

De la obligación al valor

Cómo ISO fortalece los programas de PLD

MATEOS CONSULTORES / ARTÍCULO / Luis D. Mateos

El sector financiero en México opera bajo una intensa carga de cumplimiento regulatorio, especialmente en materia de Prevención de Lavado de Dinero (PLD). Muchas instituciones perciben cualquier marco de gestión adicional, como las normas ISO, como innecesario ante tanta regulación existente. Sin embargo, adoptar estratégicamente estándares ISO puede transformar el cumplimiento de una obligación impuesta a una fuente de valor estratégico para la organización. De hecho, los estándares de la Organización Internacional de Estandarización proporcionan metodologías estructuradas que permiten mejorar la calidad, seguridad y eficiencia de los procesos, minimizando riesgos y fomentando una cultura sólida basada en principios éticos. Más allá del mero tick-the-box regulatorio, las normas ISO se han convertido en herramientas estratégicas que impulsan la confianza de clientes, fortalecen la reputación corporativa y alimentan la mejora continua. En el contexto de PLD, esto significa pasar de ver el cumplimiento solo como carga obligatoria a aprovecharlo como un mecanismo para proteger activos y reputación mientras se promueve la sostenibilidad del negocio.

ISO y PLD: de la carga regulatoria al valor estratégico

Integrar estándares ISO a los programas de PLD no implica duplicar esfuerzos o añadir burocracia, sino alinear las mejores prácticas internacionales con las exigencias locales en materia antilavado. Las normas ISO proporcionan lenguajes comunes y estructuras de gestión que pueden engranar con los requisitos de la legislación mexicana (por ejemplo, la LFPIORPI, las reglas de la CNBV y los lineamientos de la UIF) y con estándares internacionales (como las 40 Recomendaciones del GAFI/FATF y guías de la OCDE). El resultado es un programa PLD más robusto, eficiente y auditable, que cumple con la ley nacional a la vez que genera valor añadido en la organización.

Un ejemplo claro es la adopción del enfoque basado en riesgos propugnado tanto por el GAFI como por ISO. El GAFI establece que “la piedra angular de las Recomendaciones es el enfoque basado en riesgo, que enfatiza la necesidad de identificar y comprender los riesgos de lavado... para priorizar recursos en las áreas de mayor riesgo”. Las normas ISO aportan justamente un marco para implementar ese enfoque de forma sistemática.

Estándares ISO clave para fortalecer la PLD

La ISO 31000:2018 es la norma internacional de gestión de riesgos que sirve de referencia global para identificar, evaluar y mitigar riesgos de todo tipo. Un programa PLD efectivo debe basarse en la evaluación de riesgos de lavado de dinero y financiamiento al terrorismo, tal como exigen tanto las autoridades locales como los estándares internacionales. Adoptar ISO 31000 en PLD permite institucionalizar el enfoque basado en riesgo que piden los reguladores. Con esta norma, la institución desarrolla principios, un marco y procesos para gestionar riesgos de lavado de forma sistemática y proactiva, en lugar de reactiva. Esto fortalece la identificación temprana de amenazas (p. ej., clientes, productos, canales o jurisdicciones de alto riesgo) y la toma de decisiones informadas sobre controles mitigantes. En línea con los principios de ISO 31000, la gestión del riesgo PLD crea valor protegiendo activos y reputación, se integra en procesos de negocio cotidianos, apoya la toma de decisiones, aborda incertidumbres y facilita la mejora continua del sistema. Todo esto contribuye a que el programa PLD no solo cumpla con la obligación de evaluar riesgos (como exige la LFPIORPI y el GAFI), sino que realmente mejore la resiliencia del negocio ante riesgos financieros ilícitos.

