Universidad Andina Simón Bolívar

Sede Ecuador

Área de Gestión

Maestría en Administración de Empresas

Implementación de la Norma ISO 31000:2009 en la administración del riesgo de lavado de activos y del financiamiento de delitos, en bancos privados de Ecuador

Iván Danilo Ortiz Alulema

Tutor: José Esteban Melo Jácome

Quito, 2020

Cláusula de cesión de derechos de publicación de tesis

Yo, Iván Danilo Ortiz Alulema, autor de la tesis "Implementación de la Norma ISO 31000:2009 en la administración del riesgo del lavado de activos y del financiamiento de delitos, en bancos privados de Ecuador", mediante el presente documento dejo constancia que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de Magíster en Administración de Empresas, en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo por lo tanto la Universidad, utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en los formatos virtual, electrónico, digital, óptico, como usos en red local y en internet.
2. Declaro que en caso de presentarse cualquier reclamación de parte de terceros respecto de los derechos de autor de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y la Universidad.
3. En esta fecha entrego a la Secretaría General, el ejemplar respectivo y sus anexos en formato impreso y digital o electrónico.

17 de noviembre del 2020

Firma: _____

Resumen

En un mundo globalizado donde la evolución de los medios tecnológicos para facilitar la circulación del flujo de capitales de un lugar a otro en busca de oportunidades de inversión, ha provocado cambios en los modelos de negocio así como en las actividades de control de las entidades financieras, además estos cambios obligan literalmente a la evolución de la "Administración de Gestión de Riesgos" para dar respuesta a este vertiginoso avance de la tecnología y redes de negocio. Este avance ha dado lugar también a que las organizaciones delictivas aprovechen estos mecanismos para introducir en los bancos fondos de origen ilícito o de procedencia ilegal.

Con este antecedente, las leyes y marco regulatorio –local e internacional– emitidos para la prevención y control de estos delitos, representa los mecanismos que las entidades gubernamentales, organismos de control y las entidades bancarias ponen en práctica para prevenir la materialización de estos riesgos, en tal sentido, los organismos de supervisión y control periódicamente realizan revisiones in situ a los bancos nacionales para establecer la solidez de los sistemas de administración de estos riesgos, el grado de cumplimiento con la normativa, así como la emisión de observaciones y recomendaciones de mejora.

Desde la perspectiva del sector bancario nacional se vislumbra la necesidad de implementar y fortalecer sus sistemas de gestión de riesgos de prevención de lavado de activos y financiamiento de delitos, acorde a las exigencias de las nuevas tecnologías, el incremento de estos delitos a nivel mundial y las recomendaciones emitidas por el organismo supervisor. Por lo que surge la necesidad que los bancos implementen un sistema que les permita realizar una evaluación con un enfoque integral de riesgos que incluya las diferentes variables cualitativas y cuantitativas de los factores de riesgo.

Por lo expuesto, el diseño de un modelo de administración de gestión de riesgo con base a los lineamientos de la norma ISO 31000:2009 permitirá a los bancos privados locales gestionar la identificación, análisis, evaluación y tratamiento de los riesgos asociados a estos delitos, con un enfoque integral de todos los factores de riesgo que incluye la aceptación y control de los diferentes niveles de riesgo, que le permita a la entidad efectuar una gestión gerencial basada en la administración integral de riesgos para alcanzar sus objetivos de negocio, alineados al cumplimiento del marco regulatorio.

Tabla de contenido

Índice de tablas

Índice de gráficos

Introducción

1. Descripción del problema

Las entidades bancarias a nivel mundial por la naturaleza de su negocio de intermediación financiera de captación y colocación de recursos, están expuestas a riesgos relacionados con el ingreso de fondos de origen ilícito dentro del flujo de sus operaciones provenientes del lavado de activos y financiamiento de delitos, que puede provocar sanciones y hasta el cierre de sus operaciones.

El Fondo Monetario Internacional estima que el lavado de activos en el mundo podría representar una cifra de entre el 2 al 5% del PIB bruto mundial, en tanto que el Banco Mundial calcula que el flujo a través de las fronteras por actividades criminales, corrupción y evasión de impuestos es de entre US $ 1 billón y US $ 1,6 billones de dólares, de los cuales US $ 40.000 millones son producto de la corrupción en países en desarrollo y en transición (Centro de Estudios Sociales y de Opinión Pública 2012,16).

Es importante destacar que en las evaluaciones in situ y extra situ que realiza la Superintendencia de Bancos a los programas de prevención de lavados de activos y financiamiento de delitos (LAFD) de los bancos privados del país, frente al involucramiento o participación no intencional en actividades ilícitas, bajo medidas destinadas a la prevención y detección de estos delitos, se establece deficiencias identificadas por dicho organismo en las revisiones del periodo 2014, por lo que muchas operaciones injustificadas y de origen ilícito han sido procesadas sin levantar alertas ni reportes de inusualidad a las autoridades competentes.

Con los antecedentes expuestos sobre el crecimiento y materialización de estos riesgos dentro de la gestión de negocios y las deficiencias identificadas en las revisiones efectuadas por la Superintendencia de Bancos, obliga a los bancos privados del país a evaluar y reforzar sus controles preventivos para que sus productos financieros no sean utilizados como un móvil para la ocurrencia de estos riesgos, a través del ingreso de recursos de origen ilícito en el flujo de sus operaciones.

De acuerdo al estudio realizado por la Facultad Latinoamericana de Ciencias Sociales, en el Ecuador en el periodo 2010 a 2014 las denuncias por lavado de activos se incrementaron de 65 a193 (aumento del 297%) de los cuales solamente 15 casos tienen sentencia en firme en dicho periodo. Las provincias de Pichincha y Guayas son

las zonas donde se identifica la mayor concentración de estos delitos con el 39% y 38%, respectivamente, el resto de provincias tienen una participación que oscila entre el 1 al 6% (FLACSO 2015, 15). Para efecto del presente estudio se debe indicar que la probabilidad de ocurrencia de estos riesgos es más alta y son más vulnerables aquellas entidades bancarias que posean sistemas de administración de riesgos poco sólidos, limitados en procedimientos de control y sin un enfoque integral del riesgo.

Muchos bancos privados a nivel mundial han sido sancionados con cuantiosas multas que han llegado hasta US $ 1.921 millones (Stuart 2012, 1), procesos judiciales en contra de sus directivos, representantes y funcionarios implicados en estos delitos y hasta el cierre de operaciones de entidades financieras tanto a nivel local como a nivel internacional. Los casos de sanciones a entidades financieras locales y del exterior representan una amenaza permanente para la continuidad de negocio, para los bancos que no demuestren ante la autoridad competente –que juzga estos delitos– que han sido proactivos en implementar y ejecutar acciones de control preventivo.

Por lo expuesto, la presente investigación parte de la evaluación de los programas actuales de administración de riesgos con los que cuentan los bancos privados y se enfoca en la implementación de la norma ISO 31000 en el sistema general de gestión de riesgos de LAFD, norma que se adapta al manejo de estos riesgos para mejorar el sistema actual que va a permitir reforzar las variables cuantitativas y fomentar la incorporación de las variables cualitativas dentro del sistema de gestión, para obtener una administración integral de todos los factores y variables que componen tales riesgos, así como realizar su análisis, medición y evaluación en un periodo determinado por medio de una calificación ponderada (bajo, medio, alto y extremo) y la aceptación de las variables contenidas en la matriz de riesgo. Este análisis muestra valores y resultados, de acuerdo a la probabilidad y el impacto. De él se obtiene la magnitud de los riesgos, en tanto que la probabilidad hace referencia a la posibilidad de que esos riesgos terminen ocurriendo, mientras que el impacto es el nivel de perjuicio a la entidad bancaria.

2. Pregunta central

¿Cómo aporta la implementación de los lineamientos de la norma ISO 31000:2009 en el sistema de administración y gestión de riesgos de lavado de activos y de financiamiento de delitos, que desarrollan los bancos privados de Ecuador, para

minimizar su vulnerabilidad frente al riesgo de la utilización de su infraestructura física y tecnológica de servicios financieros para la colocación, estratificación e integración con apariencia de legitimidad de ciertos capitales de origen ilícitos?

3. Objetivos

Objetivo general

Mejorar el sistema de administración y gestión de riesgo de prevención de lavado de activos y financiamiento de delitos de los bancos privados de Ecuador, con base a la incorporación de los conceptos de la norma ISO 31000:2009, el cumplimiento de la normativa legal y las mejores prácticas locales e internacionales, para fortalecer dicho sistema de administración de riesgos.

Objetivos específicos

- Analizar los resultados cuantitativos obtenidos mediante la encuesta sobre el estado actual de la solidez, suficiencia y eficacia del sistema de administración de riegos de los bancos privados del Ecuador, respecto al manejo del riesgo de lavado de activos y financiamiento de delitos, que representa la línea base de la presente investigación.
- Incorporar las variables de los factores cualitativos y cuantitativos en la matriz de evaluación de riesgos de lavado de activos y financiamiento de delitos, acorde a los preceptos de la norma de gestión de riesgos ISO 31000:2009 y observaciones acotadas por la Superintendencia de Bancos.
- Dotar de lineamientos de control preventivo para realizar un monitoreo efectivo de las transacciones de clientes con base a un sistema de gestión integral que considere todos los factores de riesgo cualitativos y cuantitativos, que permita identificar señales de alerta e inusualidades en el comportamiento transaccional de los clientes.
- Optimizar el sistema actual de administración de riesgos, dentro de las operaciones de los bancos privados, basado en la incorporación de la norma ISO 31000:2009 cuyas mejoras sean cuantificadas mediante el número de alertas presentadas por el sistema de monitoreo de transacciones de clientes, así como la cantidad periódica de reportes al organismo de control de transacciones inusuales injustificadas de clientes.

4. Justificación

El lavado de activos probablemente sea uno de los problemas más graves que tendrá que enfrentar la *humanidad de la post modernidad*, llamada así por Ulrich Beck en su obra "La Sociedad del Riesgo Global" (Beck, 2006). El vertiginoso desarrollo de las tecnologías de información, las redes sociales, el comercio electrónico, la globalización de los negocios y los capitales que se movilizan de un lado a otro del mundo a la búsqueda de concreción de oportunidades de negocios para obtener utilidades, han abierto un espacio de incertidumbre de enormes dimensiones, que sirve de escenario perfecto para una delincuencia camuflada y organizada cuyos niveles de organización y especialización son cada vez más sofisticados y de alcance transnacional.

La administración de riesgos es fundamental para controlar y mitigar estos riesgos y destaca la importancia que representa para la colectividad del país los esfuerzos de las entidades bancarias para aplicar un sistema de administración y control de riesgos dentro de la labor de dirección de la empresa, en la gestión operativa interna, en la gestión comercial con los clientes, proveedores, colaboradores internos y con la comunidad en general. Por cuanto es tarea de todos los estamentos de la sociedad combatir y precautelar el avance de estos delitos de lesa humanidad que amenazan la estabilidad económica, política, social, emocional y de seguridad física de los diferentes actores de dicha sociedad.

La norma ISO 31000:2009 va a permitir incorporar en los sistemas actuales de administración de riesgos de los bancos privados, los preceptos y fundamentos de manejo del riesgo de lavado de activos y financiamiento de delitos con un enfoque global e integral de todos los factores y variables cuantitativas y cualitativas que conforman dichos riesgos, cuya gestión de control se adapte con los lineamientos y objetivos estratégicos de la alta dirección de la organización.

La presente investigación es importante para los bancos privados del país, ya que por la naturaleza de su giro de negocio de intermediación financiera, están expuestas a riesgos relacionados al ingreso de recursos de origen ilícito dentro del flujo de sus operaciones provenientes del lavado de activos y/o financiamiento de delitos. Además, las entidades bancarias están expuestas al deterioro de su imagen y reputación en el caso que se encuentre inmersa en tales delitos, que puede provocar el cierre de sus operaciones. En tal sentido, el mejoramiento del sistema de administración y control

para la gestión de riesgos de LAFD, dentro de sus operaciones va a permitir cumplir con la ley, un crecimiento sostenido de su negocio, salvaguardar el interés empresarial de los accionistas y mantenerse en el mercado como una empresa en marcha.

El enfoque de riesgo como un modelo para identificar las amenazas asociadas al lavado de activos y financiamiento de delitos, así como las vulnerabilidades de las entidades bancarias frente a este riesgo potencial, es clave y ha sido analizado por varios autores, en especial por los organismos de control locales y del exterior, entre ellos la Superintendencia de Bancos, quien a través de la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos regula el control de las entidades bancarias a través de la aplicación de los programas de revisión in situ a las entidades bancarias. En tanto que a nivel internacional el Grupo de Acción Financiera Internacional (GAFI) es el organismo que continuamente emite las normas, recomendaciones y mejores prácticas para el control de estos riesgos.

5. Marco temático

La gestión de riesgo, según la Asociación Española de Normalización (AENOR), se ha difundido y normalizado internacionalmente en este siglo XXI, siendo la norma ISO 31000:2009 el primer estándar internacional que ha proporcionado un acercamiento común para gestionar cualquier tipo de riesgo, no específico de ninguna industria o sector. Adoptando este estándar internacional *como norma nacional en más de 40 países* al rededor del mundo. Esta acogida de la norma debido a las bondades y adaptabilidad del enfoque integral para gestionar cualquier tipo de riesgos con base a una metodología estandarizada (Escorial 2012).

El tema central de la presente investigación referente a la *"Implementación de la norma ISO 31000:2009 en la administración del riesgo de LAFD en bancos privados del Ecuador"*, en su real contenido y alcance no ha sido desarrollado de manera conceptual, integral y práctica por las entidades bancarias locales o del exterior. Se han desarrollado un sin número de estudios e investigaciones académicas y científicas sobre la administración de sistemas de prevención de lavados de activos. Existen varias investigaciones de la administración y aplicación de matrices de riesgo en el marco para un plan de prevención contra el lavado de activos; y además algunos estudios sobre la norma ISO 31000 aplicado a la operatividad y seguridad de la información relacionadas

con riesgos tecnológicos de ciertas entidades del sector financiero, pero no específicamente enfocada a la administración de riesgos de LAFD para un banco.

Uno de los estudios que aborda esta temática por parte de la investigadora Diana Albanese, expone que la proliferación de fraudes corporativos y delitos financieros como el lavado de activos ha llevado a las entidades a reformular su estrategia implantando modelos de control interno que enfocan su atención en el ambiente de control y la *gestión integral de riesgo* -enfoque de la ISO 31000:2009-, cuya finalidad es aplicar la matriz de riesgo para definir perfiles de clientes, detectar posibles operaciones inusuales o sospechosas y mitigar los riesgos asociados en una entidad financiera (Albanese 2012, 206).

En el sector de servicios de las aseguradoras, según el especialista Efraín Idrovo la *disminución del riesgo operativo* fue posible en las compañías de seguros mediante la implementación de la norma ISO 31000:2009, esta disminución es factible considerando la inclusión de las diversas etapas con las cuales se deben contar para una adecuada gestión del riesgo como son la planificación, identificación, análisis, medición, control y monitoreo. La metodología de esta norma utiliza como precedente a la herramienta COSO ERM, el cual ya utilizaba algunas de las etapas que menciona la ISO 31000, la principal diferencia que se presenta con la metodología ISO es el *mayor compromiso con la alta dirección* en cuanto a la adecuada gestión del riesgo operativo y la comunicación continua que debe existir a los diferentes niveles jerárquicos de la institución sobre el riesgo de la entidad y su evolución, adicional se debe indicar que en esta norma se incluye como inicio del proceso, el establecer el contexto, con esto se captura los objetivos de la organización, el entorno en el que se persiguen estos objetivos, las partes interesadas y la diversidad de criterios de riesgo, todo lo cual ayuda a revelar y evaluar la naturaleza y la complejidad de sus riesgos (2015, 28).

El sector asegurador es uno de los más regulados en el país por lo que a través del monitoreo, mitigación y administración de riesgos se puede disminuir la probabilidad de pérdidas por el acontecimiento de eventos adversos en las compañías de seguros, por lo que la aplicación de la norma permitió identificar los principales riesgos propuestos en la normativa legal pertinente, contenidas básicamente en el actual Código Orgánico Monetario y Financiero (COMF), lo cual facilitó el determinar las señales de alerta, mismas que fueron incluidas en los indicadores de riesgo, para prevenir posibles eventos (Encalada 2018, 60).

Es de vital importancia para las empresas aseguradoras determinar el nivel de riesgo al cual se encuentran expuestos en los diversos procesos que ejecutan, conocer la situación actual permite establecer acciones futuras para reducir los índices de exposición al riesgo cuando éste se materializa, la medición de los riesgos operativos evidencian las principales falencias de la compañía a fin de tomar decisiones oportunas ante estos eventos. Para la correcta aplicación de la metodología planteada con base a ISO 31000 se debe tener claramente definidos y documentados a los responsables de cada proceso, junto con el inventario de las actividades que realizan ellos y sus colaboradores, así como contar con un presupuesto y compromiso previo de la dirección que respalde la ejecución del proyecto (Idrovo 2015, 90).

En el campo tecnológico esta norma internacional es plenamente aplicable, puesto que dado el aumento en el uso de las tecnologías de la información puede evitar o anticipar puntos de quiebre o fisuras en aspectos de seguridad con respecto a su utilización, por ello se presenta una forma de aseguramiento y control sobre la infraestructura, los sistemas de información y las medidas organizacionales desde la perspectiva tecnológica (Ramírez 2011).

La información es el elemento más valioso para cualquier organización en este nuevo siglo, la cual es un instrumento de gestión administrativa para crear una ventaja competitiva (Vásquez 2015). Sin embargo, para el investigador Esteban Crespo pese a la falta de conocimiento sobre cómo protegerla adecuadamente o a la complejidad de las normas internacionales que indican los procedimientos para lograr un adecuado nivel de protección, muchas organizaciones, en especial el sector mipyme no logra alcanzar este objetivo. Por lo que Crespo propone una metodología de seguridad de la información para la gestión del riesgo informático aplicable al entorno empresarial y organizacional del sector mipyme ecuatoriano. Para el efecto el autor propone una metodología basada en los principios de administración de riesgo, provista por los estándares ISO 31000:2009 y en las mejores prácticas de seguridad de la información: ISO 27001, ISO 27002 e ISO 27005 (2017, 7).

Entre las conclusiones de la investigación se destaca que las empresas del sector mipyme no están preparadas para enfrentar los riesgos de manera formal, esto es, los riesgos son manejados a un nivel adhoc o simplemente los maneja como respuesta a un incidente. Para que la gestión de riesgo sea efectiva en la mipyme es importante la participación de la gerencia en los procesos de gestión de riesgo que hace énfasis la ISO 31000, pues el compromiso que mantenga es primordial para lograr mitigar los riesgos

en conjunto con un buen equipo de trabajo y de esta manera alcanzar las metas y objetivos corporativos que se fusionan en una visión empresarial (Crespo 2017, 121).

Otro caso práctico de aplicación de la norma, son las instituciones que pertenecen al *sector mutual* que se encuentren reguladas por la "Norma para la Organización de las Asociaciones Mutualistas de Ahorro y Crédito para la Vivienda que pasan al Control de la Superintendencia de Economía Popular y Solidaria" contenida en la Resolución No. 362-2017-F del 8 de mayo del 2017, que tienen la oportunidad de utilizar un modelo de gestión de riesgo de crédito diseñado para entidades de su tamaño y complejidad con la finalidad de identificar, analizar, evaluar y tratar los riesgos que afectan el cumplimiento de sus objetivos estratégicos.

Según la investigación académica de Martha Bolaños, una particularidad de este tipo de industria es el crédito para la adquisición de bienes inmuebles, siendo el sector mutual uno de los partícipes del sector de la economía popular y solidaria y conociendo las semejanzas por naturaleza entre mutualistas y cooperativas pertenecientes al mismo sector; el modelo desarrollado con la ISO 31000: 2009 con algunos ajustes respecto de los indicadores, factores inherentes y umbrales puede ser utilizado también para las cooperativas para el establecimiento de niveles de riesgo inherentes (Bolaños 2016).

La investigación basada en la norma ISO 31000:2009 permite desarrollar un modelo de gestión de riesgo de crédito para el sistema mutual, para este fin se establece el marco de referencia para la gestión del riesgo contemplando los factores del contexto interno y externo, se determina un modelo de política para la gestión del riesgo para el sistema mutual, se determinan los indicadores de gestión de riesgo de crédito que son el insumo para las etapas de identificación y monitoreo y se diseña e implementa el proceso para la gestión del riesgo tomando como ejemplo la mutualista más grande del sistema mutual; es decir, se identifican, analizan y evalúan los factores de riesgo para la mutualista más grande aplicando el modelo diseñado para el efecto, se obtiene el nivel de riesgo inherente de crédito para la mutualista más grande y se sugieren medidas de tratamiento y monitoreo del modelo (Bolaños 2016, 3).

Los indicadores de *desempeño* establecidos para la gestión de riesgo de crédito miden principalmente el *desempeño* y la *efectividad* de factores como la concentración, morosidad, calidad de la cartera, nivel de provisiones y permiten identificar en primera instancia el riesgo inherente de crédito de la entidad; posteriormente se utilizan en el proceso de monitoreo para conocer el resultado de las medidas de tratamiento que la

administración ha implementado para reducir el riesgo inherente a los niveles de tolerancia establecidos por la organización (2016, 130).

En el segmento de las cooperativas de ahorro y crédito de Ecuador, reguladas por la Resolución No. 011-2014-F del 4 de diciembre del 2014 que contempla la "Norma para la Prevención de Lavado de Activos y Financiamiento de Delitos incluido el Terrorismo en las Entidades de la Economía Popular y Solidaria", existe una investigación académica de Avigail Padilla sobre el "*Diseño de un Sistema de Gestión y Administración del Riesgo de Lavado de Activos basado en la ISO 31000 para la Cooperativa de Ahorro y Crédito Riobamba Limitada*" cuyo objetivo es implementar factores de gestión de riesgo que refuercen el control y análisis aplicado en la prevención de lavado de activos, orientado al cumplimiento legal. El sistema cooperativo es propenso a distinto tipo de riesgos, por ello es importante gestionarlos y establecer medidas dirigidas a la prevención de lavado de dinero que afecta al sistema financiero ecuatoriano, en especial a las cooperativas de ahorro y crédito que son instituciones financieras vulnerables en relación a las instituciones bancarias (2016, 4).

Según la investigadora, la cooperativa local muestra un nivel de riesgo inherente moderado, un sistema de control interno débil en materia de prevención de lavado de activos, ya que solo existe un solo análisis de los factores de riesgo los cuales son insuficientes para mitigar este riesgo al analizar el comportamiento transaccional, la existencia del actual método no les permite tener un adecuado monitoreo de las actividades de los socios y la ausencia de una matriz con factores de gestión de riesgo adicionales para el análisis del nivel de riesgo que tiene cada socio. Todos los problemas citados anteriormente tienen su origen en la falta de factores de gestión de riesgo que refuercen al existente para blindar mejor a la institución, lo cual se logrará con la aplicación de la ISO 31000 (Padilla 2016, 2). Los principales resultados de esta investigación académica se describen a continuación:

- Los nuevos factores de riesgo se agruparon de acuerdo a las tipologías necesarias de cada grupo, en este caso fueron: cliente, territorio, comportamiento transaccional, actividad inusual o sospechosa observada, canal de distribución y producto o servicio.
- El sistema (topaz trace) que utiliza la entidad para el análisis, evaluación y tratamiento de la gestión de riesgo no es suficiente para realizar un adecuado análisis financiero de los socios, por lo tanto no se puede aplicar un correcto

monitoreo y supervisión de las inusualidades y operaciones sospechosas dentro de la cooperativa.

