campañas de concienciación sobre ética y denuncias.

6.5 Gestión de cambios y documentación

- Control de versiones de políticas y SOPs; aprobación formal de cambios por el Comité.
- Mantenimiento de un repositorio documental centralizado con control de acceso.
- Procedimiento de divulgación de incidentes y lecciones aprendidas.