La ISO/IEC 27001:2022 establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), protegiendo la confidencialidad, integridad y disponibilidad de la información de la organización. En términos prácticos, ISO 27001 ayuda a evitar brechas que podrían comprometer un programa antilavado. Por ejemplo, los anexos de ISO 27001 incluyen controles sobre control de accesos y retención de

información que se alinean con las exigencias de PLD de conservar expedientes por ciertos años y prevenir accesos no autorizados a datos de clientes. De hecho, proteger la información sensible es parte de “mantener la confianza del cliente y cumplir con expectativas de seguridad”. Así, la seguridad de la información deja de ser un requerimiento aislado de TI y se convierte en pilar integrado del cumplimiento PLD, reduciendo riesgos de sanciones por fugas de información o uso indebido de datos de clientes.

La ISO 37301:2021 es el estándar internacional para sistemas de gestión de cumplimiento normativo (Compliance Management Systems), sucesor certificable de la antigua ISO 19600. Implementar ISO 37301 aporta estructura y consistencia a la función PLD: establece políticas claras, roles (p. ej., un Oficial de Cumplimiento con responsabilidad sobre PLD), procedimientos documentados, evaluación continua de riesgos de incumplimiento, controles operativos, capacitación periódica y canales de denuncia/gestión de incidentes. Todos estos elementos coinciden con los requerimientos típicos de un programa antilavado. Por ejemplo, la norma requiere compromiso de liderazgo y políticas anticorrupción/antilavado alineadas con las obligaciones legales, así como procesos de debida diligencia, auditorías internas de cumplimiento y mejora continua. Esto es perfectamente compatible con lo que las autoridades financieras esperan: la CNBV y la UIF exigen políticas PLD aprobadas por el Consejo, un oficial designado, monitoreo de listas (ONU, OFAC) y auditorías independientes del sistema PLD. ISO 37301 formaliza y documenta todo ello dentro de un sistema coherente, facilitando demostrar a los reguladores un cumplimiento efectivo. Además, la adopción de un SGC certificable envía un mensaje de “tolerancia cero” al incumplimiento y refuerza la confianza de socios y clientes en la institución.

La ISO 9001:2015, de gestión de la calidad, puede no parecer directamente relacionada con PLD a primera vista. Sin embargo, ISO 9001 proporciona los cimientos de cualquier sistema de gestión. ¿Cómo aporta valor esto? Por un lado, evita duplicidades: si la institución ya cuenta con procedimientos estandarizados y controles de cambios documentales bajo ISO 9001, los procedimientos PLD pueden incorporarse allí en lugar de crear manuales aislados. Asimismo, ISO 9001 exige capacitaciones de personal competente y seguimiento de la satisfacción (que en cumplimiento se traduce en “satisfacción regulatoria” y confianza del público). Por otro lado, ISO 9001 demanda auditorías internas periódicas y revisiones por la dirección. Estas pueden ampliarse para cubrir también los procesos PLD, cumpliendo así con la obligación de verificar periódicamente la efectividad del programa antilavado (algo que la regulación local exige). En resumen, un enfoque de calidad garantiza que el programa PLD no se quede estático por “cumplir”, sino que se mantenga en mejora continua, detectando oportunamente fallos o ineficiencias y corrigiéndolos antes de que se traduzcan en incumplimientos.

Programa PLD/FT	ISO 9001 Procesos, documentación, auditoría interna, mejora, capacitación...
	ISO 31000 Enfoque Basado en Riesgos, evaluación, tratamiento, KYC/DDC, segmentación, alertas, monitoreo...
	ISO 37301 Compliance, políticas, gobernanza, debida diligencia, Oficial de Cumplimiento, auditoría, reportes (ROS/P), listas y sanciones...
	ISO 27001 Seguridad, accesos, cifrado, retención de expedientes, incidentes, LFPDPPP...