- La norma ISO 3100 ha sido un gran aporte para reestructurar el manual de gestión y administración de riesgo, el cual permitirá a la institución cumplir con las exigencias legales y reglamentarias (2016, 223).

6. Marco teórico

La administración como es concebida hoy en día tuvo un largo proceso de evolución desde las civilizaciones y sociedades antiguas para adaptarse como organizaciones sociales y poder convivir en comunidad, partiendo de hechos importantes en la historia como la revolución industrial y antes el feudalismo en la edad media, la administración también ha ido evolucionando a través del tiempo, creando nuevas escuelas de pensamiento, corrientes y herramientas administrativas (Claude1968).

La administración según Henry Fayol es prever, organizar, dirigir, coordinar y controlar (Fayol 1916), partiendo de este concepto clásico se puede observar que la administración ha ido evolucionando a través de los tiempos. Con la revolución industrial y la creación de las grandes empresas, los estudios de administración formales surgieron con las escuelas clásica y científica que después se fueron agrupando de cierta forma que dieron lugar a la ciencia que se le nombró "Administración Científica" con sus teorías, enfoques, paradigmas y avances. La administración es un concepto muy amplio y cambiante dependiendo de las necesidades y percepción de quien la aplica llegando a la época donde ésta encuentra nuevas formas y herramientas para ser aplicadas, especialmente en el mundo empresarial (Morales 2015).

Las escuelas administrativas que surgen en el siglo XX se da por la necesidad de planear y guiar los esfuerzos a un bien común, donde se dieron los progresos del conocimiento humano a través de la denominada ciencia de la administración, siendo la administración *clásica* y *científica* las escuelas más destacadas y con más aportaciones para el manejo de las empresas y sus empleados (Chiavenato 2004).

La escuela clásica cuyo mayor exponente es Henry Fayol (1916) se centra en el énfasis por la estructura y las funciones que debe tener una organización para lograr la eficiencia. Esta teoría plantea a través de funciones y principios generales que las tareas

administrativas no deben ser cargas sino responsabilidad compartida entre todos los colaboradores de la empresa (Morales 2015).

La escuela de la administración científica surge a principios del siglo XX por la necesidad de especialistas que pudieren aumentar la productividad en las empresas, su fundador fue Frederick Taylor, cuya principal aporte fue sus estudios de tiempos y movimientos en líneas de ensamble para mejorar su eficiencia, que como plantea Fred Meyers en resumen permite dividir las operaciones realizadas en una empresa en partes y posteriormente diseñar e implementar métodos más eficientes para realizar cada actividad. En tanto que Henry Ford (1947) explotó y llevó a la práctica los principios de Taylor y Fayol transformado la tecnología como la organización del proceso de trabajo en un proceso productivo en línea (Meyers 2002).

Otras importantes escuelas que han colaborado con el desarrollo y evolución de la doctrina administrativa, es la escuela de relaciones humanas cuyo fundador es Elton Mayo (1880-1949) que plantea que al tratar a los trabajadores como seres humanos con necesidades psicosociales, tenía una influencia significativa sobre la productividad en la empresa, es decir el nivel de productividad no está determinado por la capacidad física del obrero o capacidad de producción –como sostiene la teoría clásica– sino más bien por factores psicosociales, como la integración a un equipo de trabajo y buen ambiente laboral (Rendón 2011).

La escuela estructuralista de Max Weber a fines de los años 50, trata de equilibrar los recursos de la empresa y estudia los problemas de la empresa y sus causas prestando especial atención a los aspectos de autoridad y comunicación, con base a cuatro elementos comunes: autoridad, comunicación, estructura de comportamiento y estructura de formalización. Esta escuela hace especial énfasis en la causa y efecto de las disfunciones dentro de la propia estructura organizacional (Hernández 2009).

La escuela neo-humanista, cuyo mayor representante es Abraham Maslow, que puedes ser considerada como la continuación de la teoría de la escuela de las relaciones humanas, estudia las necesidades del ser humano y considera que el hombre tiene diferentes necesidades y que estos ocupan cierta jerarquía, como las necesidades fisiológicas, seguridad, sociales, estima y autorrealización (Maslow 1954).

La escuela de sistemas administrativos fundada por el filósofo Ludwimg Bertanlanfy basa su teoría en que las funciones de un sistema dependen de la estructura, los sistemas pertenecen a otro mayor, siempre son abiertos; los seguidores de esta

escuela señalan que la administración se considera como un sistema desde el punto de vista de la teoría y la práctica (Espinosa 2009).

La escuela cuantitativa o matemática se consolida durante la segunda guerra mundial (1941), donde se dio uso a la aplicación de métodos matemáticos para optimizar diferentes aspectos de la empresa ya sea asignación de recursos, producción y provisión logística. El mayor aporte de esta escuela fue la investigación de operaciones; la escuela matemática también ha contribuido al desarrollo de la administración como la conocemos hoy en día, ya que la toma de decisiones es una parte fundamental de las empresas (Münch 2010).

La "*nueva era de la corriente administrativa"* aparece durante el último cuarto de siglo pasado y lo que va de este siglo, las organizaciones y doctrinas administrativas han tenido una gran transformación principalmente por la globalización y el vertiginoso avance tecnológico. Hoy en día existen nuevos enfoques, escuelas, herramientas, filosofías, técnicas administrativas desarrolladas en la época moderna para problemas que surgen igualmente en esta época contemporánea donde el incumplimiento de los objetivos de negocio se los asocia con y riesgos internos y externos (Morales 2015).

En 1986 los 14 puntos de William Deming fueron plantados en el libro "Calidad Productividad y Competitividad, la salida de la crisis" en el que se establece los principios de la filosofía gerencial para transformar la gestión empresarial (Deming 1986), las sugerencias de ese experto cambiaron la historia y el desarrollo económico del Japón, incidieron en el cambio de las teorías de management norteamericanas, y hoy tres décadas después se mantienen vigentes.

Con la sofisticación y diversificación igualmente de las actividades de riesgo, los estudiosos e investigadores proponen modelos de gestión y administración de riesgos con base a herramientas y enfoques (incluyen normas ISO) que permiten un control integral de los mismos. Estas herramientas y enfoques actuales son de utilidad para las empresas entre las que se puede mencionar: empowerment, just in time, benchmarking, coaching, calidad total, canvas, las cinco fuerzas, entre otros. Para el investigador Antonio Barba, la sociedad mundial, la globalización y la regionalización son fenómenos que han marcado la importancia de la influencia de las instituciones en las economías, las sociedades y las culturas. Una de las expresiones más relevantes en estos procesos es la aparición de nuevas formas de organización flexibles que han demostrado ser más eficientes que los modelos tradicionales (Barba 2000).

Con este antecedente, aparece entonces la relación y fusión del tema doctrinario de la administración con el control o mitigación del riesgo, que al igual que la evolución y desarrollo de las corrientes administrativas, el riesgo también surge y evoluciona como la posibilidad o probabilidad de que se produzca un contratiempo que se derive en un perjuicio, pérdida o daño. La administración o gestión del riesgo es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso dinámico e iterativo que consta de pasos, los cuales cuando son ejecutados en secuencia posibilitan una mejora continua en el proceso de toma de decisiones de la alta gerencia.

La administración del riesgo es un término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con un actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. La administración de riesgo es tanto identificar oportunidades como evitar o mitigar pérdidas y puede ser aplicado a todas las etapas de la vida de una actividad, función proyecto o producto (Quezada 2010).

En el presente caso de investigación, la administración de riesgo está enfocada a la prevención de lavado de activos y financiamiento de delitos, riesgos inherentes y propios de la actividad bancaria. Con el avance y evolución tecnológica de la época contemporánea la propuesta de valor cambia radicalmente con el advenimiento de la era digital, así como el nuevo mercadeo digital que obliga a las empresas a gestionar hábilmente su planificación estratégica para incorporar dicha tecnología a su modelo de negocio y de manera especial sus controles de mitigación de riesgos. De esta corriente de avances y cambios uno de los sectores donde más usos y aplicaciones se han dado y se ha transformado los diversos modelos y enfoques de control, es la industria financiera y más concretamente el sector bancario a nivel mundial. Así mismo, como se da un avance acelerado del desarrollo tecnológico, de forma paralela el riesgo se abre paso también como una potencial amenaza para la concreción de los objetivos y metas empresariales.

Hoy en día se está modificando el tradicional ciclo de Deming de mejora continua por un nuevo ciclo que gira alrededor de liderazgo, el compromiso de la dirección y la creación de valor de la organización, lo que la alinea mejor con un potencial futuro de sistema de gestión y en esa mejora toma un rol preponderante los lineamientos y preceptos de las normas ISO de gestión de riesgos.

Con este antecedente la presente investigación utiliza además la norma ISO 31000:2009 aceptada como referencia mundial de Gestión de Riesgos, que comprende y

establece un conjunto de principios que se deben satisfacer para que la gestión de riesgo sea eficaz. La norma recomienda a las organizaciones desarrollar, implementar y mejorar de manera continua un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización. Se utiliza el enfoque de la ISO 31000:2009 y no otros enfoques respecto al manejo y control del riesgo como el Estándar australiano, Basilea II y III o COSO ERP (modelos que contemplan el sistema de control interno de una organización), por cuanto esta norma ISO es más integral que abarca todos los aspectos claves y estratégicos de la organización, su estructura y entorno, que serán analizadas más adelante.

Capítulo primero
Conceptualización del riesgo de prevención de lavado de activos y financiamiento de delitos

1. Definición y generalidades de lavado de activos y financiamiento de delitos

Existen diferentes denominaciones para referir estos riesgos contemplados dentro de las distintas legislaciones, normativas, congresos, eventos y foros de discusión locales e internacionales sobre estos temas, donde han sido tratados y se los conoce como: “lavado de dinero”, “blanqueo de capitales”, “blanqueo de dinero”, “legitimación de capitales”, “conversión de capitales”, entre otros. En la presente investigación se utilizará el término “lavado de activos”, que es el que contempla la normativa local y la que más se adapta y utilizan las legislaciones del resto de países de la región.

1.1 Lavado de activos

Existen diversos conceptos y definiciones sobre este tema emitidos por varios autores, profesionales y estudiosos de esta materia y por los organismos de control estatales, todas éstos conectadas con el propósito fundamental de ocultar el origen ilícito de los recursos, para su posterior vinculación o circulación en el sistema económico de un territorio.

Para el autor Ricardo Alba el lavado de activos consiste en: “El conjunto de políticas, normas y procedimientos que tienen por objeto eliminar el riesgo de que los servicios de una organización, sean usados, por comisión o por omisión, para disimular o borrar el origen, naturaleza ubicación, propiedad o control de fondos provenientes del tráfico ilícito de drogas o de otras actividades ilegales” (Alba 2003, 21).

El Departamento del Tesoro de los Estados Unidos define al lavado de dinero como: “todas aquellas actividades para disfrazar activos financieros, de tal forma que puedan utilizarse sin que se detecte la actividad ilegal que los produjo” (USDT 2002).

En tanto que la Junta Bancaria del Ecuador en la Resolución JB-2012-2146, define el lavado de activos como: “el mecanismo a través del cual se oculta o disimula la naturaleza, el verdadero origen, ubicación, propiedad o control de los activos

provenientes de actividades ilegales, tanto en moneda nacional como extranjera, para introducirlos como legítimos dentro del sistema económico de un país" (JBE 2012, 3).

En términos generales y con base a las definiciones precedentes, se puede definir el lavado de activos como el proceso de ocultamiento de fondos de origen ilegal que ingresan en el sistema financiero u otro sector de la economía, para después de realizar una serie de movimientos económicos sin levantar alertas, poder integrar dichos fondos con apariencia de legitimidad y justificados, en la circulación habitual de una economía.

1.2 Financiamiento de delitos

El financiamiento de delitos no es nuevo en la vida cotidiana de la sociedad, ya que estas actividades de origen ilícito han estado y están presentes y tipificadas en las normas legales penales de la legislación del país.

Según la Unidad de Análisis Financiero y Económico: "el Financiamiento de Delitos, se refiere a la recaudación de dinero para realizar actos ilícitos, como terrorismo, sabotaje, subversión o cualquier acto ilegal que perjudique a la comunidad" (UAFE 2017).

La Junta Bancaria del Ecuador la define como una "actividad por la cual cualquier persona deliberadamente provea o recolecte fondos o recursos por el medio que fuere, directa o indirectamente, con la intención ilícita de que sean utilizados o a sabiendas que serán utilizados, en todo o en parte para cometer un acto o actos delictivos" (JBE 2012, 3).

Dentro del financiamiento de delitos está considerado todo acto ilegal o antijurídico que puede estar tipificado como un delito en la legislación del país. Los principales tipos de delitos que imperan a través de las actividades ilícitas y originan el lavado de activos son: la extorsión o el chantaje, narcotráfico, secuestro, enriquecimiento ilícito, contrabando, robo y asalto, tráfico de niños, trata de blancas, tráfico ilegal de armas, tráfico de órganos, testaferros, evasión fiscal, estafa, terrorismo, desfalco, peculado, soborno, corrupción, entre otros.

Desde el incidente terrorista del 11 de septiembre del 2001 en Nueva York y Washington, el gobierno estadounidense ha tomado el liderazgo en la labor de inteligencia, detección, seguimiento y lucha contra actividades que de manera directa o indirecta se realizan para apoyar el terrorismo, convirtiéndose este delito en una prioridad de control preventivo para las entidades financieras y reguladoras a nivel

mundial, para lo cual Estados Unidos como nación que encabeza esta lucha emitió la Ley Patriótica[1].

1.3 El vínculo entre el lavado de activos y el financiamiento de delitos

Como regla general, los recursos provenientes de cualquier actividad ilegal o de origen ilícito suelen incorporarse al proceso de lavado de activos, así como las procedentes de actividades legales pero no reportadas o subvaloradas ante los organismos de control fiscal, generalmente aquellas que son producto de la evasión tributaria que también constituye un delito. Sin embargo hay actividades que debido a la naturaleza ilícita donde se originan y por las repercusiones de deterioro social que éstas conllevan; en la mayoría, sino en todas las legislaciones de los países son catalogadas como "actividades ilícitas", perseguidas y sancionadas en calidad de delitos por las autoridades gubernamentales.

Uno de los objetivos comunes que comparten estos delitos es el ocultamiento del origen de fondos, ya que éstos fueron generados y son producto de una actividad ilegal que está tipificada como delito y sujeta a sanción en la legislación nacional. No obstante, para cumplir el ciclo del lavado de activos, estos fondos necesitan ser incorporados al sistema financiero u otro sector económico para ser lavados o legitimados, y es justamente donde se establece el vínculo concomitante entre el "origen ilícito" producto del delito precedente, con el mecanismo para "legitimar" dichos fondos, produciéndose un círculo vicioso que fomenta y soporta la estructura operativa de estos delitos.

1.4 Etapas del lavado de activos

Existe variada literatura de diferentes autores y organismos de control estatales que se han pronunciado sobre las etapas que comprenden el lavado de activos. Para

[1] La Ley USA PATRIOT vigente desde el 26 de octubre del 2001, contiene disposiciones contra el lavado de dinero, con el fin de combatir las bases financieras del terrorismo. Los bancos estadounidenses deben evitar otorgar o abrir cuentas de corresponsalía con bancos de papel (shell bank) del extranjero. Por lo que los bancos del resto del mundo que mantienen estas cuentas deben suscribir el Acta Patriótica donde asumen el compromiso de ejecutar acciones de control preventivo contra el lavado de dinero, el terrorismo y el transporte internacional de efectivo no autorizado.

efectos de la presente investigación, el lavado de activos es un proceso dinámico que comprende las etapas de colocación, estratificación e integración.

1.4.1 Colocación

Es la primera etapa del proceso y consiste en colocar físicamente los recursos (monetarios o en especies) en el sistema financiero, mediante diversas formas de introducir fondos de origen ilícito, ya sea a través de depósito en cuenta, inversión o compra de instrumentos monetarios (certificados de depósito, cheques de viajero, entre otros) o transferencia inicial de fondos. En esta etapa el objetivo primordial es introducir recursos en el sistema bancario formal sin levantar señales de alerta, en cuya instancia se pretende alejar los fondos de toda asociación directa o indirecta con el delito.

1.4.2 Estratificación

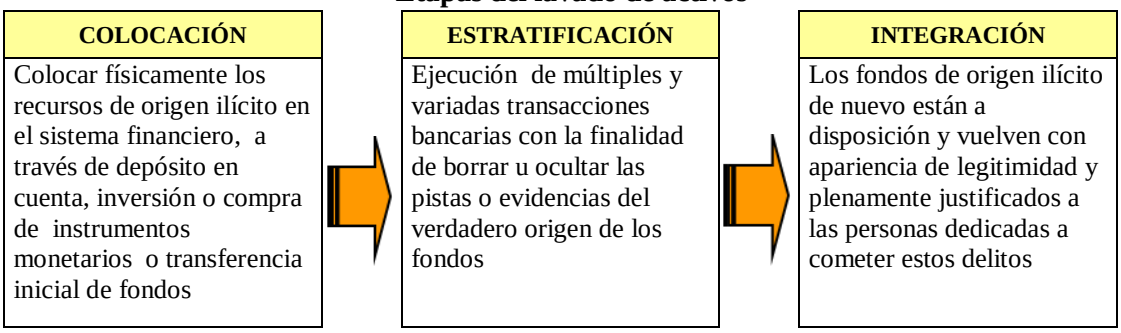
Consiste en la ejecución de una serie de operaciones financieras complejas para camuflar los recursos ilícitos, a través de la ejecución de múltiples y variadas transacciones tales como: transferencias a otras zonas dentro o fuera del país a cuentas de terceros, retiros en forma de transferencias electrónicas, inversiones, retiros fraccionados de fondos, cartas de crédito, adquisición de acciones, bonos o bienes de fácil transporte y venta (tarjetas prepago, tarjetas de crédito con saldos a favor, avales o garantías, entre otros). Esta estratificación tiene como finalidad borrar u ocultar las pistas o evidencias del verdadero origen de los fondos para evadir los procesos de control y sea más difícil para rastrear debido a su diversificación desde su origen por las múltiples transacciones efectuadas en el sistema financiero local o del exterior.

1.4.3 Integración

En esta última fase los fondos de origen ilícito que fueron colocados y diversificados a través del sistema financiero mediante la ejecución de varias transacciones o movimientos bancarios (locales o internacionales), toman apariencia de legítimos. Es decir los recursos líquidos de origen ilícito se convierten en cuentas bancarias, certificados de inversión, avales, garantías, bienes muebles o inmuebles o en negocios de fachada, al integrar y recuperar los fondos blanqueados a organizaciones o

empresas que realizan actividades legales y que aparentemente no tienen vínculos con el delito organizado y de nuevo están a disposición y vuelven con apariencia de legitimidad y plenamente justificados a las personas dedicadas a cometer estos delitos, una vez ocultado su origen y la actividad ilegal que los haya generado.

Gráfico 1
Etapas del lavado de activos



Fuente: Manual Uniforme para la Prevención de Lavado de Activos en América Latina
Elaboración propia

1.5 Principales técnicas y métodos para el lavado de activos

Son variadas las técnicas, modalidades y métodos que la imaginación y audacia de las organizaciones delictivas han logrado establecer para introducir en el sistema bancario fondos de origen ilegal, conformando verdaderas tipologías que fomentan estos delitos. La tipología comprende la clasificación y descripción de las técnicas más utilizadas para ocultar los recursos de origen ilícito, mismas que están constituidas de manera similar, poseen características comunes o siguen un patrón de comportamiento.

1.5.1 Según el Grupo de Acción Financiera Internacional de Latinoamérica

Producto de la investigación, análisis y consolidación de estas tipologías durante el periodo 2009 al 2016 por parte del Grupo de Acción Financieras Internacional de Latinoamérica[2] (GAFILAT) se han logrado consolidar y difundir estas técnicas. A continuación un resumen de estas técnicas emitidas por el GAFILAT.

1. Utilización de operaciones de comercio exterior y contrabando.

[2] El GAFILAT es una organización intergubernamental de base regional que agrupa a 16 países de Latinoamérica: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Uruguay con el propósito de combatir el lavado de dinero y el financiamiento del terrorismo.

2. Utilización de servicios de remesas y cambio de divisas, formales e informales y transporte físico de dinero en efectivo.
3. Lavado de activos a través de actividades y profesiones no financieras designadas.
4. Lavado de activos a través de desvío de fondos, procesos de licitación y otros actos de corrupción.
5. Lavado de activos a través de vehículos corporativos y estructura de personas jurídicas
6. Utilización de actividades de arrendamiento (leasing)
7. Utilización de nuevos servicios y productos de pago.
8. Incrementos inexplicables de riquezas por parte de personas físicas y uso de testaferros.
9. Financiamiento del terrorismo.

1.5.2 Según la Unidad de Análisis Financiero y Económico

En el Ecuador la UAFE producto de la recopilación y consolidación de los Reportes de Operaciones Inusuales Injustificadas (ROII) de las entidades financieras y sujetos obligados[3] que remiten información mensual a dicho organismo, ha establecido las siguientes tipologías de lavado de activos y financiamiento de delitos:

1. Captación ilegal de recursos.
2. Abuso de las facultades y atribuciones de los funcionarios públicos.
3. Exportaciones de bienes sobrevalorados.
4. Remesas recibidas del exterior, mercado cambiario de divisas, transporte transfronterizo de dinero.
5. Remesas recibidas del exterior, justificando el envío del dinero a familiares de los migrantes en el Ecuador. El dinero resultante de las remesas recibidas, termina en paraísos fiscales y por fronteras en otros países.
6. Mercado cambiario de divisas de billetes de alta denominación por billetes dólares de baja denominación, moneda local y transferencias (UAFE 2017).

[3] Son aquellas personas naturales o jurídicas que de forma obligatoria deben cumplir con las normas de prevención de lavado de activos y financiamiento de delitos y reportar periódicamente información de sus clientes, cuyas actividades no son catalogadas como financieras, como son: las bolsas y casas de valores, administradoras de fondos y fideicomisos, servicios de transferencia internacional de dinero, comercialización de vehículos, embarcaciones, naves o aeronaves, actividades inmobiliarias, entre otras.

1.6 El riesgo en el contexto del lavado de activos y financiamiento de delitos

La Resolución No. 380-2017-F emitida por la Junta de Política y Regulación Monetaria y Financiera (2017, 3) el 22 de mayo del 2017, referente a la Política para la Gestión Integral y Administración de Riesgos de las Entidades de los Sectores Financieros Público y Privado, define al riesgo de lavado de activos y del financiamiento de delitos como:

> La posibilidad de pérdida o daño que puede sufrir una entidad supervisada por su exposición a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades delictivas incluida el terrorismo, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades. Este riesgo se materializa a través de los riesgos asociados, estos son: el legal, reputacional, operativo y de contagio, a los que se expone la entidad, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera cuando es utilizada para tales actividades.

Para que exista y se materialice un riesgo dentro de un modelo, sistema, proceso o actividad es necesario que previamente exista una *probabilidad de amenaza* si se materializa dicho riesgo que afectará a los elementos indicados, además de una *condición de vulnerabilidad o impacto* dentro de los elementos sistémicos de una organización, como se analizará más adelante.