Figura: Modelo integrado ISO-PLD · No exhaustivo

Compatibilidad entre requisitos ISO y exigencias PLD: ejemplos prácticos

Lejos de significar re-trabajo, los estándares ISO complementan y en muchos casos calzan perfectamente con las exigencias regulatorias en PLD. Los siguientes son 3 ejemplos claros de esta alineación y compatibilidad:

- **Enfoque basado en riesgos:** Las normas PLD mexicanas y las recomendaciones internacionales (FATF) obligan a las instituciones a realizar evaluaciones de riesgo de lavado de dinero, segmentar clientes por nivel de riesgo y

De la obligación al valor ISO y prevención de lavado de dinero

aplicar medidas intensificadas donde haya mayor exposición. ISO 31000, por su parte, provee la metodología estándar para gestionar riesgos. Integrar ISO 31000 al programa PLD permite usar una misma matriz de riesgo y proceso de evaluación para todos los riesgos (operativos, crediticios, LAFT, etc.), evitando tener un “riesgo PLD” aislado. Por ejemplo, FATF enfatiza identificar y comprender riesgos para priorizar recursos, e ISO 31000 justamente establece principios de que la gestión de riesgos “sea parte integral de los procesos de la empresa y facilite la mejora”. Así, la institución cumple con la LFPIORPI al evaluar riesgo de clientes/productos, al mismo tiempo que mejora su gestión integral de riesgos sin esfuerzo duplicado.

- **Controles internos, auditoría y mejora continua:** Un requisito explícito de la regulación antilavado es que las instituciones mantengan controles internos eficaces, un oficial de cumplimiento responsable y realicen auditorías periódicas a su sistema PLD. Aquí, las normas ISO 37301 y 9001 resultan directamente aplicables. ISO 37301 exige tener controles documentados para mitigar riesgos de incumplimiento y un ciclo de verificación y mejora, mientras que ISO 9001 asegura que haya auditorías internas regulares de todos los procesos críticos. En la práctica, una empresa puede ampliar el alcance de sus auditorías ISO para incluir la revisión del programa PLD, cubriendo así la obligación normativa de contar con una auditoría independiente anual (o con mayor frecuencia si hay riesgos altos). La reciente reforma a la LFPIORPI en 2025, por ejemplo, exige “capacitación constante y auditorías cuando se identifiquen riesgos altos”. Un sistema integrado con ISO permite cumplir esto de forma natural: la detección de un riesgo alto activa planes de capacitación adicionales y revisiones (auditorías) especiales, como parte del mismo ciclo de mejora continua de la ISO. No hay necesidad de crear un procedimiento nuevo solo para la ley; la estructura ISO ya contempla capacitación y acción correctiva ante riesgos. Asimismo, ISO 9001 enfatiza la documentación de procesos y registros, lo cual ayuda a que, ante una inspección de CNBV/UIF, la institución tenga evidencia trazable de cada control PLD implementado, cambios realizados y resultados de evaluaciones.
- **Capacitación y cultura organizacional:** Tanto las normas ISO como la regulación PLD ponen gran peso en la formación del personal y el “tono desde la cima”. Por un lado, ISO 37301 requiere que la alta dirección demuestre liderazgo en cumplimiento y que se implementen programas continuos de capacitación y concientización en todos los niveles. Por otro lado, las disposiciones de la CNBV y la Ley Antilavado obligan a entrenar al personal en materia de PLD regularmente (de hecho, la reforma 2025 establece “capacitación obligatoria continua” para los sujetos obligados). Al integrar estas exigencias, un único programa de entrenamiento puede servir simultáneamente para cumplir la norma ISO (en términos de competencias del personal) y la ley antilavado. La ventaja de la aproximación ISO es que convierte la capacitación en un proceso planificado, medible y con mejora (evaluando eficacia), en lugar de un trámite aislado para “cumplir con la UIF”. Esto refuerza la cultura interna: los empleados no solo reciben el qué (políticas PLD) sino el porqué y el cómo, enlazando la prevención de riesgos LAFT con los valores de la empresa. El resultado es una **mayor efectividad preventiva**—personal alerta a señales de riesgo, dispuesto a reportar— que beneficia tanto al cumplimiento normativo como a la salud ética de la organización.