1.6.1 Factores de amenaza

Los factores de amenaza por lo general son de origen externo a la organización, de los cuales la entidad no tiene control o injerencia directa, la amenaza es un evento o serie de eventos que relacionados o no, tienen la probabilidad cierta de producir o materializar un efecto negativo, deterioro, pérdida o perjuicio en contra de personas o bienes, mismos que en función del grado de impacto o perjuicio son susceptibles de asignación de un grado de intensidad de dicho impacto. En el contexto del lavado de activos, estos factores pueden ser:

a) Los altos niveles de corrupción en todas las esferas y que han llegado en ciertos casos a involucrar a las estructuras del Estado, debilitando la propia institucionalidad y credibilidad de estas entidades, más aún si las organizaciones delictivas han logrado penetrar en las propias entidades de control y justicia.

b) La inclusión dentro del proceso de lavado de activos de verdaderas e innovadoras ingenierías financieras con la intervención de especialistas al servicio de organizaciones delictivas, les da buenas probabilidades de éxito en su cometido de ocultar el origen ilegal de los fondos, tras una compleja red de estructuras financieras.
c) La existencia de jurisdicciones y territorios denominados "paraísos fiscales" que brindan facilidades para ocultar la información del verdadero beneficiario final o de la persona que ejerce la administración y control de los fondos de las cuentas.
d) La existencia de grandes flujos de dinero o activos de origen ilícito alrededor de todo el mundo en poder del crimen organizado local y transnacional.
e) La intención de los actores del delito de introducir fondos ilegales en los sistemas económicos de un país a través de las entidades que no disponen de un eficiente y efectivo sistema de administración de riesgos.

1.6.2 Condición de vulnerabilidad

La condición de vulnerabilidad está dada por el nivel de solidez y efectividad de los controles preventivos generales y específicos para evitar la ocurrencia de una determinada amenaza. Estas condiciones al encontrarse al interior de la organización son susceptibles de procesos de tratamiento, administración y control siempre y cuando éstas sean identificadas y tratadas con la oportunidad y efectividad del caso. Esta condición pueda darse por la disfunción de los siguientes factores:

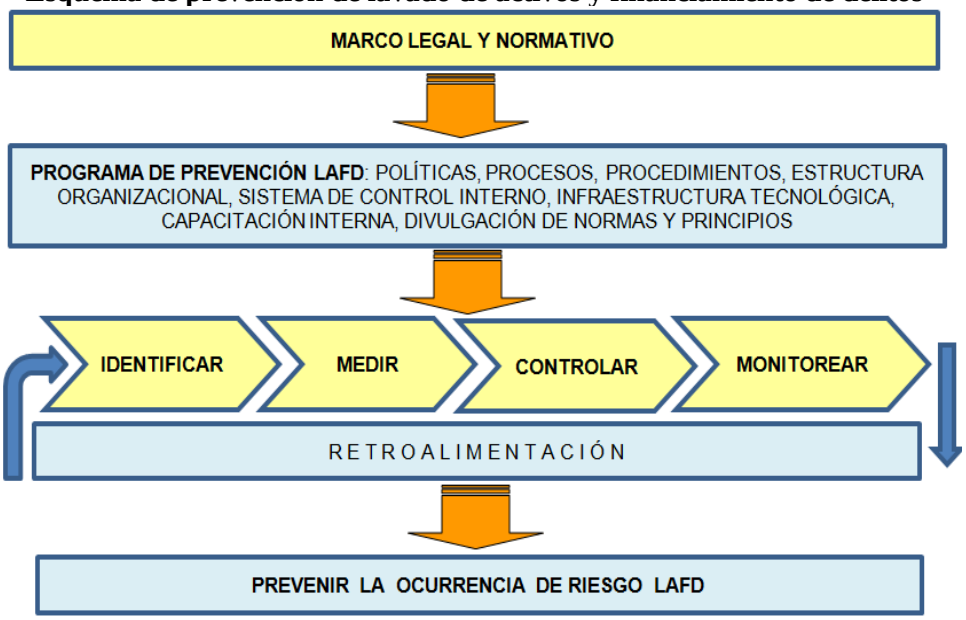
a) *Por la detección*. Cuando los controles no pudieren detectar y prevenir la amenaza, debilidad o disfunción del control existente que provocan su vulnerabilidad.
b) *Por la protección*. Son las acciones que se activan inmediatamente que el control de detección no pudo mitigar el riesgo, y que tienden a minimizar el impacto e incidencia de la amenaza.
c) *Capacidad de respuesta*. Referente a las acciones internas para el manejo de la amenaza, así como la creación de oportunidades de mejoramiento, reforzamiento o actualización del control vulnerado, para esto se requiere procesos iterativos de retroalimentación del sistema de gestión de riesgos.

1.6.3 Metodología actual de la administración y gestión de riesgos

1) Antecedentes de la metodología actual

Con base al marco legal que se ha emitido para el control y mitigación de estos delitos, el sector financiero ecuatoriano recoge e incorpora las definiciones de la ley local dentro de sus sistemas de administración de riesgos. Para construir y reforzar una metodología también se utiliza como apoyo el marco de referencia pragmático de las metodologías de ciertos países de la región que cuentan con legislaciones más avanzadas, es el caso de Colombia, que en el 2008 expidieron la metodología del Sistema de Administración de Riesgos de Lavado de Activos y Financiamiento del Terrorismo (SARLAFT) que incluye con énfasis la ponderación de las variables cualitativas y cuantitativas de los factores de riesgo dentro del sistema.

Gráfico 2
Esquema de prevención de lavado de activos y financiamiento de delitos



Fuente: Normativa de prevención de lavado de activos
Elaboración propia

En el caso del país, gran parte del contexto ideológico del enfoque del riesgo del SARLAFT está inmersa en la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos y demás resoluciones complementarias emitidas por la Junta de Política y Regulación Monetaria y Financiera (JPRMF) en esta materia según lo dispone el Código Orgánico Monetario y Financiero, con base a las cuales los bancos desarrollan sus actuales programas y sistemas de administración de riesgos

2) Alcance actual del programa de administración de riesgos

Los bancos privados locales que prestan servicios de intermediación financiera, tienen la responsabilidad y obligatoriedad de contar con un programa de administración de riesgos de prevención de LAFD en sus diferentes etapas de gestión, que se refiere a la identificación, medición, evaluación, control y monitoreo de estos riesgos.

a. Programa de prevención de lavado de activos y financiamiento de delitos

El esquema general actual de prevención de riesgos de las entidades bancarias del país (con base al SARLAFT), está contenido en los "Programas de Cumplimiento de Prevención de Lavado de Activos y Financiamiento de Delitos" que los bancos planifican y desarrollan anualmente (SBE 2013).

Tabla 1
Elementos del programa de prevención de LAFD

Elementos	Contenido del programa de prevención de LAFD
Políticas	Lineamientos y directrices que deben adoptar las entidades sujetas al control del organismo regulador, orientadas a prevenir y mitigar estos riesgos. Cubren todos los productos y servicios financieros, sin importar que se realicen en efectivo o no, ejecutadas a nivel local o en el exterior.
Procedimientos	Documentados y aplicables a su operatividad de negocio, en especial para identificar, medir, controlar y monitorear las transacciones de los clientes en función del análisis de los criterios de riesgo definidos.
Procesos	Conjunto de actividades definidas por la organización, que están interrelacionadas entre sí y que al interactuar con los elementos de entrada de los proceso de control de LAFD los compila en un orden secuencial y los convierte en datos de salida o resultados
Manual de prevención LAFD	Los sujetos obligados a reportar a la UAFE deben contar con el manual respectivo, que contemple procesos y procedimientos enfocados al control preventivo de LAFD
Estructura organizacional	El directorio debe aprobar las políticas y procedimientos de control, el código de ética, el manual de prevención de LAFD, el plan de trabajo anual de la unidad de cumplimiento, designar al oficial de cumplimiento y miembros del comité de cumplimiento, conocer los informes emitidos por el oficial o comité.
Sistema de control interno	Se debe efectuar una evaluación objetiva del sistema de control de riesgos de prevención de LAFD, a fin de que se puedan determinar sus disfunciones y debilidades e informar a las instancias pertinentes con la oportunidad del caso para la toma de acciones correctivas
Infraestructura tecnológica	Se debe contar con adecuados sistemas tecnológicos como soporte de la gestión automatizada del sistema de gestión de riesgos de prevención de LAFD, de acuerdo a su necesidad, tamaño de la organización y complejidad de su modelo de negocio
Capacitación interna	Funcionarios a cargo del control deben ser capacitados, puesto que el fin de estos delitos es buscar las vulnerabilidades de control de las organizaciones, por lo que se requiere personal técnico capacitado que administre, precautele y minimice estos riesgos
Divulgación de normas y principios	Información referente al sistema de gestión de riesgos debe ser bajada y conocida por los colaboradores internos y cada responsable los cumpla en el ámbito de su competencia, en especial aquellos que están a cargo de preparación los reportes de información internos y externos

Fuente: Superintendencia de Bancos
Elaboración propia

b. Sistema de gestión de evaluación de riesgo

Según la normativa emitida por la Junta Bancaria, las políticas y procedimientos de control deben ser definidos y consolidados en una *matriz de riesgo* sobre la base de factores y criterios de riesgo establecidos por la entidad financiera, considerando:

- Categorías previamente definidas, permitirán a través de matrices de riesgos, segmentar a los clientes y obtener su perfil de riesgo y combinar el riesgo de cada uno de los factores identificados.
- La metodología que se adopte, según las necesidades y características de cada institución, debe permitir el diseño de factores y criterios de riesgo y cuidar que las ponderaciones y categorías que se implemente se ajusten a la operatividad de la institución y debe ser documentada y aprobada por el directorio.
- Los resultados que se obtenga de la matriz de riesgo servirán de base para la realización del monitoreo permanente, adoptando las medidas de debida diligencia hacia los clientes que corresponda.
- Los mecanismos de control adoptados por las instituciones del sistema financiero serán aplicados a todas las transacciones y de manera reforzada a aquellas cuyas cuantías individuales sean iguales o superiores a US $ 10.000 o su equivalente en otras monedas, así como a las transacciones múltiples cuyo monto, en conjunto, dentro de un periodo de treinta días igualen o superen los US $ 10.000 o su equivalente en otras monedas, cuando sean transacciones únicas, es decir, sean realizados en beneficio de una misma persona, para lo cual se puede utilizar un software o sistemas de monitoreo aplicable a las necesidades de cada entidad financiera (JBE 2012, 7).

c. Sistema de monitoreo

Por el volumen de operaciones que procesan las entidades bancarias y para aprovechar las facilidades que proporciona la tecnología, es recomendable desarrollar o adquirir un software especializado. Este sistema de monitoreo representa una valiosa herramienta automatizada de manejo de datos, que facilita la compilación de información referente a la identificación de los factores de riesgo (actividad económica, zona geográfica, edad, nacionalidad, tipo de transacciones, montos, productos), valorar estos factores y en función de ellos determinar las operaciones atípicas que salen fuera del perfil transaccional del cliente, aplicando reglas, modelos matemáticos, estadísticos y filtros de datos para evaluar las alertas emitidas en el proceso de monitoreo.

Capítulo segundo
Marco normativo en materia de lavado de activos y financiamiento de delitos del sistema bancario del Ecuador

1. Marco normativo

La norma ISO 31000:2009 utilizada en la presente investigación está estructurada en cinco capítulos, el primero contempla el objeto y campo de aplicación de la norma; el capítulo dos contempla los términos y definiciones; el capítulo tres el propósito de la norma de creación y protección del valor de la gestión de riesgo que se encuentran reflejados en el marco de trabajo y en los once principios de dicha gestión; el capítulo cuatro trata la estructura de la guía y el diseño de la estructura del marco de trabajo para apoyar la integración de la gestión del riesgo en la organización en todas sus actividades y funciones; por último está la sección de los atributos de la mejor gestión del riesgo referentes a la mejora continua, plena responsabilidad de los riegos, aplicación de la gestión de riesgos en todas las decisiones, comunicación continua y la plena gobernanza de la organización.

El desarrollo de la presente investigación demanda además el estudio del marco legal complementario que regula estas actividades de control de riesgos. Al tratarse de un tema de implicación y connotación mundial, las regulaciones promulgadas en materia de gestión y administración de estos riesgos han sido emitidas por los principales organismos internacionales de control de Estados Unidos. Entre los que se encuentran el Consejo Federal de Inspecciones Financieras (FFIEC por sus siglas en inglés), Departamento del Tesoro, Grupo de Acción Financiera Internacional (GAFI), la Oficina de Control de Activos Extranjeros (OFAC), FinCEN (Red de Lucha contra Delitos Financieros de USA), resoluciones de la Organización de las Naciones Unidas, la Ley Patriótica de Estados Unidos, entre otros.

A nivel local el marco normativo está dado a través de la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos –que la administran la Superintendencia de Bancos y la Unidad de Análisis Financiero y Económico–, que está basada en el marco conceptual de control de los organismos y leyes internacionales indicadas. Además como

complemento del marco local la presente investigación se fundamenta en el Código Orgánico Monetario y Financiero y el Código Orgánico Integral Penal.

Un análisis comparativo sobre la aplicación de los diversos enfoques de gestión para la administración de los riesgos objeto de estudio, con la finalidad de establecer las razones por las que el marco teórico de referencia de la norma ISO 31000:2009, es más efectivo que otros, en el tratamiento de estos riesgos, se menciona a continuación.

1) Regulación de Basilea II y III

La norma de Basilea II –publicado en 2004– es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con el objeto de establecer los requerimientos de capital necesarios para asegurar la protección de las entidades frente a los riesgos financieros y operativos. Los bancos con mejor calidad de riesgo requieren menores niveles de capital y los más débiles los requieren mayores. Porque la competencia en pie de igualdad no debe entenderse referida a niveles iguales de capital, proporcionales simplemente con el tamaño del balance, sino como niveles de capital igualmente proporcionados a los riesgo reales de cada banco (De Juan, 2005).

Esta regulación está enfocada en el nivel apropiado de capital más que en el riesgo operativo o de prevención de lavado de activos, ya que la regulación sobre los requerimientos de capital empieza a quedarse obsoleta ante los avances en la gestión de riesgos que amplían su espectro de control.

Según el Bank for International Settlements (BIS) la norma de Basilea III es un conjunto de medidas internacionales que el Comité de Supervisión Bancaria de Basilea desarrolló en respuesta a la crisis financiera de 2007 a 2009 (hipotecas subprime). El objetivo de dichas medidas es reforzar la regulación, la supervisión y la gestión de riesgos de los bancos, cuyo enfoque está dirigido hacia los requerimiento de "*capital*" que incluye la cobertura de riesgo de crédito, de mercado, de ajuste de valoración del crédito, la contención del apalancamiento, la gestión de supervisión del riesgo y la disciplina del mercado; en tanto que el requerimiento de "*liquidez*" incluye los estándares internacionales de liquidez y vigilancia supervisora (BIS 2010). Los puntos críticos de esta regulación financiera según la FELABAN, se resumen en:

a. *Comparabilidad*.- en aras de una mejor comparación entre jurisdicciones, se ha perdido la capacidad de predicción con base a modelos.

b. *Simplicidad*.- la tendencia a usar modelos estándar -en detrimento del uso de modelos internos- puede sacrificar competitividad de las entidades al restringir los modelos propios. Como es el caso de la norma IS0 31000:2009 que con base

a un enfoque integral para la administración del riesgo, cada entidad puede diseñar el modelo de gestión a su medida de acuerdo a su percepción, análisis y nivel de tolerancia de los riesgos.

c. *Prociclicidad*.- subsisten dudas sobre los modelos actuales que no incentivan que las variables bancarias sean proclives a seguir el ciclo económico.

d. *Prevención de crisis*.- aunque los acuerdos de supervisión bancaria de Basilea operan desde los años 70, y pese a cumplirse en muchos países, esto no ha sido suficiente para la ocurrencia de crisis bancarias en Asia (1997), Rusia (1998), Brasil (1999), Argentina (2001) y Estados Unidos (2008). La mayor regulación, supervisión y vigilancia pone en dificultades al sector y su eficacia es al menos discutible. (FELABAN 2018).

Las normas de Basilea si bien es cierto que tratan de regular y fortalecer el marco de la gestión del riesgo de las entidades bancarias, sobre todos los riesgos financieros, estas recomendaciones son aplicables al fortalecimiento financiero de las organizaciones; sin embargo, para el caso del riesgo reputacional que está ligado a la prevención de LAFD no es suficiente dicho estándar internacional.

2) Estándar australiano

El estándar AS/NZS 4360:1999 se centra en la identificación y tratamiento de los riesgos para aumentar la probabilidad de éxito y reducir tanto la probabilidad de fracaso como la incertidumbre de lograr los objetivos y metas generales de la organización. La administración de riesgo debe estar incorporada dentro de la organización a través de los procesos de estrategia y presupuesto. Este estándar se centra en las etapas: establecer el contexto, identificación, análisis, evaluación, tratamiento y el monitoreo en curso de los riesgos. (Cuello 2013). La aplicación metodológica del estándar australiano implica el levantamiento de eventos de riesgo para dar paso a la formulación de la matriz de implementación de controles y matrices de riesgo.

En las conclusiones de la investigación académica sobre "*Viabilidad y efectos de la aplicación del estándar australiano como sistema de administración del riesgo de lavado de activos y financiamiento del terrorismo-SARLAFT en el sector cooperativo ecuatoriano*" se expone que está demostrada la viabilidad de la implementación del estándar australiano en la administración del riesgo en el sistema cooperativo del Ecuador, se demostró la utilidad de esta metodología porque proporciona bases para la identificación de los riesgos del entorno, estratégicos y financieros (Morillo 2017). Es

decir como un antecedente cierto de investigación académica el estándar australiano es aplicable eficazmente al sector cooperativo local.

La norma ISO 31000:2009 frente a las limitaciones del alcance integral de tratamiento del riesgo del estándar australiano, es más *efectiva* debido a que ayuda a identificar las *oportunidades* y *amenazas* al efectuar una *evaluación integral de riesgos*, además de cumplir con las exigencias legales, minimizar pérdidas, integrar los objetivos de control dentro de los objetivos estratégicos de la organización.

Ciertos bancos locales, sino todos en la práctica utilizan directa o indirectamente las directrices del estándar australiano, ya que sus programas de gestión del riesgo de LAFD lo desarrollan a partir de la identificación del riesgo hasta llegar a la etapa del monitoreo y revisión, es decir los sistemas actuales no contemplan muchas veces ni siquiera los lineamientos que demanda el proceso de gestión del riesgo que establece el estándar australiano, ya que si bien es cierto que desarrollan una metodología para gestionar el riesgo, éste estándar no cubre un enfoque integral ni está apalancado en un marco de trabajo y principios previamente planificados y definidos.

3) COSO ERM 2017

Dentro del COSO ERM 2017 (Committee of Sponsoring Organizations of the Treadway Commission) de gestión de riesgo de la empresa que destaca la importancia de considerar el riesgo tanto en el proceso de establecimiento de estrategias como en el desempeño de la administración, se obtienen diferentes beneficios que proceden de: conocer la *metodología para identificar todos los riesgos*, *documentarlos* y además de identificarlos de forma específica con un medidor de desempeño para poder conocer el impacto en el negocio. La gestión de riesgos empresariales (ERM) está asociado al Gobierno Corporativo en la medida que provee información a la dirección superior respecto a los riesgos más significativos y a la forma como los mismos están siendo administrados (Bueno 2010, 13).

Esta versión, según la investigadora Dennisse Vaca ayuda a las organizaciones a tener beneficios tangibles en su administración de riesgos. Este nuevo marco se encuentra compuesto por los 5 componentes (gobierno y cultura; establecer objetivos; desempeño; evaluación y revisión; información, comunicación y reporte) y 20 principios, cuyos beneficios son:

- Conocer la metodología a utilizar para controlar los riesgos.
- Saber documentar los riesgos desde la estrategia para que puedan ser medidos.

- Establecer un medidor de desempeño para saber hacia dónde van los riesgos y cuál es el impacto que genera en el negocio.

Una visión global de negocio basada en la administración de riesgos genera en el accionista, en el consejo de administración, a los empleados, clientes y proveedores una sensación de tener un ambiente de confianza (Vaca 2017).

La investigación de Alcina De Sena Portugal menciona que COSO sobre gestión de riesgo empresarial es una valiosa contribución a la práctica emergente de la gestión de riesgos empresariales (ERM), pero tiene serias limitaciones al no proporcionar un estándar viable para identificar la efectividad del ERM. Su definición de riesgo desvía la atención de las oportunidades y de las incertidumbres que quedan fuera de su perspectiva de sistemas racionales cerrados, por lo que muchas empresas prefieren utilizar el estándar ISO 31000:2009 porque es más fácil trabajar con él y fue bastante innovador mucho antes que la actualización de ERM en 2017 (De Sena 2017, 78).

La administración de riesgos con base al COSO ERM todavía se realiza una vez al año con el plan de auditoría interna de la organización, en cambio la norma ISO 31000:2009 transforma la cultura sobre cómo realizar la administración de riesgos de manera continua en el transcurso de un ejercicio económico, por lo que se lleva a cabo una estrategia clara sobre cómo llevar adelante la gestión flexible y dinámica de tratamiento de los riesgos. Se puede utilizar la norma ISO 31000:2009 en la toma de decisiones planificadas de forma consensuada entre todas las partes de la organización.

El marco normativo en materia de prevención de LAFD emitido para el efecto es el componente y base fundamental del sistema de administración de riesgos, ya que en función de éste se debe establecer su alcance y profundidad, además cada vez que exista reformas o actualizaciones a las leyes pertinentes (locales o del exterior), la entidad debe tener procedimientos operativos internos para identificar todas y cada una de las nuevas regulaciones específicas que demandan realizar modificaciones al sistema.

1.1 Marco normativo local

1.1.1 Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos

Esta ley fue emitida el 21 de julio del 2016 por la Asamblea Nacional y es aplicable a todas las actividades económicas susceptibles de ser utilizadas para cometer

estos delitos. Esta Ley tiene como finalidad prevenir, detectar y erradicar estos delitos, así mismo señala a la Junta de Política y Regulación Monetaria y Financiera (JPRMF) para ejercer la rectoría de la materia de prevención del lavado de activos y el financiamiento de delitos y emitirá las políticas públicas, la regulación y supervisión monetaria, crediticia, cambiaria, financiera, de seguros y valores, para la prevención del LAFD (EC 2016, art.9). Los objetivos de la ley se describen a continuación:

- Detectar la propiedad, posesión, utilización, oferta, venta, corretaje, comercio interno o externo, transferencia gratuita u onerosa, conversión o tráfico de activos, que fueren resultado o producto de los delitos de los que trata la ley, o constituya instrumentos de ellos, para aplicar las sanciones correspondientes.
- Detectar la asociación o tentativa para ejercer las actividades citadas en el punto anterior o su tentativa, la organización de sociedades o empresas que sean utilizadas para este propósito, su gestión y financiamiento, para la aplicación de las sanciones respectivas.
- Realizar acciones para recuperar los activos producto de estos delitos cometidos en el territorio nacional y que se encuentran en el exterior (EC 2016, art.1).

Respecto a la información, esta ley puntualiza que se debe mantener en medios fehacientes, fidedignos y confiables la información de todos los clientes de la entidad financiera, así como mantener cuentas y operaciones en forma nominativa –nunca cifradas o codificadas–, registrar y reportar bajo responsabilidad personal e institucional cada mes a la UAFE en la estructura y contenido definidos las operaciones y transacciones que individual o acumulada sean igual o superior a US $ 10.000 en beneficio de una misma persona en un período de treinta días, además de reportar las operaciones o transacciones inusuales injustificadas de clientes, así como sus propias operaciones nacionales e internacionales cuya cuantía sea igual o superior a US $ 10.000 o su equivalente en otras monedas (EC 2016, art.4).

1.1.2 Código Orgánico Monetario y Financiero

El Código Orgánico Monetario y Financiero[4] (COMF) tiene por objeto regular los sistemas monetario y financiero, así como los regímenes de valores y seguros del

[4] El COMF publicado en Registro Oficial No. 332 del 12 de septiembre del 2014, crea la Junta de Política y Regulación Monetaria y Financiera, en reemplazo de la Junta Bancaria del Ecuador. El control del mercado de seguros y valores es transferido a la Superintendencia de Compañías, Valores y Seguros.

Ecuador, además de establecer el marco de políticas, regulaciones, supervisión, control y rendición de cuentas respectivas, basados en los principios de la prevalencia del ser humano por sobre el capital, la subordinación de estos sectores como instrumentos al servicio de la economía real, el ejercicio de la soberanía monetaria y financiera y la inserción estratégica internacional, la inclusión y equidad, el fortalecimiento de la confianza y la producción de los derechos ciudadanos (EC 2014, arts.1-4).

El código señala a la Superintendencia de Bancos como un organismo técnico de derecho público, que efectuará vigilancia, auditoría, intervención, control y supervisión de las actividades que ejercen las entidades públicas y privadas del Sistema Financiero Nacional, cuya función principal es verificar el cumplimiento de las disposiciones del código y las regulaciones dictadas por dicha Junta, en lo que corresponde a las actividades financieras de las entidades de este sector, para lo cual debe establecer programas de supervisión intensiva a dichas entidades (EC 2014, art.62).

En materia de prevención de LAFD este código dentro del sistema monetario, menciona que las remesas de dinero físico para garantizar el circulante en la economía nacional, desde y hacia el Ecuador, solo podrá ser efectuada por el Banco Central y excepcionalmente por las entidades del sistema financiero nacional, de acuerdo con las normas que para el efecto emita la Junta y cumpliendo las disposiciones de la Ley de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos (EC 2014, art.96).

En cuanto a las disposiciones comunes para el sistema financiero nacional se dispone que las infracciones sobre el LAFD como el terrorismo se sancionará de conformidad con las disposiciones del COIP y la ley indicada; en tanto que sobre el control y prevención de lavado de activos, las entidades del sistema financiero nacional tienen la obligación de establecer sistemas de control interno para la prevención de delitos, incluido el LAFD como el terrorismo, en todas las operaciones financieras (EC 2014, arts. 243-4).

1.1.3 Código Orgánico Integral Penal

El Código Integral Penal[5] (COIP) tipifica y sanciona los delitos de lavado de activos, omisión de control de lavado de activos, terrorismo, financiación del

[5] EL COIP publicado mediante Registro Oficial No. 180 del 10 de febrero del 2014.

terrorismo, delincuencia organizada y otro tipo de delitos que generan recursos económicos que pueden ser objeto de lavado de activos. Este marco legal permite al país cubrir con las exigencias internacionales de incorporar y puntualizar en este código el financiamiento del terrorismo y a las organizaciones calificadas como terroristas.

En el COIP está tipificado el delito de la producción, financiamiento, suministro, siembra o cultivo y tráfico ilícito de sustancias catalogadas sujetas a fiscalización o de precursores químicos, relacionadas a la producción, fabricación y extracción de estas sustancias ilícitas que usualmente derivan en lavado de activos (EC 2014, arts. 219-23).

Dentro de la sección de Graves Violaciones a los Derechos Humanos y Delitos Contra el Derecho Internacional Humanitario, se trata puntualmente sobre los delitos contra la humanidad, trata de personas y las diversas formas de explotación referente al tráfico ilegal de órganos, explotación sexual y prostitución en sus diversas modalidades, tipifica una serie de delitos que generan recursos de origen ilegal relacionados al lavado de activos con la ejecución de delitos precedentes (EC 2014, arts. 91-104).

1.2 Marco normativo internacional de lavado de activos y financiamiento de delitos aplicable al sistema bancario del Ecuador

Por las operaciones internacionales que realizan los bancos privados y al ser parte de un mundo económico globalizado, éstos tienen la responsabilidad de observar y cumplir ciertas normas internacionales inherentes a estas operaciones para poder ofrecer una gama de servicios a sus clientes, y para su propio giro operativo como son: las cuentas de corresponsalía[6], operaciones de financiamiento o préstamos externos, avales, garantías bancarias, entre otros.

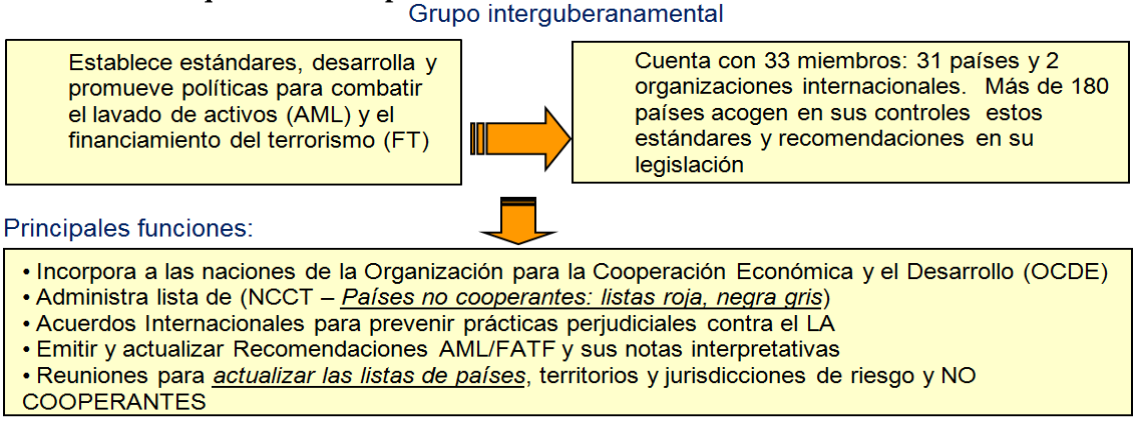
1.2.1 Recomendaciones del Grupo de Acción Financiera Internacional

El Grupo de Acción Financiera Internacional (GAFI) es un organismo intergubernamental creado en París en 1989 con el auspicio de los siete países industrializados (G7: Estados Unidos, Alemania, Francia, Japón, Reino Unido, Italia y

[6] Corresponsal es una entidad financiera local o externa con la cual se mantiene relaciones comerciales o bancarias, previa firma de un convenio. Es una cuenta abierta por un banco a fin de que otro banco (local o extranjero) reciba depósitos o realice pagos u otros desembolsos en nombre del banco que apertura dicha cuenta o para encargarse de otras transacciones relacionadas con el banco titular de la cuenta.

Canadá), cuyo propósito es desarrollar, promover medidas y recomendaciones estandarizadas de control preventivo y las mejores prácticas de control a ser consideradas por sus miembros en esta materia, para combatir principalmente el lavado de activos y el financiamiento del terrorismo.

Gráfico 3
Esquema del Grupo de Acción Financiera Internacional – GAFI



Fuente: Grupo de Acción Financiera y Control - GAFI
Elaboración propia

Las recomendaciones son lineamientos para el control preventivo del lavado de activos en las cuales se basan la mayoría de legislaciones de los países miembros, inicialmente fueron emitida cuarenta recomendaciones y en el año 2012 fueron actualizadas nueve recomendaciones adicionales para el control preventivo del financiamiento del terrorismo.

Tabla 2
Detalle de las recomendaciones del GAFI

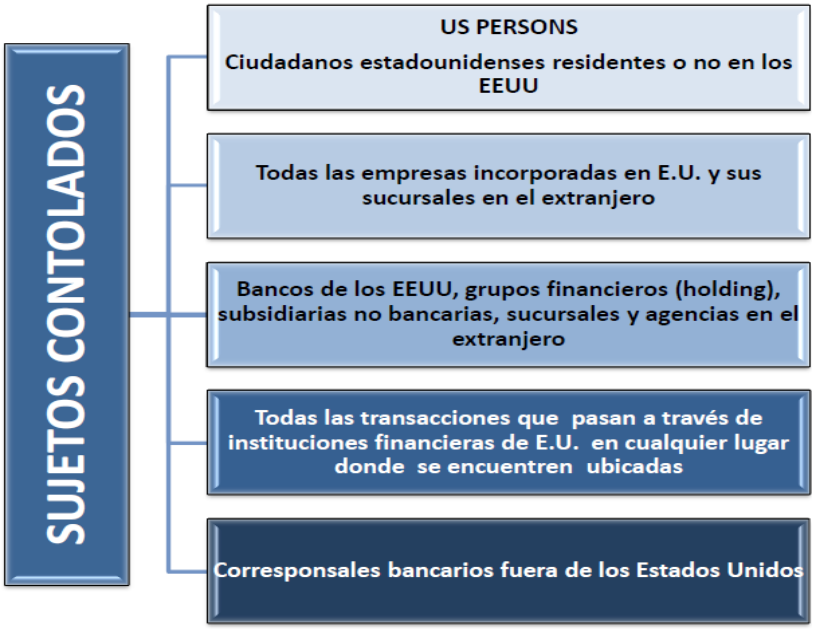
Cuarenta recomendaciones	Nueve recomendaciones
Grupos de Normas	1) Ratificación y ejecución de los instrumentos de las Naciones Unidas
Políticas y coordinación anti-lavado de activos y contra la financiación del terrorismo.	2) Tipificación del financiamiento del terrorismo y el lavado de dinero asociado.
Lavado de activos y decomiso	3) Congelamiento y decomiso de activos terroristas
Financiamiento del terrorismo y proliferación de armas de destrucción masiva	4) Reporte de transacciones sospechosas relacionadas con el terrorismo
Medidas preventivas enfocadas a la debida diligencia del cliente y mantenimiento de registros	5) Mayor cooperación internacional referente a la ayuda legal mutua e intercambio de información
Transparencia y beneficiario final de las personas jurídicas y otras estructuras jurídicas	6) Sistemas alternativos de envío de fondos
Facultades y responsabilidades de las autoridades competentes y otras medidas institucionales	7) Transferencias electrónicas (información completa del ordenante y beneficiario).
Cooperación internacional	8) Organizaciones sin fines de lucro
	9) Controles para los correos de efectivo y el transporte transfronterizo de efectivo

Fuente: Recomendaciones GAFI -GAFISUD
Elaboración propia

1.2.2 Regulaciones de la Oficina de Control de Activos Extranjeros

La Oficina de Control de Activos Extranjeros (OFAC) de Estados Unidos administra e impone sanciones económicas y comerciales con base a la política exterior estadounidense y sus objetivos de seguridad nacional; dichas sanciones están dirigidas a ciertos países extranjeros, personas y organizaciones delictivas terroristas y narcotraficantes internacionales y aquellos que participen en actividades relacionadas con la proliferación de armas de destrucción masiva, para lo cual existen listas con información restrictiva para el control preventivo antes de procesar una transacción.

Gráfico 4
Sujetos controlados por la OFAC



Fuente: Manual de Inspección Anti-lavado de Dinero del FFIEC
Elaboración propia

La verificación en listas de control debe aplicarse a clientes, ordenantes y beneficiarios de transferencias, empleados, accionistas, proveedores y corresponsales, durante los procesos de vinculación y durante su permanencia o relación con el banco.

1.2.3 Organización de las Naciones Unidas

El Ecuador es suscriptor y miembro de la “Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional”, cuyo propósito es promover la

cooperación entre los países miembros, para prevenir, combatir más eficazmente la delincuencia organizada transnacional. La Convención de Naciones Unidas contra el tráfico ilícito de sustancias sujetas a fiscalización (Convención de Viena) firmada en 1988, hicieron un llamado a los firmantes para que consideren el lavado de dinero como un delito, cuyo objetivo era el de *asegurarse que el secreto bancario* no constituya una barrera a las investigaciones y más bien se fomente la cooperación internacional.

La Resolución 1373 apoyado por el gobierno de Estados Unidos, contra el terrorismo y a ésta se le adicionó una resolución en la que se le solicitaba a todos los miembros de la ONU que considerarán ilegal el permitir que las personas designadas como terroristas tuvieran acceso a sus fondos. Las continuas actualizaciones de la lista de terroristas por parte de la ONU, en consecuencia, deben ayudar a eliminar la seguridad financiera para este tipo de delitos y a atacar de raíz al problema del terrorismo (Lara 2002, 31).

1.2.4 La Ley Patriótica

Es una ley federal de Estados Unidos que entró en vigencia el 26 de octubre del 2001 como respuesta a los atentados terroristas del 11-S, contiene disposiciones contra el lavado de dinero, con el fin de atacar las bases financieras y de inteligencia del terrorismo, apoyados en el *conocimiento del cliente y la debida diligencia* efectuada por parte de las instituciones financieras.

Si bien es cierto que los bancos estadounidenses deben evitar otorgar servicios financieros (directa o indirectamente) o abrir cuentas de corresponsalía con bancos extranjeros de "fachada o de papel", el Departamento del Tesoro ha establecido requisitos mínimos para la apertura de cuentas para bancos del exterior, que por la globalización económica del mundo estas cuentas son imprescindibles para el giro operativo de los negocios de los bancos extranjeros, quienes por la presente regulación deben entregar *información oficial* referente a su composición accionaria, información financiera, cuestionarios y certificaciones de aplicación de control de lavado de activos y financiamiento del terrorismo, suscripción del Acta Patriótica, entre otros.

Capítulo tercero

Cumplimiento de controles de lavado de activos y financiamiento de delitos y propuesta de mejora al sistema de gestión de administración de riesgos

1. Estructura del sistema bancario ecuatoriano

La estructura del sistema bancario está basada en el régimen designado por los organismos de administración y control, como es la JPRMF, la Superintendencia de Bancos y el Banco Central. Este último, apoya a la gestión operativa de los bancos al administrar el sistema nacional de pagos y sistemas auxiliares, garantizar el suministro y la distribución de las especies monetarias y dinero en el país y evaluar y controlar la cantidad de dinero de la economía a través del encaje bancario (EC 2014, art. 36).

1.1 Las entidades bancarias del sistema ecuatoriano

En la actualidad el sistema bancario privado está integrado por veinte y dos (22) bancos activos que operan en el mercado de intermediación financiera, estos son:

Tabla 3
Catastro de bancos privados que operan en Ecuador a abril del 2017

No.	Código	Nombre de la institución	No.	Código	Nombre de la institución
1	1002	BP AMAZONAS	12	1020	BP GENERAL RUMIÑAHUI
2	1004	BP AUSTRO	13	1006	BP GUAYAQUIL
3	4214	BP BANCO DESARROLLO *	14	1023	BP INTERNACIONAL
4	1007	BP BOLIVARIANO	15	1014	BP LITORAL
5	1151	BP CAPITAL	16	1025	BP LOJA
6	1009	BP CITIBANK	17	1026	BP MACHALA
7	1011	BP COMERCIAL DE MANABI	18	1029	BP PICHINCHA
8	1134	BP COOPNACIONAL	19	1148	BP PROCREDIT
9	3960	BP D-MIRO S.A.	20	1033	BP PRODUBANCO
10	1422	BP DELBANK	21	1037	BP SOLIDARIO
11	1165	BP FINCA S.A.	22	4593	BP VISIONFUND ECUADOR S.A.

Fuente: Superintendencia de Bancos * Oficina de representación de BANDES de Venezuela
Elaboración propia

1.1.1 Análisis del sistema bancario local y regional en la aplicación de la norma ISO 31000:2009

La implementación de la norma ISO 31000:2009 en la administración de los riesgos objeto de estudio, va a permitir mejorar el actual sistema de control preventivo,

ya que con la inclusión o reforzamiento de las variables cualitativas y cuantitativas con las que se establece la determinación y aceptación de riesgos, se va a lograr obtener una mayor cobertura de monitoreo del total de transacciones de clientes con base a criterios técnicos ponderados del riesgo integral y en consecuencia se obtendrá un mayor y más acertado número de alertas de operaciones inusuales que salen fuera del perfil económico y financiero de los clientes, que se generan en las distintas áreas comerciales y operativas de los bancos a través de los canales, productos o servicios.

La protección del riesgo tecnológico está bastante relacionada a la industria financiera donde se maneja grandes volúmenes de información transaccional y el aspecto tecnológico juega un rol importante en la captura y procesamiento de la información, las disfunciones relacionadas a la suspensión de servicios puede impactar negativamente en la imagen y reputación de la entidad, aparte que puede provocar ingentes pérdidas y quizá algo que no es valorado con la importancia que el caso amerita como es la fragilidad de los sistemas y controles preventivos durante la ocurrencia de estas disfunciones, que puede derivar en la ocurrencia de fraudes y transacciones inusuales al interior de una entidad financiera, justamente por la fragilidad temporal de los sistemas de control. La información es el elemento más valioso para cualquier organización en este nuevo siglo, la cual es un instrumento de gestión administrativa para crear una ventaja competitiva (Vásquez 2015).

Para complementar el marco empírico y establecer un diagnóstico de la realidad actual de este sistema de administración de riesgos, se muestra ciertas experiencias prácticas de entidades bancarias de países de la región sobre la aplicación esta norma internacional. En América Latina la norma ISO 31000:2009 ha ganado impulso entre los modelos de gestión de riesgos con base a dicha norma (Valdivia, 2015, 36), algunas entidades financieras de la región que han aplicado esta norma son:

Banco Central de la República Dominicana

Se convirtió en el primer banco de su tipo en adquirir la certificación ISO 31000:2009. La entidad definió la metodología para la gestión de riesgos y de continuidad del negocio basada en la norma ISO 22301, de manera que sea compatible con los lineamientos de la norma ISO 31000:2009 para la gestión de riesgo operativo, así como para la gestión de riesgo de seguridad de la información y tecnología de la información para lo cual previamente se hizo necesario alinear los proceso internos, en especial aquello considerados como críticos (BCRD 2017, 14).

Los logros principales de la aplicación de esta norma permitieron establecer un nuevo Plan Estratégico Institucional correspondiente al periodo 2018 a 2021, cuyo propósito es lograr una organización ágil, dinámica y sostenible, así como el desarrollo del ejercicio de continuidad correspondiente al año 2017, comprobando que el Banco Central cuenta con un plan efectivo para enfrentar una situación de desastre total desde el Sitio Alterno de Trabajo (SAT) en interconexión con el Centro Alterno de Procesamiento de Datos en Santiago, que le ha permitido mantenerse en las mejores posiciones del ranking de las instituciones oficiales que mejor utilizan las tecnologías de la información y comunicación (BCRD 2018, 10). Esta implementación permitió cumplir los objetivos institucionales en el periodo 2017 respecto a la gestión de riesgos y la continuidad del negocio que se resumen en:

- Mantener la estabilidad de precios.
- Promover la estabilidad y fortalecimiento del sistema financiero y la eficiencia del sistema de pagos.
- Optimizar la ejecución de las operaciones monetarias y cambiarias.
- Incrementar la efectividad de la regulación y vigilancia de los sistemas financieros y de pago.
- Mantener niveles efectivos de comunicación transparencia y gobernabilidad institucional.
- Incrementar el nivel de eficiencia operacional, del capital humano y tecnológico.
- Optimizar la gestión financiera interna.

Bancolombia

Bancolombia implementó la gestión de riesgos tecnológicos basada en las normas ISO 31000:2009 e ISO 27005 y su aporte a la continuidad de negocios, cuyo costo de inserción de la norma y el verdadero compromiso de las partes fueron los principales inconvenientes de esta implementación. El riesgo de origen tecnológico puede incidir sobre los objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de tecnología de información (TI) puede implicar pérdidas financieras significativas en las organizaciones, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico. Esta situación descrita ocurrió en Bancolombia, en febrero del 2011; donde se presentó una caída de la red del banco que produjo una suspensión en sus operaciones, que trajo

como consecuencia caos en la atención a usuarios por *aproximadamente una hora*; que implicó pérdidas monetarias y afectación de la imagen del banco (Ramírez 2011, 57).

Estos antecedentes motivaron el desarrollo de la metodología propuesta, que permite la gestión de riesgos de origen tecnológico cuya base son los estándares ISO 31000 e ISO/IEC 27005 de los cuales se realizaron las adaptaciones y especificaciones requeridas para este tipo de riesgo. De igual forma se presenta una forma de ajustar esta metodología a la gestión de continuidad de negocios en lo que respecta a la definición de planes de gestión de incidentes tecnológicos (2011,57).

La metodología diseñada, según la investigadora Alexandra Ramírez trabaja sobre procesos, teniendo en cuenta que esto facilita el entendimiento sobre el funcionamiento de la organización y la definición de interacciones para identificar los activos y riesgos asociados. Además, analizar procesos permite obtener una visión global de la organización y con ello el apoyo requerido por parte de la dirección al mostrar la necesidad de proteger y gestionar procesos críticos de la entidad. El trabajo sobre procesos no se debe entender como un trabajo aislado puesto que esta visión tiene en cuenta el factor humano que se encarga de su ejecución y desarrollo y toda la infraestructura que se requiere para su funcionamiento, enmarcado dentro de los objetivos y estrategias organizacionales. De igual forma dentro del análisis de procesos se tienen en cuenta las actividades críticas que sustentan estos y a su vez sustentan la cadena de valor que permite ofrecer los productos de la organización (2011, 58).

Las situaciones de interrupción de los servicios a causa de la caída y suspensión de los sistemas operativos en línea es un caso de riesgo similar a los que se ven expuestos los bancos ecuatorianos, que de manera permanente sufren esta interrupciones o corte de los servicios financieros, estos retrasos y limitaciones en los servicios bancarios es percibido con malestar por los propios usuarios internos y con más razón por los clientes, situación que provoca el deterioro de la imagen de la entidad que incurre constantemente en estas suspensiones temporales del servicio. No basta solo con llevar un registro o control estadístico de los problemas tecnológicos, ni tampoco aplicar soluciones parciales, sino es necesario actuar con toda celeridad y sobre la marcha gestionar el riesgo de manera definitiva y preventiva, ya sea al evitar o al proteger el riesgo ante estas disfunciones operativas.

Scotiabank Perú S. A.

El Banco Scotiabank Perú S. A., subsidiaria de The Bank of Nova Scotia-Scotiabank (BNS) el tercer grupo financiero más grande de Canadá y el banco

canadiense con mayor presencia internacional, dentro de su gerenciamiento de riesgo utilizó una investigación académica de la norma ISO 31000:2009 para la gestión del riesgo crediticio y su efecto en la morosidad en la ciudad de Trujillo. La gestión del riesgo crediticio de Scotiabank es preparada por un funcionario de negocios y presentada al área de riesgos de acuerdo a las políticas del banco para créditos.

El propósito de la aplicación de esa norma fue para conocer la manera cómo afecta la gestión del riesgo crediticio en la morosidad de la entidad bancaria en la ciudad de Trujillo en 2014, que permita establecer la relación que existe entre las variables de estudio como: edad, sexo, experiencia crediticia, antigüedad de negocio del cliente aplicante a la línea de crédito, experiencia en el negocio y el monto de ingresos o ventas; para determinar la manera que la gestión de riesgo afecta a la morosidad de la entidad tomando en consideración las variables, los cambios del entorno económico, financiero y tributario que influye de manera significativa en los índices de morosidad, una buena y acertada gestión de riesgos influyen de manera positiva en la disminución de los índices de morosidad del banco (Belacha 2014, 36).

Los resultado una vez aplicado el modelo de gestión muestran que una mejor gestión de riesgo crediticio permitirá tener un bajo índice de morosidad, la gestión del riesgo crediticio en la entidad bancaria es la adecuada para evaluar a los futuros clientes que soliciten créditos y se determinó que el índice de morosidad es de 2,26%; cifra que se enmarca en los parámetros permisibles para el control y administración de la cartera (2014, 40).

Superintendencia de Bancos del Ecuador

La Superintendencia de Bancos de Ecuador (SBE) dentro de la metodología de gestión de riesgos de *seguridad de la información*, establece en base de los lineamientos dispuestos por la Política General de Seguridad de la Información, que contiene procedimientos y lineamientos básicos con la finalidad de poder identificar de manera oportuna y preventiva posibles riesgos que de materializarse afectarían a sus operaciones normales, con base a la norma ISO 27005:2012 e ISO 31000:2009 (SBE 2017, 7).