ISO 37301 (cláusula/tema)	PLD México (LFPIORPI/CNBV/UIF) - requisito equivalente
Política de compliance y liderazgo (cl. 5.1, 5.2)	Políticas y Manual PLD aprobados por Consejo; 'tono desde la cima'
Roles y responsabilidades (cl. 5.3)	Designación del Oficial de Cumplimiento y Comité (CCC); independencia y facultades
Obligaciones de cumplimiento y evaluación de riesgos (cl. 4.2, 6.1)	Metodología basada en riesgos (cliente, producto, canal, geografía); segmentación KYC/DDC
Planificación y controles operativos (cl. 6.2, 8.1)	Procedimientos PLD (KYC, listas, monitoreo); umbrales y alertas
Información y comunicación (cl. 7.4)	Difusión de políticas; avisos regulatorios; reporte interno a Consejo/Comité
Competencia y formación (cl. 7.2)	Capacitación anual obligatoria en PLD; registro de evidencias
Información documentada (cl. 7.5)	Manual, políticas y expedientes; conservación conforme a plazos legales
Seguimiento, medición y evaluación (cl. 9.1)	Monitoreo de operaciones; indicadores; reporte a UIF (ROS/ROP)
Auditoría interna (cl. 9.2)	Auditoría independiente periódica del Sistema PLD (interna/externa)
Revisión por la dirección (cl. 9.3)	Informe del Oficial de Cumplimiento al Consejo/Comité; evaluación anual
No conformidades, acciones y mejora (cl. 10.1, 10.2)	Planes de remediación y mejora continua tras hallazgos o visitas de supervisión

Tabla: Vinculación de cláusulas ISO 37301 con requisitos equivalentes de LFPIORPI/CNBV/UIF.

Conclusiones

En el entorno regulatorio actual, cumplir con PLD ya no es un simple checklist estático, sino un proceso dinámico que demanda estrategia y resiliencia. Convertir el cumplimiento “de obligación a valor” es posible aprovechando los estándares ISO como aliados. Estos proporcionan lenguajes comunes, marcos estructurados y buenas prácticas que fortalecen la implementación correcta de los programas antilavado, a la vez que facilitan demostrar cumplimiento tanto frente a autoridades mexicanas (LFPIORPI, CNBV, UIF) como en el concierto internacional (FATF, OCDE). Lejos de ser esfuerzos paralelos, las normas ISO integradas conllevan sinergias: la organización gana en eficiencia (menos reprocesos, controles integrados), en eficacia (mejor identificación y mitigación de riesgos de lavado) y en confianza de los stakeholders (clientes, socios, reguladores perciben una institución sólida y comprometida).

En palabras de expertos, invertir en estos sistemas de gestión convierte el compliance de un costo a una ventaja estratégica, permitiendo “fomentar la confianza, proteger la reputación y adelantarse a las amenazas de delitos financieros”. Para los profesionales del sector financiero en México, el mensaje es claro: adoptar normas ISO no significa sumar cargas, sino potenciar el programa PLD existente. Con una integración inteligente y progresiva, es posible cumplir mejor con la ley (incluso reducir el riesgo de sanciones) y simultáneamente agregar valor a la organización mediante procesos más robustos, culturas más íntegras y operaciones más seguras. En definitiva, se trata de unificar objetivos: lo que es bueno para el cumplimiento puede y debe ser bueno para el negocio. Las normas ISO ofrecen la hoja de ruta para lograr esa unificación de forma tangible y sostenible.

Fuentes: Las afirmaciones y ejemplos provistos se basan en estándares internacionales y mejores prácticas documentadas por organismos y expertos en la materia, incluyendo lineamientos de ISO, recomendaciones del GAFI [fatf-gafi.org] y casos de estudio de implementación de sistemas integrados de gestión en entornos de cumplimiento, entre otros. Cada referencia citada en el texto corresponde a la fuente original que sustenta la información, evidenciando la compatibilidad y beneficio de integrar ISO en programas de PLD. Todas ellas apuntan a una conclusión común: un cumplimiento robusto apoyado en ISO no es un lujo opcional, sino una inversión que rinde frutos en eficacia regulatoria y excelencia operativa.