Esta política de seguridad amparada en la Resolución No. SB-CGPMC-2018-004 del 4 de abril del 2018, considera a la información como un activo de alto valor institucional, por lo cual debe seguir parámetros adecuados para garantizar la seguridad de la información confidencial, crítica y sensible sin importar el medio en el que se encuentre, en tal sentido esta norma internacional define el modelo de control de

administración de riesgos y manejo de la información reservada. Los parámetros mínimos con los que se definirá el "Sistema de Gestión de Seguridad de la Información" serán: confidencialidad, disponibilidad e integridad; adicionalmente serán considerados parámetros de autenticidad, trazabilidad, etc., así como los referentes a reputación institucional (SBE 2018, 2).

La norma ISO 31000:2009 justamente establece los lineamientos, sobre los cuales se desarrolla el sistema de gestión, con la finalidad de asegurar la confidencialidad de la información definiendo el uso de leyes y normas del Ecuador, así como la aplicación de normas y buenas prácticas especializadas en seguridad de la información. Estas regulaciones hacen énfasis sobre todo en la confidencialidad y reserva de la información que maneja el regulador, mismas que por su sensibilidad está protegida por disposiciones contempladas en la Constitución de la República y demás leyes complementarias.

Banco Capital

Existe un estudio académico para el Banco Capital de Ecuador sobre una propuesta de un plan de continuidad sobre riesgos tecnológicos que amenazan los procesos de negocio, la aplicación de la norma permite identificar las amenazas y riesgos para asegurar la prevención de los daños y posibles pérdidas que estos riesgos pueden producir. Para establecer la metodología propuesta se tuvo en cuenta el estándar internacional de la norma ISO 31000:2009, para implementar un plan de continuidad de negocio que demuestran las imperfecciones de los procesos actuales y la forma en que pueden ser rediseñados para disminuir las consecuencias de la ocurrencia de la materialización de eventos inesperados (Rojas 2017).

La preocupación de los directivos en el logro de mejores resultados en la eficiencia de los negocios a través de un buen servicio a los clientes, es un factor de suma importancia, en tal virtud el plan de continuidad de negocios para esta entidad bancaria con base a la norma ISO 31000:2009 busca identificar las principales amenazas y riesgos tecnológicos que pueden interrumpir la continuidad de los negocios de la entidad. Esta evaluación está en función de la magnitud de los daños o perjuicios, período de recuperación, tiempo máximo de interrupción que puede ocasionar. Los bancos del país donde se generan gran volumen de información de importancia a fin de canalizar los ahorros, préstamos e inversiones de muchos clientes tienen el deber y obligación de establecer medidas que garanticen la continuidad de operaciones en caso de ocurrencia de cualquier amenaza contra su normal funcionamiento (Rojas 2017).

Entre los beneficios de manejar el plan de continuidad de negocio resaltan los siguientes: a) aseguramiento de continuidad de las actividades, b) prevención o minimización de las pérdidas en casos de desastres o interrupción de servicios, c) ventaja competitiva frente a otras organizaciones, y d) asignación más eficiente de las inversiones en materia de seguridad (Béjar 2013).

Según el investigador Jairo Rojas, con el detalle de las características fundamentales de las instituciones financieras del sector privado de Ecuador, se establecieron los principales flagelos y riesgos del tipo tecnológico a las que están sometidas estas entidades y a las formas de no verse afectadas por los mismos. Las amenazas y los riesgos fueron identificados satisfactoriamente, lo cual asegura la prevención de daños, así como las posibles pérdidas que puedan traer consigo la ocurrencia de desastres y la materialización de los riesgos y las consecuencias que la ocurrencia de eventos inesperados puede traer consigo (Rojas 2017, 134).

1) Desafíos de implementación de la norma ISO 31000:2009

Todos estos bancos, entidades financieras y reguladores descritos han aplicado con buenos resultados los preceptos y los lineamientos de esta norma en los sistemas de gestión de riesgos; sin embargo, en lo referente a la aplicación total de esta norma internacional al sistema de gestión de riesgos puntual de LAFD no se evidencian resultados de estudios o investigaciones en entidades bancarias en particular.

En el Grupo Financiero Pichincha de Ecuador, los principales desafíos e inconvenientes para lograr establecer el enfoque de la ISO 31000:2009 es la fase de preparación y alineación de los diferentes procesos internos para obtener una información depurada e íntegra de la base de clientes, por lo que previamente se realizó un trabajo de campañas de actualización de información de los clientes dando prioridad a los segmentos de alto y extremo riesgo, esto incluye además realizar reformas y actualizaciones a ciertos procedimientos y políticas, cambios que demandaron tiempo para el consenso de las partes, recursos humanos y financieros significativos no previstos dentro de la planificación anual presupuestaria de la unidad de cumplimiento y demás áreas involucradas en el proyecto, que compartieron los costos respectivos.

Con estos antecedentes, el principal desafío de esta mejora sustancial se centra en las *acciones previas* a realizar con la *revisión y mejora de los procesos internos*, el éxito y buen término de esta implementación depende en gran medida de que éstos estén alineados a los requisitos previos que exige la aplicación de esta norma; muchas veces esta tarea fue la más ardua y complicada de planificar y ejecutar puesto que demanda

tiempo, recursos monetarios, esfuerzo adicional del personal y el compromiso de todos y cada uno de las partes intervinientes. Por lo que es fundamental llegar con el mensaje correcto y hacer comprender a la alta gerencia y directorio del banco que aparte de cumplir la ley en esta materia, la importancia de esta implementación radica en la administración del riesgo con un enfoque integral que ayuda a minimizar el riesgo de LAFD al cual la entidad bancaria se encuentra expuesta.

2) Resultados obtenidos

Tanto en Ecuador como en el exterior no existen bancos que hayan aplicado en *todo su contexto* la metodología de la norma ISO 31000:2009 aplicado a la prevención de LAFD, sino más bien los sistemas de gestión del riesgo de los bancos se han centrado en el *proceso de gestión del riesgo* y han partido directamente con la identificación, análisis, evaluación, tratamiento del riesgo y el monitoreo, apoyados en una función de retroalimentación y seguimiento sin adecuados lineamientos soportados en un marco de trabajo documentado; y menos aún, que responda a principios de gestión de riesgo definidos por la organización.

Por otro lado, en los bancos locales del Grupo Pichincha (Rumiñahui, Pichincha, Loja y Diners) y del exterior (Banco Financiero del Perú, Pichincha Colombia, Pichincha Panamá, Pichincha Agencia Miami-USA y Pichincha España) donde se aplica el enfoque de la norma ISO 31000:2009, han mostrado resultados de mejora sustancial en especial en la calidad y cantidad de las excepciones o alertas que genera el sistema de monitoreo, lo cual ha permitido priorizar y optimizar los recursos de la unidad de cumplimiento para la gestión interna de tales alertas en función de la valoración y aceptación al riesgo definido, así como una mejora en el canal de comunicación con la red de oficinas para gestionar las excepciones de transacciones producto de la labor de monitoreo. Al respecto, desde hace varios años se viene realizando un trabajo de alineamiento normativo y de buenas prácticas de control en materia de cumplimiento de los bancos de este grupo financiero encaminado a un enfoque y tratamiento integral del riesgo de LAFD (BP 2013, 28), cuyos resultados generales se resumen a continuación:

- El proceso de la implementación del enfoque integral de la norma hizo notar a las entidades bancarias la necesidad de contar con información de calidad de los clientes (integridad, pertinencia y exactitud) para el buen funcionamiento del modelo, por lo que hubo la necesidad previa de evaluar y mejorar todos los

procesos internos operativos con todos los inconvenientes, carga operativa y retrasos que demanda realizar estas actividades previas.

- Incremento de alertas de las operaciones que exceden el perfil del cliente, cuya efectividad fue notoria, después de contar con el modelo de gestión con base a esta norma.
- Mejor canalización y tratamiento de las excepciones generadas por el sistema y mayor interacción con la red de agencias para descartar alertas de transacciones, en zonas geográficas y segmentos de negocio de clientes, donde antes no se presentaban alertas de operaciones inusuales.

Una vez recopiladas algunas experiencias de la aplicación práctica de la norma ISO 31000:2009 en los distintos bancos y entidades financieras extranjeras, más la experiencia de ciertos bancos locales –aunque con un enfoque parcial del modelo en cuestión– se puede establecer que la aplicación de los lineamientos de esta norma en la administración de riesgos muestran resultados positivos en la operatividad de las entidades financieras donde ésta ha sido implementada, respecto a la cobertura integral del riesgo reflejada en la calidad y certeza de inusualidad de las alertas o excepciones que los sistemas automatizados de monitoreo de los bancos muestran sobre aquellas transacciones de clientes que exceden el perfil asignado (demográfico y transaccional). Se determina la importancia de contar con un sistema de administración del riesgo de LAFD que permita identificar, valorar, mitigar y elevar la capacidad de respuesta institucional ante estos riesgos, por lo tanto, no basta con la aplicación empírica y parcial de procedimientos y políticas que aporten al establecimiento de un control interno sólido, sino que es preciso la *adopción de un modelo integral* que viabilice los procesos hacia la consecución de los objetivos estratégicos de la organización.

3) Dificultades de implementación

En la aplicación práctica de este modelo se presentaron dificultades para las entidades financieras que implementaron esta norma en sus modelos de administración de riesgos, respecto al trabajo adicional que representa ajustar y alinear a la realidad teórica y práctica los procedimientos operativos y tecnológicos internos y la calidad de la información de la base de datos de clientes, estas tareas previas demandaron inversión de tiempo y recursos, por lo que para que el proyecto sea efectivo y viable el personal del área de cumplimiento –muchas veces sin el respaldo total del resto de áreas– debió mostrar de forma clara y contundente las ventajas y el costo-beneficio esperado de la implementación de la norma ISO 31000:2009 y recalcar que esta erogación de recursos

sea tomada como una inversión más que como un gasto, esto tiene que ver con la buena imagen reputacional –beneficio intangible– de la entidad financiera que le permita incrementar sus negocios con una seguridad razonable de sus operaciones.

En cuanto a la obtención de la información sobre la aplicación práctica de este modelo se presentaron limitaciones y dificultades para los propios bancos que quisieron tomar como referencia y conocer experiencias previas en gestión de riesgos de LAFD para adoptar el enfoque de este modelo de gestión, debido a que la norma aún no se la está aplicando en todo su contexto teórico y práctico por entidades bancarias locales y tampoco formalmente en bancos del exterior. Ante esta limitación se optó por recabar información de las asociaciones bancarias de la región (Ecuador, Perú, Colombia, Chile) y ante la Federación Latinoamericana de Bancos (FELABAN que asocia a más de 600 bancos privados de 19 países), agremiaciones que no disponen de esta información ni tampoco tienen registros o conocimiento sobre la implementación de la norma ISO 31000:2009 en la prevención de LAFD entre sus bancos asociados, por lo que se procedió a investigar en base de datos científicas y académicas ciertos casos de bancos y entidades del exterior que ya la han implementado, aunque no puntualmente en la gestión de riesgo de prevención de LAFD.

1.1.2 Análisis de las deficiencias identificadas por la Superintendencia de Bancos

Por disposición del COMF una de las funciones de la JPRMF es conocer sobre los resultados del control efectuado por la Superintendencia de Bancos respecto a la supervisión de las entidades que conforman el sistema monetario y financiero, entre ellas las instituciones bancarias. Las deficiencias y/o debilidades más significativas que se detallan más adelante son producto de las revisiones de campo y consolidadas por personal experto y técnico de la Superintendencia de Bancos (Torres 2014) con base al Manual Único de Supervisión (MUS) de dicho regulador, cuyo detalle se describe a continuación:

1) *Debida diligencia respecto al cliente*: comprende las debilidades relacionadas a la falta de revisión y análisis de un número significativo de clientes por la falta de un monitoreo con base a un enfoque integral de riesgos considerando factores de riesgo cualitativos y cuantitativos.

2) *Transacciones inusuales*: No se reportan a la UAFE transacciones con verdaderas características de *inusual e injustificada*, ya que no existe una evaluación objetiva y consensuada de las mismas.
3) *Persona Políticamente Expuestas (PEPs)*: Ausencia de un control focalizado y falta de identificación y actualización de los clientes que cumplen esta condición.
4) *Terceros y negocios presentados por terceros*: Gran cantidad de clientes manejan en cuentas personales negocios de terceras personas, dificultando la identificación del real propietario o beneficiario final de la cuenta.
5) *Protección y falta de advertencia sobre irregularidades*: Procesamiento de transacciones inusuales sin existir la identificación y reporte oportuno de operaciones sospechosas presentadas a la UAFE.
6) *Reglamentación, supervisión y control*: El proceso de administración de gestión del riesgo adolece de una reglamentación interna dentro de las entidades bancarias.
7) *Mantenimiento de registros*: No se cuenta con todos los requisitos de información de clientes en los archivos físicos de clientes de acuerdo a la normativa local en la apertura de cuentas de clientes y en el transcurso de la relación comercial.
8) *Recursos, integridad y capacitación*: Falta de integridad de operaciones y recurso humano para el monitoreo de ciertas áreas internas y/o productos, donde se generan transacciones de clientes, además de una adecuada capacitación y entrenamiento al personal que incluya a todos y cada uno de los empleados de los distintos niveles.
9) *Informes de operaciones inusuales*: Los reportes de operaciones inusuales e injustificadas (ROII) no son presentados con la oportunidad del caso y no cuentan con toda la información requerida.
10) *Controles internos, cumplimiento y auditoría*: No existe una adecuada labor de seguimiento y revisión del proceso de gestión del riesgo, que permita realizar un mejoramiento continuo del modelo actual.
11) *Sucursales y filiales extranjeras*: Dentro de la planificación del programa general de cumplimiento no se considera labores de coordinación y colaboración con el personal de cumplimiento de las agencias u oficinas en el extranjero de los bancos revisados (en los casos que aplica).

12) *Directrices, matrices y comentarios*: Se refieren a la ausencia o deficiencia en la construcción de las matrices de riesgo, de conformidad con las exigencias de la normativa local.
13) *Falta de supervisores /supervisiones*: Esta observación está dirigida al reducido personal con el que cuenta la unidad de cumplimiento, que es el denominador común de las entidades bancarias locales.
14) *Banca corresponsal*: Existe deficiencias en la evaluación del riesgo de las entidades corresponsales locales y del exterior con los que operan los bancos privados.

Si bien es cierto, que las debilidades indicadas corresponden al periodo 2014, sin embargo, para efectos de la presente investigación se toman en consideración estos hallazgos a efecto de *enriquecer el marco empírico* y efectuar un diagnóstico de las falencias reales y debilidades de los sistemas de gestión de riesgos de los bancos privados, así como tomar como punto de partida para aplicar el modelo de gestión establecido por la norma ISO 31000:2009 y obtener el mejoramiento de dichas debilidades.

Como un aporte de la presente investigación, se focalizan y desarrolla un modelo de los hallazgos materiales identificados por parte de la Superintendencia de Bancos, efectuada a los programas de prevención de riesgos de LAFD de los bancos privados del país, con base a la "Condición, Criterio, Causa y Efecto" de cada uno de ellos del Grupo Financiero Pichincha (Anexo 1).

1.2 La norma ISO 31000:2009 para solventar deficiencias de la administración del riesgo de lavado de activos y financiamiento de delitos

Producto de la labor de supervisión del órgano de control y en razón de las debilidades identificadas y reportadas por la Superintendencia de Bancos sobre la revisión de los sistemas de administración de riesgos de prevención de LAFD con base al sistema de administración de riesgos denominado GREC (contenido en el Manual de Supervisión de Instituciones Financieras), se hace indispensable para el sector bancario privado replantear el enfoque de su tratamiento y gestión.

El actual programa de administración de riesgos de prevención de LAFD que cumplen los bancos privados (descrito en la Metodología general actual de la administración y gestión de riesgos) que contempla las etapas de identificación,

medición, evaluación, control y monitoreo de estos riesgos no resulta suficiente para cubrir las medidas de prevención exigidas y orientadas a prevenir y mitigar tales riesgos**,** puesto que el mismo *no cumple todos los criterios de evaluación integral* que facilite la aplicación de una metodología práctica y eficiente de controles preventivos exigidos por la normativa vigente.

Con la presente propuesta se busca presentar un sistema de gestión que interrelacione todo un esquema de control con un orden lógico y práctico que facilite la conducción y fluidez del proceso de gestión de riesgos de LAFD, cuyas ventajas esperadas son:

1. Disponer de una calificación individual de clientes, con un perfil de riesgo demográfico y transaccional.
2. Diseñar controles preventivos en función de la identificación del riesgo integral.
3. Establecer niveles de tolerancia a los riesgos identificados.
4. Cumplir con las disposiciones legales locales e internacionales en esta materia.
5. Acercar, integrar y mejorar las relaciones de las partes interesadas (stakeholders) en la gestión del riesgo.
6. Ayudar a alcanzar los objetivos estratégicos de las organizaciones, que se verán reflejados en una mayor rentabilidad y crecimiento en el mercado.

Bajo este contexto, la norma ISO 31000:2009 de Gestión de Riesgos cumple las condiciones de integrar políticas, procedimientos y un esquema de trabajo para incorporar el proceso de administración del riesgo de LAFD dentro de los objetivos macros y planeación estratégica de una entidad bancaria.

1.3 La norma ISO 31000: 2009 un modelo de gestión de riesgo

La norma ISO 31000:2009, Gestión de Riesgos tiene como objetivo ayudar a las organizaciones de todo tipo y tamaño a administrar y gestionar el riesgo con efectividad, que les permitan alcanzar los objetivos estratégicos de negocio. Toda organización dentro de su giro operativo gestiona en mayor o menor grado los riesgos identificados, esta norma establece una serie de principios que deben ser observados para lograr un marco de trabajo o estructura de soporte (Castro 2010, 1).

La norma es aplicable a cualquier tipo de riesgo, cualquiera sea su naturaleza, causa u origen, además provee los principios, el marco de trabajo y un proceso destinado a gestionar cualquier tipo de riesgo de una manera transparente, sistemática y

creíble dentro de cualquier alcance o contexto (González 2016, párr. 3) y ayuda a las organizaciones en los siguientes aspectos:

1) Aumentar la probabilidad de lograr los objetivos macros empresariales.
2) Ser conscientes de la necesidad de identificar y tratar el riesgo organizacional.
3) Mejorar la identificación de oportunidades y amenazas, al realizar una evaluación de riesgos con un enfoque integral.
4) Cumplir con las exigencias legales y reglamentarias pertinentes locales, así como las normas internacionales, de ser el caso.
5) Mejorar la información financiera y la gobernabilidad de la organización.
6) Mejorar la confianza de los grupos de interés internos y externos (stakeholder).
7) Establecer una base confiable para la toma de decisiones y la planificación.
8) Mejorar y fortalecer los controles nuevos o existentes.
9) Mejorar la eficacia y eficiencia operacional y de los recursos.
10) Mejorar la salud y la seguridad ocupacional y la protección del medio ambiente.
11) Mejorar la prevención de pérdidas, así como la gestión de incidentes.
12) Mejorar el aprendizaje organizacional y minimiza pérdidas.

Algo fundamental de esta norma ISO 31000 es que permite la interrelación de políticas, procedimientos y argumentos en relación al entorno objetivo e integral de la entidad, establece los principios, guías y directrices de carácter genérico sobre la gestión del riesgo de una entidad y está estructurada en tres enfoques:

a. Los principios de gestión del riesgo[7]
b. El marco de trabajo (framework) para la gestión del riesgo
c. El proceso de gestión del riesgo

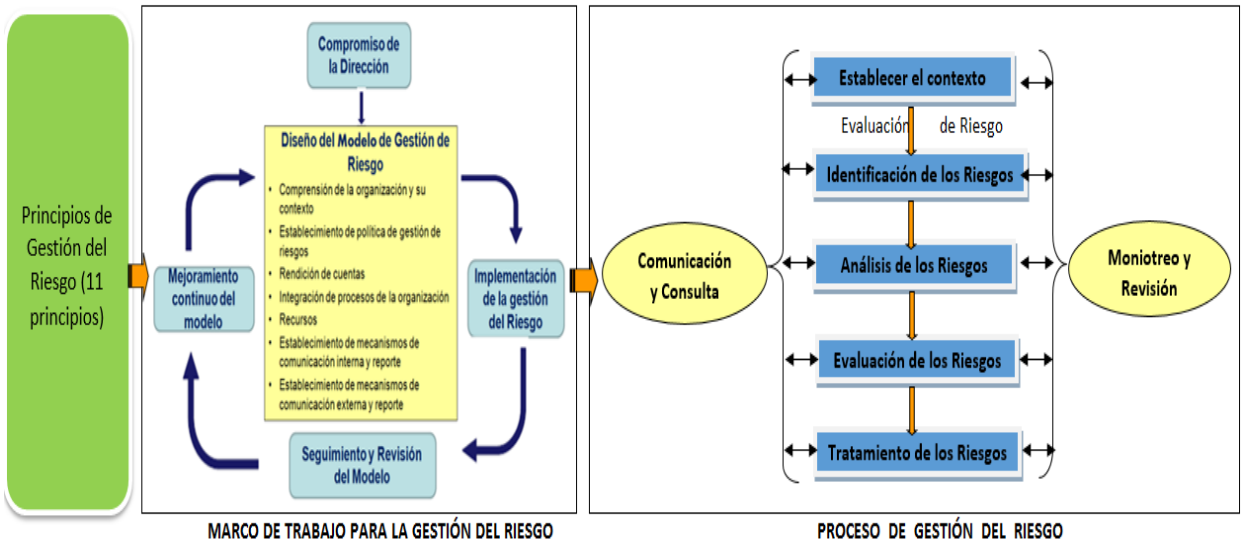
1.3.1 Estructura de la norma ISO 31000:2009

Los principios de gestión del riesgo, el marco de trabajo (framework) y el proceso de gestión del riesgo desarrollado según esta norma, se encuentran interrelacionados entre sí y se resume en la siguiente ilustración:

[7] En esta norma internacional en términos generales la expresión “gestión del riesgo” se refiere a la arquitectura (marco, principios y procesos) para la gestión de los riesgos de manera efectiva, mientras que “gestionar el riesgo” se refiere a la aplicación de esta arquitectura a determinados riesgos.

Gráfico 5

Relación de principios, marco de trabajo y proceso de gestión de riesgo



Fuente: Norma ISO 31000 – basado en AS/NZS 4360:1999 estándar australiano
Elaboración propia

1.3.2 Los principios de gestión del riesgo

La gestión de la norma ISO 31000 (2009, 8) establece una serie de principios que deben ser observados y satisfechos para ejecutar una acción eficaz:

1) Crea valor
2) Está integrada en los procesos de la organización
3) Forma parte de la toma de decisiones
4) Trata explícitamente la incertidumbre
5) Es sistemática, estructurada y adecuada
6) Está basada en la mejor información disponible
7) Está hecha a medida
8) Tiene en cuenta factores humanos y culturales
9) Es transparente e inclusiva
10) Es dinámica, interactiva y sensible al cambio
11) Facilita la mejora continua de la organización

1.3.3 El marco de trabajo para la gestión de riesgo

Según la norma ISO 31000, el marco de trabajo es el conjunto de componentes que proporcionan las bases de organización para diseñar, controlar y realizar la mejora

continua de la gestión de riesgos en toda la entidad. Las bases incluyen las políticas, objetivos estratégicos, mandatos y compromiso con la gestión de riesgo (2009, 4).

1) Compromiso de la Dirección

La implementación de la gestión de riesgo demanda un fuerte compromiso de la alta gerencia y dirección, así como el resto de niveles de la organización, por lo que la dirección debe dotar de los recursos necesarios para esta gestión, así como establecer indicadores de gestión y definir y aprobar la política de gestión de riesgos y garantizar que se encuentren alineados con la cultura de la organización.

2) Diseño del modelo para la gestión de riesgo

Por lo general el diseño del modelo requiere una serie de actividades y acciones previas.

Tabla 4
Componentes del diseño del modelo para la gestión de riesgo

Componente	Descripción
a) Comprensión de la organización y el contexto	• *Interno*: estructura organizativa, gobernanza, políticas, objetivos, estrategia, entre otros. • Externo: aspectos políticos, jurídicos, sectoriales, económicos, el entorno en general de la organización, además de los factores clave y las tendencias con repercusiones en los objetivos de la entidad.
b) Establecimiento de la política de gestión de riesgos	• Vínculos entre los objetivos y políticas generales de la organización con la política de gestión de riesgos y la rendición de cuentas. • Forma en que los intereses en conflicto de los intervinientes son tratados. • Establecer recursos necesarios para ayudar a responsables de la gestión. • La forma en que los resultados de la gestión de riesgo serán medidos y reportados –con indicadores de gestión–.
c) Rendición de cuentas	A cargo de los responsables de los riesgos que tienen la designación y la autoridad para gestionar los mismos y establecer mecanismos para la medición del desempeño.
d) Integración en los procesos de la organización	Forma parte del funcionamiento de los procesos estratégicos de la entidad y debe ser incorporado en las políticas de desarrollo empresarial, la planificación y control estratégico y procesos de gestión de cambio.
e) Recursos	Considerando las personas inmersas en el proceso de gestión, sus habilidades, experiencia y competencia, los recursos materiales y financieros necesarios para cada etapa del proceso, los sistemas de administración de gestión del riesgo y los programas de formación y entrenamiento en el mismo (ISO 3100:2009, 12).
f) Establecimiento de mecanismos de comunicación interna y externa	Incluyen los procesos para consolidar la información de varias fuentes internas de la entidad, deben considerar la sensibilidad y confidencialidad de la misma, e implementar un plan de comunicación con las partes interesadas externas para cumplir con los requisitos legales, reglamentarios y de gobierno.

Fuente: Norma ISO 31000:2009
Elaboración propia

3) La implementación del proceso de gestión de riesgos

La implementación debe enfocarse a garantizar que el proceso de gestión de riesgo diseñado con base al marco y las políticas y procesos de dirección, se aplica y funciona a través de un plan de gestión de riesgos en todos los niveles y funciones pertinentes de la entidad como parte de sus prácticas y procesos habituales.

4) Seguimiento y revisión del modelo de gestión

La organización debe medir y evaluar periódicamente el riesgo con indicadores de gestión, en función de los resultados obtenidos y/o esperados, sus avances y acciones realizadas para mitigar y establecer las desviaciones del plan de la gestión de riesgos para (ISO 31000:2009, 13).

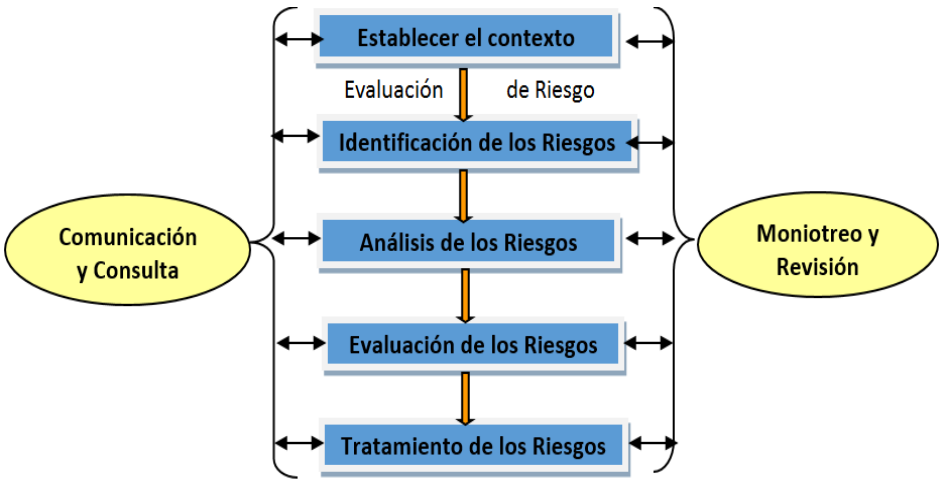
5) Mejoramiento continuo del modelo

Las decisiones deben tomarse para mejorar el funcionamiento del marco, la política y el plan de gestión respectivo. Estas decisiones deben conducir a mejoras en la organización respecto a la administración de gestión del riesgo y grado de cumplimiento debe ser una parte integral de la gestión, formar parte de la cultura organizacional y ser adaptado a los procesos de negocios de la entidad (ISO 31000:2009, 13).

1.3.4 Proceso de gestión de riesgo

Este proceso establece las directrices de planificación, ejecución y desarrollo, seguimiento, evaluación y control de la gestión de riesgo.

Gráfico 6
Proceso de gestión de riesgo



Fuente: Norma ISO 31000 - AS/NZS 4360:1999 estándar australiano
Elaboración propia

1) Comunicación y consulta

La comunicación y consulta con las partes involucradas permite emitir juicios de valor y enfoques de control con base a sus percepciones del riesgo. Estas percepciones pueden variar debido a diferencias en los valores, necesidades, conceptos, preocupaciones y expectativas de los interesados, ya que sus puntos de vista pueden

tener un impacto significativo sobre las decisiones adoptadas. Las percepciones de las partes interesadas deben ser identificadas, registradas, evaluadas y tener en cuenta para la toma de decisiones de mitigación del riesgo (ISO 31000:2009, 14).

2) Establecer el contexto del proceso de gestión de riesgos

Parte importante de esta actividad es la necesidad de justificar y especificar los recursos y la logística utilizada en su ejecución (ISO 31000:2009, 16). El contexto del proceso de gestión del riesgo puede variar de acuerdo a las necesidades de la entidad y puede incluir:

a. La definición de las metas, objetivos, responsabilidades y profundidad de las actividades de gestión de riesgos.
b. La definición en términos de tiempo y lugar de las relaciones entre proyectos, procesos o actividades de la entidad, las metodologías de evaluación de riesgos y los recursos necesarios.

Al definir estos criterios se debe considerar la naturaleza, tipos de causas y consecuencias que pueden ocurrir y cómo medirlos, así como definir la probabilidad de ocurrencia de los eventos y el nivel del riesgo aceptable o tolerable que la entidad está dispuesta a asumir (ISO 31000:2009, 17).

3) Identificación de riesgos

La organización debe identificar las fuentes de riesgo, zonas de impactos, vulnerabilidades internas en productos y servicios, los acontecimientos y cambios en las circunstancias del contexto, sus causas y sus posibles consecuencias. El objetivo de este paso es *generar una lista completa de los riesgos* basados en los acontecimientos, información pública oficial o datos históricos que puedan crear, mejorar, prevenir, acelerar o retrasar la consecución de los objetivos.

Las personas con los conocimientos adecuados sobre el funcionamiento de la organización deben participar en la identificación de riesgos con base a información actualizada, con apoyo de herramientas y técnicas de identificación de riesgos que se adapten a sus objetivos particulares y capacidades técnicas (ISO 31000:2009, 17).

4) Análisis de los riesgos

El riesgo debe ser analizado mediante la determinación de las consecuencias (impacto) y la probabilidad de ocurrencia (amenaza), también se debe tener en cuenta que un evento de riesgo puede tener múltiples consecuencias y puede afectar a múltiples objetivos empresariales, por lo que en este análisis se debe tener en cuenta la implantación de los controles preventivos pertinentes.

El análisis puede ser de tipo cualitativo, cuantitativo o semi-cuantitativo, o una combinación de estos, dependiendo de las circunstancias y naturaleza del riesgo, así como las consecuencias pueden ser expresadas en términos de efectos tangibles tales como pérdida de mercado, disminución de ingresos, incremento de costos, montos de fraudes, casos de lavado de activos, entre otros; e intangibles como el riesgo reputacional, probabilidad de ocurrencia, pérdida de credibilidad y confianza, incertidumbre financiera, entre otros (ISO 31000:2009, 18).

5) Evaluación de riesgos

El propósito de la evaluación de riesgos es ayudar en la toma de decisiones basadas en los resultados del análisis de riesgos, que permita gestionar aquellos riesgos que necesitan tratamiento y su prioridad. Supone la *comparación del nivel de riesgo identificado durante el proceso de análisis, con los criterios de riesgo establecidos* cuando se considera el contexto total de la naturaleza del riesgo, con base a esta comparación, se establece la necesidad del tratamiento a ser aplicado.

Las decisiones adoptadas deben tomarse de conformidad con los requisitos legales y reglamentarios y deben tener en cuenta el contexto total del riesgo y *considerar rangos o márgenes de la tolerancia de los riesgos asumidos* por parte de una o varias áreas de la organización, esta tolerancia en cierto modo beneficia la coexistencia de los riesgos controlados dentro de una entidad.

Esta evaluación también puede dar lugar a una decisión de tratar el riesgo a través de mantener o mejorar los controles existentes para mitigarlo. Esta decisión se verá influida por la actitud y predisposición de tolerancia y aceptación a los criterios del riesgo asumidos y aceptados por parte de la entidad (ISO 31000:2009, 18).

6) Tratamiento de los riesgos

Consiste en seleccionar una o más opciones de modificación y control de los riesgos y la aplicación de esas opciones en su mitigación, esto implica:

a. Decidir si los *valores del riesgo residual son tolerables* o aceptables.
b. Si no son tolerables, generar un nuevo proceso de tratamiento del riesgo.
c. La evaluación de la eficacia del tratamiento.

Las opciones de tratamiento de riesgos no son necesariamente excluyentes o apropiadas en todas las circunstancias, éstas dependen del grado de aceptación del riesgo. Estas opciones pueden incluir los siguientes aspectos:

- Evitar el riesgo al decidir no iniciar o continuar con la actividad que lo origina.
- Tomar o aumentar el riesgo con el fin de perseguir y concretar una oportunidad.

- Eliminar la fuente de riesgo.
- Los cambios en la probabilidad y en la consecuencia.
- La distribución del riesgo con la otra parte o partes involucradas en su gestión.
- Mantener el riesgo por decisión informada y aceptada.

7) Monitoreo y revisión

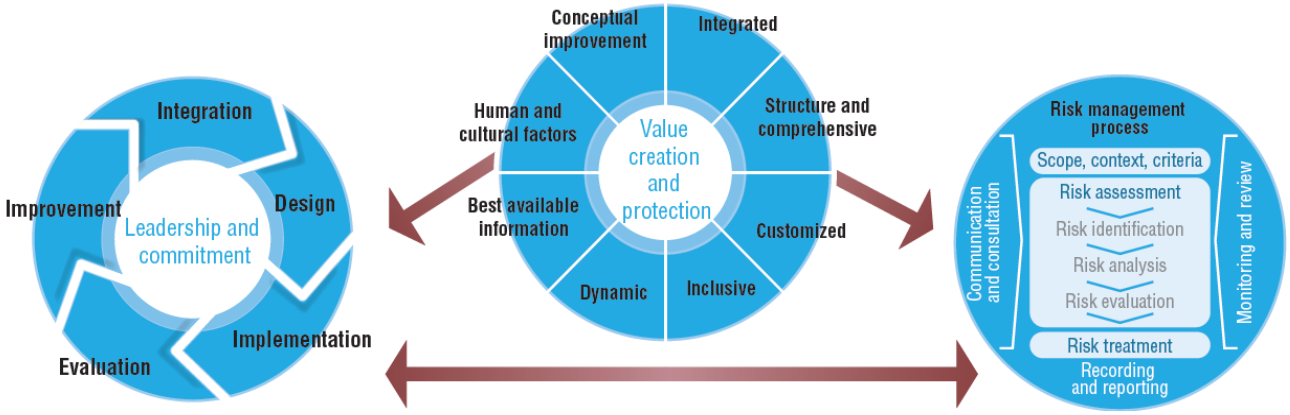
Los sistemas de monitoreo requieren una cuidadosa selección de metas y planificación que no afecten la disponibilidad de recursos, ya que existen factores que podrían modificar los niveles de probabilidad y consecuencia, y factores que impactan el costo de las opciones de tratamiento, por lo que se debe priorizar:

- Riesgos calificados como altos o extremos.
- Criterios de tolerancia del riesgo, especialmente cuando de esto resultan altos niveles de riesgo residual.
- Avances tecnológicos que podrían ofrecer alternativas más eficaces o de menor costo al tratamiento actual del riesgo (ISO 31000:2009, 22).

1.4 La nueva versión de la norma ISO 31000:2018 Gestión de Riesgos

La última versión de la norma se *centra de forma exhaustiva* en la atención de gestión del riesgo como una herramienta para minimizar de *forma anticipada* las posibles inseguridades o materialización de riesgos que pudieren producirse. Por tanto, la ISO 31000 se actualiza en febrero del 2018 para dar respuesta con eficiencia y seguridad a los riesgos actuales a los que se enfrentan las organizaciones.

Gráfico 7
Relación de la nueva versión de la norma ISO 31000:2018



Fuente: Norma ISO/FDIS 31000
Elaborado por Asociación Española de Normalización (AENOR)

El liderazgo, el compromiso y la integración de las posibles amenazas dentro de la estructura de una empresa u organización cobran especial *relevancia* en esta nueva versión. Es el primer estándar que establece la gestión de *riesgos sociales y ambientales*, desarrollando nuevos procedimientos para la prevención de posibles contingencias (ISO 31000:2018).

En esta última versión de la norma sobre el sistema de gestión de riesgos los principales cambios se fundamentan principalmente en:

1. ***Alta dirección y liderazgo***

La norma refuerza el liderazgo de gestión de la alta dirección en el sistema de gestión, dándole un enfoque de arriba - abajo; es decir, desde el gobierno corporativo hasta el nivel de gestión. Por tanto se trata de "crear valor", de utilizar la gestión de los riesgos como herramienta de seguimiento y control y como apoyo en la toma de decisiones, con el objeto de *reducir la incertidumbre* frente al logro de los objetivos y mejorar el rendimiento de la organización.

2. ***Principios de Gestión de Riesgos***

La norma realza como propósito de la norma el primer principio de la versión 2009 de creación y protección de valor de la gestión de riesgo; los restantes diez (10) principios se sintetizan en los ocho (8) que se describen más adelante. En este punto todos los sistemas de la norma circundan alrededor de uno esencial que funciona como un núcleo: *crear valor y protegerlo*, estos principios son

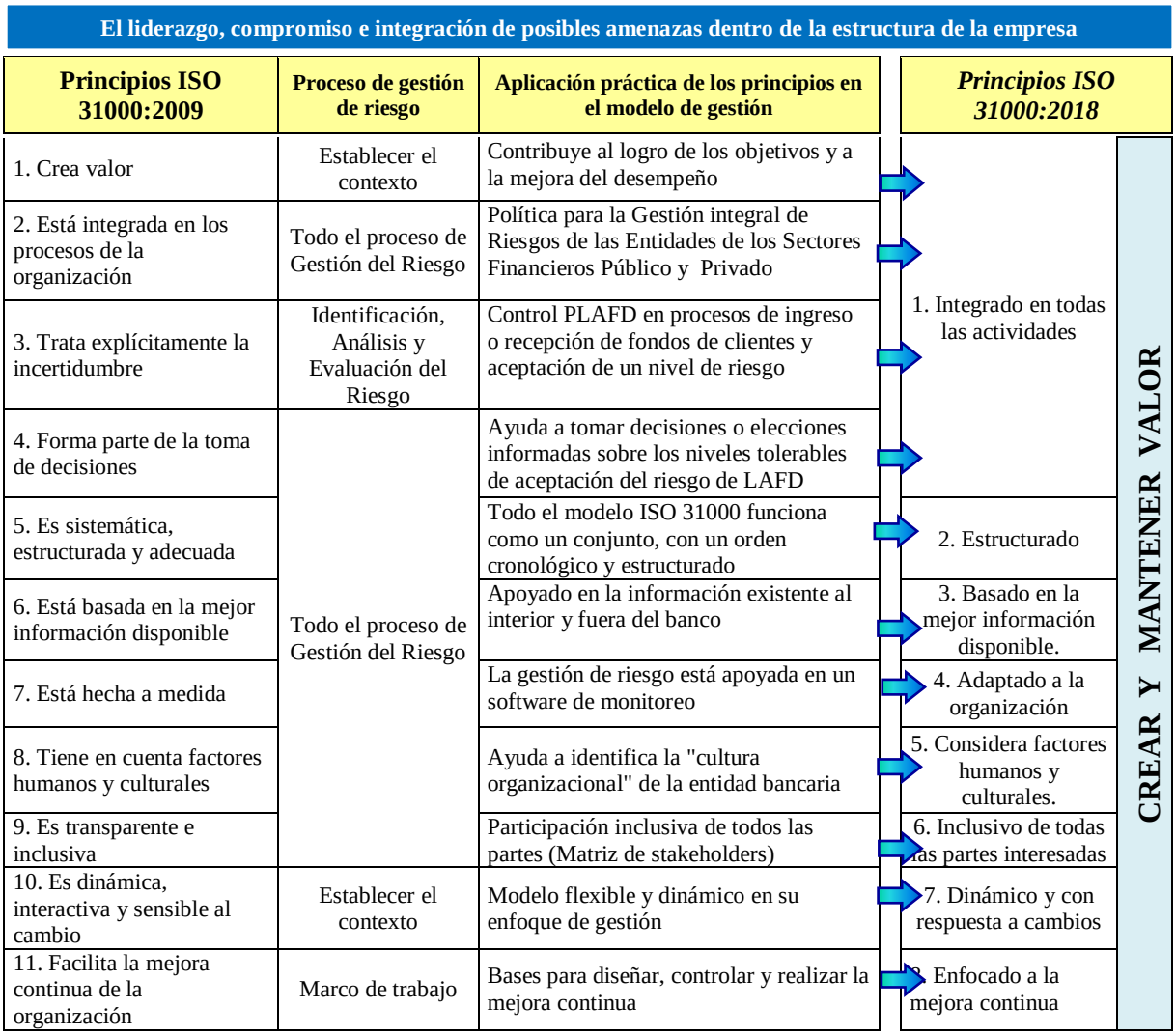
a. *Integrado en todas las actividades*. No aislado del resto de procesos de la organización.
b. *Estructurado*. Es decir, tiene que presentar resultados consistentes que permitan comparar de manera tangible un período con otro y observar el avance.
c. *Adaptado a la organización*. De manera que se ajuste al contexto organizacional y esté íntimamente relacionado con los objetivos.
d. *Inclusivo de todas las partes interesadas*. Se debe involucrar a todas las partes para conseguir una gestión de riesgo más informada.
e. *Dinámico y con respuesta a cambios* o que se anticipe a ellos.
f. *Basado en la mejor información disponible*. Respetando la confidencialidad a todos los niveles especialmente las partes interesadas.
g. *Considera factores humanos y culturales*. Influyen considerablemente en todos los aspectos de la gestión de riesgos en todos los niveles y etapas, que influyen, tanto interna como externamente.

h. *Enfocado a la mejora continua*. A través del aprendizaje que da la experiencia.

Este realineamiento de principios no modifica en gran medida el porqué de la norma, pero sí conlleva ajustes y prioridades con énfasis en algunos de ellos, como los factores humanos y culturales o la mejora continua mediante el aprendizaje. Un esquema comparativo de las dos versiones de la norma ISO 31000 (2009 y 2018) se desarrolla a continuación:

Gráfico 8

Relación de versiones de la norma ISO 31000: 2009 e ISO 31000: 2018



Fuente: Norma ISO 31000 (versiones 2009 y 2018)
Elaboración propia

3. La integración de los riesgos, en el marco de referencia

La norma establece que el *marco de referencia* será el factor clave para la integración de los riesgos dentro del sistema de gestión. En este punto ejerce una alta *influencia* la *alta dirección* y su liderazgo, así como el compromiso de las partes

interesadas. Por tanto la versión de la norma 31000:2018 busca diseñar el sistema más adecuado para la organización teniendo en cuenta la convergencia de riesgos.

El desarrollo del marco de referencia abarca el diseño, implementación, evaluación y mejora de cada uno de los elementos que componen el sistema de gestión de riesgos. Se concluye este tema puntualizando que la *alta dirección* será la *responsable de alinear* la *gestión de riesgos con la estrategia, objetivos y cultura organizacional* de la entidad.

4. La naturaleza iterativa del riesgo

Es decir los procesos iterativos en respuesta a los diversos cambios internos y externos que presenta el entorno, en este aspecto no ha habido mucho cambio en la norma ISO 31000:2018, es más el proceso para la identificación del riesgo se mantiene, pero con *mayor implicación y compromiso* de la alta dirección. Promover la conciencia y la mentalidad *para que los riesgos sean entendidos y comprendidos* por cada uno de los principales interesados, asegura un mejor tratamiento de los riesgos. Además, considerar las consultas ayuda a tener *retroalimentación* oportuna e información que ayuda en el proceso de toma de decisiones.

La norma ISO 31000:2018 resalta la *importancia que a este respecto tiene la* confidencialidad de la información *y los derechos de privacidad de las personas* en un programa de comunicación y consulta. (ISO Tools, 2018).

La versión de la norma ISO 31000:2018 centra su atención en el liderazgo y el compromiso de la dirección en la gestión del riesgo, desde el gobierno corporativo hacia el resto de niveles operativos de la organización. Con la versión actual de la norma los resultados que se proyectan obtener son más sólidos y de *mayor valor agregado*, puesto que se enfatiza y prioriza el apoyo y la gestión que la alta dirección debe brindar al programa de cumplimiento de los bancos, ya que un capítulo aparte merece los resultados que la dirección debe informar sobre el manejo del riesgo de LAFD a la Junta Directiva, al organismo de control y a las contrapartes locales y del exterior.

La norma refuerza el *liderazgo y apoyo de la alta dirección* en el sistema de gestión, dándole un enfoque de arriba - abajo; es decir, desde el gobierno corporativo hasta el nivel de gestión. Por tanto se trata de “crear valor”, de utilizar la gestión de los riesgos como herramienta de seguimiento y control y como apoyo en la toma de decisiones, con el objeto de *reducir la incertidumbre* frente al logro de los objetivos y mejorar el rendimiento de la organización.

1.5 La norma ISO 31000:2018 en función de los resultados de la ISO 31000:2009

Las variables con base a las cuales se realiza el tratamiento del riesgo según ISO 31000:2018 van más allá de las consideraciones económicas, es primordial tomar en cuenta las opiniones de las partes interesadas, las obligaciones y los objetivos de negocio de la organización. El tratamiento de riesgos según la norma aunque se diseñe e implemente de forma cuidadosa puede no ofrecer los resultados esperados para el banco o para alguna de las partes intervinientes; por ello el *monitoreo y la revisión* deben formar parte integral del proceso de tratamiento de riesgos a fin de garantizar que las acciones implementadas sigan siendo siempre efectivas.

Con la finalidad de realizar un análisis de la versión de la norma ISO 31000:2018 y tomando en consideración que de esta nueva versión aún no se dispone de resultados sobre su implementación y aplicación en los sistemas de gestión de riesgos, se procede a realizar un análisis prospectivo de los potenciales resultados a priori que se obtendrán con base a los resultados de mejoramiento establecidos en la presente investigación con la norma ISO 31000:2009.

Tabla 5

Resultados esperados en función de la norma ISO 31000:2018

Situación actual Deficiencia	Acciones de regularización de brechas identificadas	Resultados preliminares con la norma ISO 31000:2009	Base, fundamento, principio ISO 31000:2018	Resultados proyectados con norma ISO 31000:2018
Debida diligencia respecto al cliente	Análisis de riesgos con enfoque cualitativo y cuantitativo.	Mayor cantidad y calidad de alertas presentadas	Principios de gestión de riesgos	Número de alertas de óptima calidad en función del análisis integral del riesgo
Transacciones inusuales	Consenso interno de criterios en Comité de Cumplimiento	Reporte ROII con consenso y autorización del comité de cumplimiento	Basado en la mejor información disponible	Aplicar Tratamiento del riesgo, proteger el riesgo
Personas Políticamente Expuestas	Ingresar y actualizar en el software de monitoreo base oficial de PEPs	Generación de un repositorio con información de los clientes PEPs	Basado en la mejor información disponible	Proceso de monitoreo y actualización de los cargos de PEPs y su entorno según normativa
Terceros y negocios presentados por terceros	Obtener e ingresar en los sistemas del banco la información requerida como parte de la política Conozca a su cliente	Alertas generadas por clientes que prestan sus cuentas a terceros	Basado en la mejor información disponible	Capacidad para identificar, desagregar y depurar a las personas o últimos beneficiarios de las cuentas
Protección y falta de advertencia sobre irregularidades	Rediseño del modelo del monitoreo con base a la norma ISO 31000:2009	Mejoramiento de reportes oportunos a la UAFE	Enfocado a la mejora continua	Envíos de reportes ROII a UAFE dentro de las 48 horas de aprobarse en el comité de cumplimiento
Reglamentación, supervisión y control	Actualización de manuales de procesos internos relacionados a PLAFD con base a la norma de gestión de riesgos y marco legal	Manuales de procesos internos de PLAFD actualizados	Adaptado a la organización y se ajusta al contexto organizacional	Todos los procesos de la Unida de Cumplimiento y áreas afines documentados, actualizados y operativos

Mantenimiento de registros	* Desarrollar procesos internos de evaluación y mejora de calidad de información de clientes * Enlazar e incorporar en el software de monitoreo los datos mínimos requeridos por el sistema. * Desarrollar interfaces con la base de datos central para los procesos de actualización de información de clientes	Integridad de información de clientes de acuerdo a la normativa y requerimientos de los campos de datos del software de monitoreo	* Principios de gestión de riesgos: Basado en la mejor información disponible * Marco de trabajo: Implementación de la gestión de riesgo	Información completa del cliente que a más que cumplir con la norma sirva de insumo para el software de monitoreo y explotación de los procesos de manejo de inteligencia artificial
Falta de integridad y recurso humano para monitoreo de ciertas áreas internas y/o productos, que generan transacciones de clientes, además de una adecuada capacitación al personal.	* Consolidar en una base de datos central todos los aplicativos * Evaluar la real carga operativa de la unidad de cumplimiento * Elaborar un plan de capacitación anual para el personal	*Base de datos (DWH) centralizada con toda la integridad de transacciones de clientes *Personal de área de cumplimiento de acuerdo a capacidad de llegada y atención de alertas generadas *Plan de capacitación aprobado por la alta dirección	*Integración de los riesgos en el marco de referencia *Enfocado a la mejora continua	* Base de datos central * Personal de cumplimiento entrenado acorde a la capacidad de gestión del área * Capacitación con evaluaciones internas y externas y niveles de aprobación
Informes de operaciones sospechosas	Rediseñar y documentar el proceso de reporte de transacciones inusuales	*Efectuar el reporte de operaciones (ROII) en los plazos establecidos con toda la información que exige la normativa *No generar observaciones o multas por el retraso en el envío de reportes a los órganos de control	* Principio de gestión de riesgo: Enfocado a la mejora continua	Desarrollar una interface transmisión de operaciones inusuales con el módulo de recepción de datos de la UAFE, simplifica tiempo y refuerza la seguridad de dicha información reservada
Controles internos cumplimiento y auditoría	Instaurar procesos de revisión continua del modelo de administración de riesgos	La instauración del modelo de gestión de riesgos basado en ISO 31000:2009 requirió alinear los procedimientos internos a los requerimientos de calidad de información de los datos de clientes	* Alta dirección y liderazgo * Integrado en todas las actividades * Estructurado * Inclusivo de todas las partes interesadas * Enfocado a la mejora continua	La norma ISO 31000:2018 contempla el mejoramiento continuo del modelo a través del marco de trabajo que está relacionado con los principios y proceso de gestión de riesgo
Sucursales y filiales extranjeras	Desarrollar e incorporar en el plan anual de cumplimiento las actividades de coordinación PLAFD y revisión de las filiales en el exterior	Coordinación y desarrollo de los programas de cumplimiento de las oficinas o filiales del extranjero, de acuerdo a la normativa local y del exterior, según aplique	* Inclusivo de todas las partes interesadas * Considera factores humanos y culturales	Aplicar directrices y políticas de control LAFD de la matriz local en oficinas del exterior considerando su aplicabilidad de acuerdo a la legislación de la jurisdicción del exterior
Directrices, matrices y comentarios	Desarrollar las matrices de riesgo conforme el análisis de las variables de los factores de riesgo	Modelo de gestión de riesgo de PLAFD con base al estándar de la norma ISO 31000:2009 considerando variables cualitativas y cuantitativas de los factores de riesgo	* Alta dirección y liderazgo * Integración de los riesgos en el marco de referencia * La naturaleza iterativa del riesgo * Principios de gestión de riesgos * Marco de trabajo * Proceso de gestión de riesgo	Gestión de riesgo de PLAFD con base a la norma ISO 31000:2018 considerando variables cualitativas y cuantitativas de los factores de riesgo y adicionando procesos automatizados de inteligencia artificial con base a la explotación automática del Big data y las bondades de las nuevas versiones de estas herramientas de manejo de grandes volúmenes de información y datos

Falta de Supervisores / supervisiones	*Levantamiento de funciones para evaluar la carga operativa del área *Determinar la capacidad de atención versus la capacidad de llegada de pedidos	Se establece una capacidad de atención y gestión de excepciones por parte de los analistas de cumplimiento, en función de las alertas presentadas en los segmentos de clientes con valoración de riesgo alto y extremo	Alta dirección y liderazgo (supervisión de arriba hacia abajo)	Generar un modelo de gestión de excepciones con apoyo de la red de oficinas, para que los analistas coordinen los resultados y monitoreo de los mismos en la bitácora del software de monitoreo
Banca corresponsal	Desarrollar procesos de calificación y aceptación de corresponsales previo a iniciar relaciones de corresponsalía	Envío de formularios o cuestionarios de recolección para calificación y aceptación de los bancos y entidades corresponsales	* Marco de trabajo: Establecimiento de la política de gestión de riesgo	Parametrizar en una lista interna dentro del aplicativo de lista de observados los bancos y entidades corresponsales autorizados para procesar transacciones de clientes.

Fuente y elaboración propia

El reducido volumen de monitoreo de operaciones de clientes, con base a los principios de gestión de riesgo de la nueva versión 2018: “basado en la mejor información disponible” y “estructurado”; se proyecta tener un número de alertas de óptima calidad en función del análisis integral del riesgo. Una vez que se encuentre realizada la valoración del riesgo con base a las condiciones de amenaza y vulnerabilidad que se ha desarrollado con la norma ISO 31000:2009, el resultado obtenido es el aumento de alertas de transacciones que salen fuera del perfil del cliente, esta situación ayuda a identificar una mayor cantidad de operaciones inusuales; sin embargo, este incremento demanda una mayor cantidad de recursos humanos para gestionarlo, que muchas veces el personal de la unidad de cumplimiento no alcanza a cubrirla, por lo que se requiere utilizar proactivamente los indicadores de gestión del monitoreo y revisión del proceso mejorado.

Con este antecedente y con base al “*principio de la inclusión de todas las partes interesadas”*, se espera que todo el personal del banco esté en capacidad de gestionar las alertas de inusualidades de transacciones de clientes presentadas en las áreas y ámbito de su competencia en coordinación con el oficial de cumplimiento, por lo que para cumplir este principio y el incremento inminente de alertas en transacciones, se debe planificar y ejecutar un programa de capacitación integral a todos los funcionarios del banco.

Sobre la falta de integridad de información de ciertas áreas o productos, si bien es cierto que para la aplicación de la norma ISO 31000:2009, previamente hubo que realizar una evaluación y cierre de brechas entre la falta de integridad de la información de ciertas áreas o productos donde se generan transacciones de clientes, para regularizar estas deficiencias se debe realizar una revisión del diseño y funcionamiento de los

procesos de captura y compilación de la información especialmente en aquellos bancos que no tienen centralizada su base de datos en un data warehouse (DWH), con toda la carga operativa e inconvenientes técnicos y retrasos que demanda este proyecto . Para efectos de la aplicación de la norma ISO 31000:2018 se remarca el liderazgo que debe asumir la dirección, puesto que se proyecta la gestión y compromiso desde arriba hacia abajo, por lo que bajo este enfoque la gestión y cierre de brechas para obtener el escenario operativo apto previo a la implementación de la nueva versión de la norma, va a resultar más efectivo con el apoyo, involucramiento y seguimiento de la alta dirección.

Así mismo, es indispensable la coordinación y el alineamiento de controles de prevención LAFD con las oficinas del exterior relacionadas, para obtener un programa integral de cumplimiento del grupo financiero local y sus filiales del exterior.

Incorporar variables cualitativas y cuantitativas en la medición del riesgo, con base a la aplicación de la norma ISO 31000:2009 se logró mejorar la calidad de la información de los clientes, a la vez que la valoración del riesgo de LAFD se realizó con base a criterios consensuados de las partes interesadas internas del banco. Con la actualización de la versión 2018 de la norma, uno de los puntos que hace énfasis en la *naturaleza iterativa del riesgo,* alineada a los cambios externos que presente el entorno y el compromiso de la alta dirección.

En este sentido, la inteligencia artificial en la digitalización bancaria toma un rol preponderante, ya que el sector financiero debe cuidar más sus plataformas de seguridad. La inteligencia artificial es una tecnología de big data que manejan grandes volúmenes de información acumulada de las operaciones del cliente, tanto de la información que él provee y sobre todo el comportamiento que muestra con base al uso de sus productos, toda esa inteligencia se aplica para establecer grupos de perfiles e identificar operaciones inusuales, para gestionar y conocer el origen de los fondos del cliente y como los utiliza, este comportamiento debe ser objeto de análisis y pasar todo el proceso de justificación de tales operaciones alertadas (Castellanos 2018). El uso de herramientas de big data aplicado a esta materia permite un profundo conocimiento a base de la interacción de la base de clientes del banco, identificación de posibles fuente de riesgo de LAFD y fraudes, lo cual obliga a que también el software de monitoreo desarrolle e incorpore estos conceptos de inteligencia artificial en sus nuevas versiones, que los principios de la norma actual los contempla.

Las herramientas de inteligencia artificial pueden aprender y monitorear el comportamiento de los usuarios y sus patrones para identificar señales de alerta. Al

aprovechar la inteligencia artificial y manejar una gran cantidad de datos en un periodo de tiempo las instituciones financieras pueden automatizar el mecanismo de manejo, incluso puede ajustar ciertos procesos para realizar reportes ROII directamente al regulador en los tiempos y plazos definidos, para disminuir el tiempo total de procesamiento y también los costos de manejo, mientras que también mejora la experiencia del cliente (Bakingly 2018).

Respecto al *conocimiento insuficiente sobre la actividad económica y el origen de fondos*, con el enfoque de la norma ISO 31000:2018, se debe considerar además el aspecto social y ambiental de aquellas actividades económicas de clientes relacionadas a la explotación de los recursos naturales (sector minero, hidrocarburífero) que tienen un directo impacto ambiental. No se debe dejar de mencionar que la mayoría de bancos privados, sino todos están comprometidos y han firmado el pacto global de responsabilidad social empresarial (RSE) que es un compromiso voluntario incluido en la planificación estratégica sobre los riesgos sociales y ambientales a través de un modelo de gestión socialmente responsable que alinee el desempeño social, ambiental y económico con las estrategias de las organizaciones.

La *falta de información y documentación*, con base a los principios de gestión de riesgo de la nueva versión 2018: "basado en la mejor información disponible" y al ser una condición necesaria disponer de información completa de la base de clientes previo a la implementación de esta norma; se proyecta y se hace necesario tener una base de datos y documentación acorde a la normativa y exigencias de los requisitos mínimos de los campos de información de clientes que requiere el software de monitoreo.

El nuevo modelo de la versión 2018, además debe tomar en consideración la evolución de la banca comercial tradicional hacia una banca más electrónica y digital, en consecuencia se debe priorizar y realizar los proyectos masivos de digitalización de toda la información de los clientes e integrarla a los sistemas automatizados. La nueva banca se desarrolla bajo una corriente de simplificar procesos engorrosos y documentos físicos voluminosos, ya que la era digital es una realidad del cual la banca es una de sus mayores referentes. El cambio de los hábitos del cliente ha provocado un nuevo modelo de relación con el banco: un cliente omnicanal. Esto obliga a desarrollar modelos de distribución que cubran sus necesidades de servicios bancarios a la par con las acciones de control pertinentes. Sin duda, la importancia de los canales ha cambiado drásticamente en los últimos años y los canales digitales se han convertido en los principales puntos de interacción de los clientes del banco. (Galdo 2015, 19).

Capítulo cuarto
Propuesta de implementación del sistema de administración de riesgo de prevención de lavado de activos y financiamiento de delitos bajo el enfoque de la norma ISO 31000

1. Aplicación de la norma ISO 31000:2009 a la administración y gestión del riesgo

En este capítulo se muestra una visión general del proceso de gestión de riesgos aplicado y propuesto con base a la norma ISO 31000:2009, adecuado y diseñado para abordar y administrar el fenómeno del riesgo de LAFD a las que se ven expuestas las entidades bancarias del país, puesto que al momento la Superintendencia de Bancos no aplica un modelo de revisión integral de estos riesgos como lo tipifica esta norma.

La metodología propuesta muestra un orden lógico y práctico que facilitará la conducción del proceso de gestión de estos riesgos, que resultará de utilidad práctica para las entidades y personas calificadas como sujetos obligados a implementar programas de prevención en esa materia; sobre todo para instituciones bancarias cuyo giro principal de negocio es el servicio de intermediación financiera, ya que proporciona el marco teórico y de trabajo para la implementación de dicho programa de prevención.

1.1 Principios de la gestión de riesgos aplicado a la prevención de lavado de activos y financiamiento de delitos

Según los lineamientos de la norma, para una mayor eficacia del cumplimiento de los objetivos estratégicos de negocio –incluyen los objetivos de control– toda entidad o sujeto obligado local en la prevención de LAFD; en este caso una entidad bancaria, debe tener en cuenta los siguientes principios aplicados a la gestión de estos riesgos.

1) Crea valor

Desde la perspectiva de las entidades bancarias la creación de valor está enfocada además en la creación y proyección de una buena imagen reputacional de la organización, lo cual genera confianza en sus clientes, colaboradores, accionistas y demás partes interesadas, que le permita a la entidad crecer en el tiempo y mantenerse en el mercado financiero como una empresa en marcha.

2) Integrada en los procesos de la organización

La gestión de riesgo no debe ser entendida como un actividad aislada, sino como parte de las actividades y procesos principales de una entidad; en tal sentido, la "Política para la Gestión Integral y Administración de Riesgos de las Entidades de los Sectores Financieros Público y Privado", emitida por la Junta de Política Regulación Monetaria y Financiera (Resolución 380-217-F de 22 de mayo de 2017) establece que las entidades deben integrar y establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo de negocios, por lo que la administración de la prevención de LAFD es una gestión fundamental dentro de la citada normativa.

3) Trata explícitamente la incertidumbre

La incertidumbre que genera los delitos de LAFD debe ser gestionada como un riesgo inherente propio de las operaciones de los bancos, su tratamiento está basado en la implementación de procedimientos de control generales y específicos en todos los procesos relacionados al ingreso o recepción de fondos de los clientes, capaz que el banco pueda obtener una certeza razonable sobre su procedencia legítima. Al ser la actividad bancaria inherente al riesgo, está en la decisión de la alta gerencia la aceptación de un nivel de riesgo permisible o tolerable en las operaciones, sobre el cual la entidad se sienta cómoda para operar con base a un proceso de evaluación plena del riesgo para minimizar su impacto y grado de incertidumbre.

4) Forma parte de la toma de decisiones

Toda entidad bancaria dentro de su giro operativo de negocio debe evaluar y adoptar decisiones que apuntalen los objetivos estratégicos predefinidos, siempre tomando en consideración todos los riesgos que se pudieren presentar para el logro de tales objetivos. Bajo este enfoque, es indispensable evaluar y controlar el riesgo de LAFD, que se encuentra presente en toda instancia de toma de decisiones, ya que se trata de un riesgo que recorre transversalmente toda la organización y puede afectar todos los procesos, operaciones y áreas internas del banco.

5) Es sistemática, estructurada y adecuada

El sistema de gestión de riesgos contribuye a la eficiencia de las operaciones y en consecuencia a la obtención de resultados fiables en materia de control preventivo, para lo cual el sistema debe pasar por un adecuado proceso de planificación de las diversas etapas que comprenden el Sistema de Administración y Gestión de Riesgos de LAFD (identificar, medir, controlar y monitorear), ya que sus etapas están

interrelacionadas para que funcionen en conjunto y como un todo estructurado. Por lo que su concepción y diseño integral demanda amalgamar sus elementos bajo un pensamiento y enfoque sistémico, que considere cada uno de los elementos del sistema de gestión, pero que a su vez los integre con un orden cronológico y estructurado.

6) Está basada en la mejor información disponible

Los inputs del proceso de gestión del riesgo están basados en fuentes de información como datos históricos, la experiencia, la observación, las previsiones y la opinión de expertos. Un sistema de gestión de prevención de LAFD debe apoyarse en la información disponible existente, sea dentro de la entidad como fuera de ella. Se debe considerar que si bien es cierto gran parte de la información que facilita obtener un conocimiento pleno de la organización y sus potenciales riesgos se encuentra al interior de la entidad, es importante obtener información de las fuentes externas y del entorno del banco, como son los organismos de supervisión y control, asociaciones y comités gremiales, que recogen y proveen información sobre las tendencias y problemática actualizada del sector bancario.

7) Está hecha a medida

Por lo general los bancos locales adquieren paquetes de software Anti-Lavado de Dinero (AML por sus siglas en inglés) que les permitan administrar sus bases de datos y obtener alertas sobre transacciones que salen fuera del perfil de los clientes. Las principales características de los programas AML consisten en la extracción, procesamiento y compilación de la base de datos central del banco de la información transaccional de los clientes en un período determinado, que con base a la parametrización automatizada de filtros de montos y umbrales de las variables de información (cuantitativas y cualitativas) permite establecer operaciones que están fuera del perfil de riesgo asignado a los clientes.

8) Tiene en cuenta factores humanos y culturales

Al ser la administración de riesgos un proceso iterativo y dinámico es fundamental identificar la "cultura organizacional" y la actitud respecto a la prevención y mitigación de los riesgos asociados al LAFD, ya que gran parte de las acciones de control van a ser ejecutados por parte del propio personal del banco, como parte del rol continuo de sus funciones dentro de la entidad.

9) Es transparente e inclusiva

La apropiada y oportuna participación de los grupos de interés (stakeholders) en la administración de gestión de riesgos y en particular de los responsables de todos los

niveles de la organización, asegura que esta gestión permanezca activa, en marcha y respaldada por todo el personal de la entidad bancaria para cumplir los objetivos de control preventivo.

10) Es dinámica, iterativa y sensible al cambio

La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la entidad y su entorno. Al igual que el avance tecnológico se desarrolla de forma acelerada, así también las metodologías de control de LAFD deben ser flexibles, cambiantes y dinámicas en sus enfoques de gestión.

11) Facilita la mejora continua de la organización

Las organizaciones deben desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto que le ayude a la entidad a optimizar sus procesos y recursos para lograr la reducción de riesgos, así como un crecimiento sostenido de sus operaciones para mantenerse como una empresa en marcha en el mercado que opera.

1.2 Comunicación y consulta

Al tratarse de riesgos de LAFD corresponde al equipo de la Unidad de Cumplimiento impulsar las medidas desarrolladas para mejorar los términos del sistema de gestión de riesgos. De hecho, la normativa vigente señala entre las atribuciones del oficial de cumplimiento, respecto a sus funciones de comunicación y consulta las siguientes:

- Coordinar con la administración en la elaboración de la planificación de cumplimiento para prevención de lavado de activos y financiamiento de delitos de la entidad (JBE 2012, 27), esta tarea demanda una comunicación interior dinámica, interactiva y continua entre las partes.
- Cumplir con el rol de enlace con autoridades e instituciones en materia de prevención de lavado de activos y financiamiento de delitos, para lo cual debe existir un adecuado y formal canal de comunicación y consulta (JBE 2012, 29).

En torno a la gestión del oficial de cumplimiento se encuentran los actores internos y externos que interactúan con la administración de gestión de riesgos. Entre los actores internos tenemos a todas las áreas y funcionarios de la entidad bancaria como el Directorio, Junta de Accionistas, Gerencia General, Comité de Cumplimiento,

Auditoría Interna, áreas de negocio, operativas y apoyo, empleados, entre otros; en tanto que entre los actores externos se encuentran los organismo de control (UAFE, Superintendencia de Bancos), Fiscalía General, Banco Central, Defensoría del Cliente, gremios y asociaciones, otros organismos gubernamentales y demás poderes del Estado, así como el resto de actores como los bancos corresponsales del exterior, remesadoras de dinero, entre otros.

Además, la gestión de riesgos debe fusionarse y acoplarse con otras áreas y funciones organizacionales complementarias incluyendo por ejemplo, la investigación de nuevos segmentos de mercado, productos, cumplimiento de políticas y normativa, retroalimentación de clientes y actores externos, planeación estratégica, inteligencia de negocios, marketing digital, comercio electrónico, comercio justo, entre otros.

1) Fuente de valor agregado para la entidad

Es importante compartir y dar a conocer los beneficios del control de riesgos entre los funcionarios de la entidad, puesto que ellos deben ser la fuerza estratégica aliada del oficial de cumplimiento para poder identificar las áreas y procesos operativos críticos susceptibles a estos riesgos y cuya colaboración en conjunto ayudará aparte del cumplimiento de los controles preventivos, al alcance de las metas de negocio, en especial los ejecutivos del área comercial que manejan portafolios de clientes. En este sentido, alinear los objetivos de la gestión de riesgo de LAFD con los objetivos de negocio, son *una prioridad y una oportunidad* de practicar el principio "ganar, ganar" para todas las partes.

La comunicación con los grupos de interés externos puede proveer seguridad y confianza sobre áreas críticas e información de mutuo interés, tal es el caso de las listas restrictivas de control, sistemas de monitoreo, personas en procesos judiciales de seguimiento, enfoques de control para cumplimiento de la normativa, entre otros. Este compromiso externo también agrega valor creando asociaciones y alianzas para la obtención de resultados y beneficios comunes para las partes mediante una acción conjunta, a través del intercambio de información que se puede desarrollar y coordinar mediante el Comité de Oficiales de Cumplimiento, la Asociación de Bancos Privados, autoridades judiciales, organismos de control, entre otros.

2) Incorporar varios puntos de vista

Las percepciones pueden variar entre los distintos actores internos, esto es entre el oficial de cumplimiento, funcionarios del negocio, los miembros del equipo de un proyecto y otros grupos de la institución, por lo que es indispensable mantener de forma

continua canales de comunicación abiertos para la discusión, retroalimentación, acuerdos y toma de decisiones consensuadas.

Tabla 6
Percepciones internas sobre prevención de lavado de activos

Oficial de cumplimiento	Áreas de negocio	Áreas operativas
Aplicar el programa de prevención de LAFD	Alcanzar las metas y presupuestos comerciales sin incumplir controles	Procesar operaciones en los tiempos establecidos
Atender requerimientos de organismos de control	Ejecutar los controles de prevención de LAFD definidos	Facilitar la parametrización de controles automáticos
Atender pedidos de bancos corresponsales del exterior	Solicita a clientes los justificativos de transacciones alertadas	Apoyar la gestión de nuevos proyectos de control de LAFD
Informar actividades al Comité de Cumplimiento y de Riesgos	Crecimiento de cartera de clientes aplicando políticas de control LAFD	Automatizar procesos de control de LAFD
CANALES DE COMUNICACIÓN PARA LOGRAR CONSENSOS Y ACUERDOS		

Fuente y elaboración propia

Es importante dar a conocer las expectativas e incertidumbre de los diversos actores internos, en especial las de las áreas comerciales, ya que son los funcionarios de estas áreas de las que en buena parte depende el diseño y cumplimiento de los controles *para la aceptación del riesgo por parte del banco*, basados en criterios tales como:

a. La aceptación o no de ciertos tipos de negocios o actividades económicas de los clientes catalogadas como riesgosas (negocios con altos flujos de efectivo, casas de cambio y cambistas informales, actividades de minería ilegal, courier, transporte de valores, comercio informal, entre otros).
b. El nivel de severidad y exigencia del control que se puede ejercer sobre una actividad económica en la que se desempeñan los clientes, sin afectar la relación comercial y hasta manejar un cierto grado de molestia de dichos clientes.
c. Las potenciales consecuencias negativas que por error u omisión puede ocasionar al banco y a sus funcionarios la materialización de estos riesgos.

3) Promover un ambiente de confianza

En el ámbito local, los bancos privados del país en cumplimiento con las mejores prácticas colaborativas dispuestas por el GAFI generan un esfuerzo y trabajo en conjunto con los organismos de supervisión y control, las autoridades judiciales, gremios y asociaciones sectoriales e incluso se ha desarrollado un marco de cooperación internacional con entidades y contrapartes del exterior para poner en marcha programas de apoyo y colaboración recíproca para fortalecer los controles.

4) Optimizar la evaluación de riesgos

Un enfoque integral va a permitir un proceso de evaluación del riesgo más óptimo, ya que la experiencia y conocimiento de los diferentes actores internos del banco tiende a mejorar dicho enfoque y la comprensión de estos riesgos. Si se toma en cuenta la diversidad de percepciones, se amplía y enriquece el contexto de discusión y evaluación de los riesgos y se puede llegar a establecer *criterios de control consensuados* respecto a los riesgos, su tratamiento y consecuencias.

Con la finalidad de tener una visión global de las partes interesadas es conveniente elaborar una matriz de los principales actores, identificando en ella las personas, grupos o instituciones, sus funciones y roles generales, la importancia de cada actor, cómo contribuyen al programa de prevención de LAFD, cómo pueden retrasar el programa y la estrategia para lograr la colaboración del actor (Anexo 2).

1.3 Establecer el contexto

La gestión de riesgos al ser un sistema abierto y flexible se ve afectada por los cambios del entorno del mercado financiero, tales como nuevas regulaciones normativas locales o recomendaciones internacionales, políticas gubernamentales y régimen económico que afectan las condiciones de negocio de los bancos, así como también los cambios que se producen al interior de la institución, como puede ser la reorientación estratégica, desarrollo de nuevos productos y servicios, cambios en tecnologías, cambios de miembros de la alta gerencia, procesos de fusión, clima organizacional, elementos culturales que afectan el desempeño del control, entre otros.

Para asegurar que se consideren todos los riesgos específicos significativos, es indispensable conocer los objetivos de cada línea de negocio, tipo de banca, producto o canal de servicio y en general toda la información relacionada con el origen y el manejo del flujo de fondos de los clientes del banco.

1.3.1 Objetivos del contexto

- Implementar un sistema de administración de riesgo de LAFD que evite que los servicios financieros de la entidad sea utilizada para estas actividades ilícitas.
- Fomentar una cultura organizacional de compromiso y prevención en todos los niveles de la institución bancaria.

- Alinear los objetivos de control dentro de los objetivos estratégicos de negocio de la entidad, bajo la consideración que un adecuado sistema de gestión de riesgos permitirá incrementar negocios que se verá reflejado en la rentabilidad.
- Cumplir con las disposiciones legales y regulatorias de esta materia.

En este punto es necesario revisar documentos e información, que permitan reforzar el conocimiento del negocio y el contexto del proceso de gestión de riesgos, tales como:

- El plan estratégico y de negocios de la entidad.
- Contenido de informes anuales y semestrales del oficial de cumplimiento.
- Informes de auditoría interna, auditoría externa o revisiones del organismo de control respecto a la revisión de la gestión desarrollada por parte de la Unidad de Cumplimiento y demás áreas responsables de la tarea de prevención.
- Análisis económicos y cualquier otra documentación relevante sobre el banco, que generalmente están contenidos en la memoria anual.

1.3.2 Identificación y análisis de las partes

El análisis de stakeholders bajo el enfoque de la gestión de riesgo de LAFD se debe llevar a efecto en una etapa temprana de dicho proceso. Este análisis al menos debe considerar a las siguientes partes:

- El directorio, los accionistas y la alta dirección.
- Altos ejecutivos, gerentes comerciales, gerentes y jefaturas de unidades de negocio u operativas y demás empleados que podrían verse afectados.
- Autoridades de supervisión, control y judiciales.
- Proveedores externos y otras instituciones financieras locales o del exterior.
- Otros actores identificados.

1.3.3 Criterios de determinación y medición de los niveles de riesgo

Estas medidas pueden estar dadas por indicadores de desempeño, tales como: número de reportes de operaciones sospechosas a la UAFE, número de clientes gestionados en listas restrictivas, número de pedidos de información requeridos por organismos de control y/o bancos corresponsales, entre otros.

Al establecer el contexto, se puede considerar escalas de valoración del riesgo que definen la criticidad de cada uno de los componentes que forman parte de los factores de riesgo que serán tratados más adelante. Los criterios de valoración sugeridos se describen a continuación:

- ***Riesgo bajo*** (1).- Al materializarse los riesgos, la imagen de la institución bancaria no se ve afectada.
- ***Riesgo medio*** (2).- Al materializarse los riesgos, la imagen de la institución bancaria no se ve afectada ante sus clientes y los demás bancos nacionales, sin embargo puede ser objeto de llamados de atención por parte de los organismos de control.
- ***Riesgo alto*** (3).- Afectan a la imagen y reputación de la entidad bancaria, enfrenta problemas de tipo legal y sanciones pecuniarias impuestas por los organismos de control y se pueden ver afectadas las relaciones con la banca corresponsal.
- ***Riesgo extremo*** (4): Al materializarse los riesgos, afectan de manera significativa la imagen y reputación de la entidad bancaria, enfrenta sanciones de tipo legal y sanciones pecuniarias impuestas por los organismos de control y se pueden ver afectadas las relaciones con la banca corresponsal, posibilidad de suspensión temporal de operaciones.

1.4 Identificación de riesgos

El propósito de esta etapa es generar una amplia lista de fuentes de riesgos y eventos de LAFD que pueden tener un alto impacto en el logro de los objetivos del banco, identificados en el contexto respecto a la administración del riesgo. Para facilitar la identificación de riesgos se puede utilizar listas de verificación (check list), juicios basados en la experiencia (criterio experto) y registros históricos, diagramas de flujo, lluvia de ideas, talleres de evaluación de riesgos, entre otros. Además de la revisión de información relevante tales como:

- Reportes de reclamos sobre clientes inconformes con la cancelación de cuentas por falta de justificación de transacciones.
- Reportes de transacciones sospechosas reportadas a la UAFE y sus tipologías.

- Resultados e informes de auditoría (interna y externa) y de las inspecciones de la Superintendencia de Bancos, en esta materia.
- Experiencia local o del exterior obtenida en revistas especializadas, congresos, foros, seminarios o cursos de capacitación.
- El juicio de los expertos como resultado de las reuniones del Comité de Oficiales de Cumplimiento o de la Asociación de Bancos Privados del Ecuador.

Cabe mencionar que la labor de identificación de riesgos, puede diferir de una entidad a otra, en función de las percepciones y expectativas con las que se aborda estos riesgos y otros factores tales como el tamaño de la entidad, estilo de dirección, cultura organizacional, el entorno de la organización, entre otros, por lo que los factores de riesgo que se detallan más adelante son los mínimos requeridos para realizar una adecuada e integral identificación y gestión del riesgo. Los factores que se detallan más adelante corresponden a un caso real de identificación de riesgos de un grupo de bancos locales (Banco Pichincha, Rumiñahui, Loja y Diners).

Tabla 7
Identificación de factores de riesgos de los bancos locales

Condiciones de amenaza
a.- Tipo de cliente
b.- Persona natural / jurídica
c.- Zona geográfica
d.- Transacciones
e.- Conducta inusual observada

Condiciones de vulnerabilidad
a.- Productos y servicios
b.- Canal de atención

Fuente y elaboración propia

En esta etapa se identifican los elementos que actúan como *agentes generadores del riesgo*, tomando como punto de partida los mencionados en la normativa local referente a clientes, productos y servicios, canales y situación geográfica (JBE 2012, 7).

Corresponde al oficial de cumplimiento de la entidad bancaria liderar y coordinar el proceso de identificación de los riesgos de LAFD, así como incorporar una metodología para identificar y administrar el riesgo, que en el presente caso se basa en las directrices de la norma ISO 31000.

Es común que la Unidad de Cumplimiento o el área e Talento Humano realice además el monitoreo interno periódico de las transacciones de los empleados del banco, tomando en consideración los diferentes niveles de riesgo y solicitando justificaciones en casos de alertas que excedan de manera significativa el perfil asignado al empleado respecto a ingresos ajenos a las remuneraciones percibidas en relación de dependencia.

1.5 Análisis de riesgos

Esta fase comprende el proceso por el cual se lleva a cabo la separación de los elementos en grupos homogéneos al interior de ellos y heterogéneos entre ellos. La separación se fundamenta en el reconocimiento de las diferencias significativas en sus características e identificación de los componentes asociados a cada uno de los factores de riesgo. Dada la capacidad instalada de personal de la Unidad de Cumplimiento, es necesario enfocar el esfuerzo de análisis en aquellos casos que dada su relevancia, tienen una alta probabilidad de estar asociados a operaciones sospechosas que pueden ocasionar consecuencias graves para el banco.

El resultado de la metodología indicada en el párrafo anterior, está en función de cada uno de los componentes que forman parte de los factores de riesgo identificados y su fuente de origen, que luego derivarán en la asignación de un perfil de riesgo demográfico y transaccional, conforme sus características individuales.

1.5.1 Según las condiciones de amenaza

a) Tipo de cliente

Conformado por personas naturales (riesgo alto) y jurídicas (riesgo medio).

- Clientes que presentan elevado número de casos con transacciones inusuales en sus cuentas; prestan sus cuentas a terceras personas para que realicen transacciones que no corresponden a su actividad económica; clientes que tienen acceso a fondos públicos y que eventualmente los pueden desviar para su beneficio propio; propietarios de negocios que por su transaccionalidad y montos no han sido formalizados.
- Clientes que realizan transacciones con personas que residen en países no cooperantes o paraísos fiscales, alta transaccionalidad de transferencias enviadas y recibidas de paraísos fiscales, no cooperantes o sancionados por organismos de control internacionales, clientes que realizan transacciones que no están de acuerdo con su actividad económica o su patrimonio no guarda relación con el giro de su negocio.

b) Zona geográfica (agencia u oficina de anclaje del cliente)

Corresponde a la sucursal, agencia u oficina a la que se encuentra anclado o asignado comercialmente el cliente y/o la cuenta de la cual es titular. Cada entidad

bancaria mantiene una calificación de riesgo por zona, regional, ciudad y agencia, con base a un historial de casos de ocurrencia de transacciones inusuales injustificadas, fraudes operativos, entre otros. Generalmente esta información es levantada y mantenida por el área de Riesgos y Cumplimiento.

- *Oficinas ubicadas en:* zonas vulnerables al almacenamiento o acopio de estupefacientes y al tráfico de armas; zona de frontera que es atractiva para actividades de narcotráfico y contrabando; existe alta transaccionalidad y circulación de dinero en efectivo que pueden estar relacionadas con actividades ilícitas que producen grandes montos de efectivo, cercanas a puertos marítimos o aeropuertos que constituyen en puntos de entrada y salida de estupefacientes y contrabando.
- *Oficinas en*: zonas con alta presencia de negocios informales conformados tanto por clientes locales, como por extranjeros indocumentados; oficinas donde una sola persona realiza múltiples depósitos para varios clientes; presencia de clientes renuentes a presentar información personal o de sus negocios.
- Oficinas donde se presentan fraccionamiento de transacciones en un mismo día con el propósito de evadir el control de umbrales del banco. Procesamiento de transacciones en lugares distintos a la zona de residencia del cliente, sobre todo en zonas fronterizas.
- Clientes que habitualmente transaccionan en las oficinas indicadas, donde no abrieron los clientes sus cuentas con el fin de no ser identificados.

c) Transacciones

Está constituido por todas las transacciones que los clientes realizan en el banco por cualquier canal de atención.

- Operaciones que deliberadamente son fraccionadas para ser procesadas en un mismo día con el fin de eludir controles de licitud y origen de fondos; aceptación de depósitos superiores al umbral sin previa verificación de su origen; transferencias recibidas y enviadas del y al exterior por medio de países no cooperantes o paraísos fiscales; un mismo cliente realiza múltiples transferencias por montos considerables a diversos países y dirigidos a diferentes beneficiarios.
- Captación de inversiones en efectivo y sin solicitar al cliente el origen de los fondos; pago anticipado total o parcial de deudas sin una razón aparente,

especialmente si se realizan en efectivo; emisión de cheques de gerencia o del exterior a nombre de terceros sin que el cliente presente documentos de justificación; transferencias internas o interbancarias por diversos medios electrónicos.

- Cancelación de préstamo con certificados de depósitos que garantizan la operación; pre-cancelación de inversiones sin que al cliente le interese la penalización en el pago de intereses; excesivos consumos con tarjeta de crédito cuya totalidad es cancelada en efectivo; cancelación de préstamo con efectivo.

d) Conducta inusual observada

Relacionada con la cantidad de alertas generadas por el sistema de monitoreo, así como las relaciones identificadas con otros clientes dentro de la entidad, también se incluye los pedidos de información de las autoridades judiciales y los pedidos de información de bancos corresponsales para justificar transacciones.

1.5.2 Según las condiciones de vulnerabilidad

a) Productos y servicios

Está conformado por los productos y servicios financieros ofrecidos por el banco a sus clientes de acuerdo a sus necesidades.

- Utilización de cuentas para acreditar dinero a personas que pueden ser o no beneficiarias; la transaccionalidad se realiza mediante medios tecnológicos como cajeros automáticos o cash management; alto número de clientes a quienes no se les ha definido un producto para control de transaccionalidad.
- Productos en los que se realizan todo tipo de transacciones ya sea por ventanilla o por medios electrónicos; susceptible a recibir transacciones ya sea de clientes propietarios o de terceras personas; tienen acceso personas naturales y jurídicas sean estas nacionales y extranjeras..
- Se presentan productos destinados a migrantes que les permite enviar remesas del exterior a través de remesadoras con las que el banco no tiene convenios; cuentas dirigidas al segmento empresarial con alta transaccionalidad de efectivo.
- Productos dirigidos al ahorro programado donde el dinero permanece a un plazo determinado sin que el cliente lo pueda retirar; productos donde se transacciona con euros e interviene la cotización de divisas; productos que no registran clientes ni cuentas para operar.

b) Canales

Son todos los medios físicos, electrónicos y virtuales a través de los cuales el cliente tiene acceso a realizar sus transacciones (dentro o fuera del país) y consultas en línea sobre sus cuentas, gran parte de las cuales se ejecutan y afectan en línea.

- Canal vulnerable a los fraudes y delitos informáticos; se realizan transacciones en línea sobre todo transferencias, sin que se justifique su ejecución; acreditación de dinero a varias personas que pueden ser o no beneficiarias, mediante el proceso de pago a proveedores o rol de pagos; depósitos en efectivo por medio de cajeros depositarios sin que exista un límite para hacerlo.
- Canales donde se realiza la mayor cantidad de transacciones sobre todo en efectivo; vulnerabilidad a los asaltos puesto que es de libre acceso para clientes y no clientes.
- Consultas o movimientos de dinero con información sustraída de clientes; vulnerabilidad al robo de claves para ingreso a los aplicativos internos.
- Apertura de cuentas sin que previamente se solicite al cliente la documentación personal de respaldo.

Tabla 8
Detalle de canales de servicios bancarios

Canales	Detalle del canal	Riesgo
FÍSICO	Agencias	Alto
	Ventanilla de atención	Alto
	Puntos pago	Medio
	Ventanilla Express	Bajo
	Corresponsal no bancario (CNB)	Bajo
INTERNET	Banca electrónica personas	Extremo
	Banca electrónica empresas (cash management)	Extremo
AUTOSERVICIO	Kioscos de consultas y transacciones	Alto
	Cajeros automáticos	Medio
	Depositarios	Medio
CELULAR	Servicio telefónico transaccional en agencia	Bajo
	Celular	Medio
	Dispositivos móviles	Medio
TELEFÓNICO	IVR (Interactive Response Unit) reconocimiento de voz	Medio
	Call center	Medio
	Telemercadeo	Bajo

Fuente y elaboración propia

Existe un control en línea sobre el nombre y número de identificación de los clientes y partes interesadas en una transacción (dentro o fuera del país) que los bancos han implementado al inicio y durante la vigencia de la relación comercial con los clientes, cuyas transacciones son objeto de verificación previa a su ejecución (Anexo 3).

1.6 Evaluación del riesgo

Con base a los resultados de la etapa de análisis y con el criterio experto del oficial de cumplimiento, en esta etapa se aplica procedimientos de valoración, que determinan el nivel de riesgo de cada uno de los componentes que forman parte de los factores de riesgo.

1.6.1 Análisis cualitativo

En este análisis se utiliza ideas textuales para describir la magnitud de las consecuencias potenciales y la probabilidad que ocurran esas consecuencias, se utiliza información que tiene relación con cada uno de los componentes que forman parte de los factores del riesgo. Dichos eventos definen el nivel de riesgo de cada uno los componentes de acuerdo a sus propias características. La información se puede obtener de las siguientes fuentes:

- Artículos de prensa, literatura relevante de organismos locales e internacionales, análisis y estudios realizados por organismos reconocidos que emiten información relacionada con análisis de riesgos.
- Señales de alerta, tipologías u operaciones inusuales y sospechosas, emitidas por la UAFE u otros organismos internacionales (GAFILAT, GAFISUD).
- Informes de casos relacionados con prevención de LAFD.
- Información histórica relevante de la entidad o sector económico.

1.6.2 Análisis cuantitativo

El análisis cuantitativo utiliza cifras numéricas y estadísticas lo cual determina la asignación de un nivel de riesgo a los componentes que forman parte de los factores. La calidad del análisis e información obtenida, dependen mucho de la precisión e integridad de las cifras estadísticas utilizadas.

Para la determinación del riesgo mediante esta metodología, se puede utilizar un modelo o matriz de valoración con base a datos históricos reales, tales como: información mensual con montos transados de clientes remitidos al organismo de control, estadísticas de monitoreo transaccional, ponderaciones de riesgos, número de alertas presentadas por cliente, tipologías de transacciones injustificadas presentadas por

clientes que en su oportunidad fueran reportadas a la UAFE por presentar señales de alerta que no fueron justificadas, entre otras.

1) Determinación de niveles de riesgo

Una vez identificadas las características particulares de cada uno de los componentes y con base a la definición de los análisis cuantitativo y cualitativo, que pueden ser aplicados de forma individual o combinada, se puede establecer escalas de valoración del riesgo que definen la criticidad de cada uno de los componentes que forman parte de los factores definidos como son: clientes (incluye empleados) y las operaciones realizadas en la entidad bancaria y que fueron definidos en el establecimiento del contexto, estos son: "Riesgos Bajo, Medio, Alto y Extremo".

2) Consolidación de factores para comparar el riesgo de clientes con los parámetros definidos

Cada uno de los factores identificados forma parte de la matriz de riesgo, que una vez consolidados permiten establecer un nivel de riesgo real que facilita la comparación con los niveles de riesgo definidos en el establecimiento del contexto y en la presente etapa. Los factores son aquellos que ponderados en conjunto, determinan el nivel de riesgo de clientes del banco, considerando que:

- Cada componente que forma parte de un factor de riesgo, es medido por medio de la asignación de un nivel de riesgo, cuyo resultado es producto del análisis cualitativo y cuantitativo realizada para cada uno de ellos.
- Una vez que se determina el nivel de riesgo de cada uno de los componentes se procede a asignar un peso porcentual (ponderación de riesgo no debe exceder al 100%) a cada uno de los factores de riesgo que forman parte de la matriz, de acuerdo a su importancia e impacto que estos pueden representar al banco.
- La relación del valor porcentual asignado a los factores con el nivel de riesgo establecido para sus componentes (multiplicación), genera un puntaje por cada uno de los factores.
- La suma de los puntajes obtenidos por cada factor, genera un resultado, el mismo que es comparado con una escala de medición, la cual determina el perfil de riesgo del cliente con base a los factores de amenaza y vulnerabilidad.
- Los rangos de valoración que se pueden establecer para los factores de riesgo de clientes y las operaciones se pueden situar en función del criterio experto de cada entidad bancaria, que por lo general puede ser de uno a cuatro (1 a 4 o 5) o

en la escala de cero a cien (0 – 100). Las escalas van a estar en función del sistema o software tecnológico que posea cada banco (Sentinel Compliance & Risk, Monitor, Assist) que usualmente contemplan una de las escalas indicadas.

Tabla 9
Rangos para la calificación de riesgos

Rangos	Riesgo
1,00 - 1,80	BAJO
1,81 - 2,60	MEDIO
2,61 - 3,40	ALTO
3,41 - 4,00	EXTREMO

Rangos	Riesgo
0 - 1,0	BAJO
1,1 - 2,0	MEDIO
2,1 - 3,0	MEDIO
3,1 - 4,0	ALTO
4,1 - 5,0	EXTREMO

Rangos	Riesgo
0 - 65	BAJO
66 - 85	MEDIO
86 -89	ALTO
90 - 100	EXTREMO

Fuente: Escalas de valoración de los sistemas automatizados
Elaboración propia

3) Matriz de valoración de riesgos en el análisis de operaciones inusuales

Es una herramienta de control y gestión utilizada para identificar riesgos y minimizarlos mediante la aplicación de controles adecuados, con la finalidad de que los productos y servicios de la entidad bancaria, no sean utilizadas por los clientes para actividades de LAFD. Esta matriz incluye el análisis y ponderación de las variables cualitativas y cuantitativas que recomienda se incluya en el análisis integral del riesgo la Superintendencia de Bancos.

Las definiciones que se detallan más adelante son *propuestas* con base a los *criterios reales* y análisis de información que un grupo de bancos privados del país aplica en la práctica para establecer el perfil demográfico y transaccional de los clientes. Los valores del componente de riesgo (bajo, medio, alto y extremo) son tomados de la *valoración del riesgo* que se detallaron en cada uno de los factores identificados en la etapa de análisis del riesgo. En tanto que los valores de la ponderación de factores de riesgo fueron establecidos en función de la criticidad e importancia de cada factor identificado y sujeto al análisis de riesgo.

Para *conjugar y combinar varios de los factores de riesgo* de clientes (incluye empleados), canales y operaciones indicadas en esta sección, se procede a desarrollar la "Matriz de valoración de riesgos en el análisis de operaciones inusuales de lavado de activos y financiamiento de delitos". Los factores sobre los que opera esta matriz son:

a. *Condiciones de vulnerabilidad (Impacto)*: productos y canales
b. *Condiciones de amenaza (Probabilidad)*: cliente: tipo de persona, zona geográfica, comportamiento transaccional y actividad inusual registrada

Para una mejor ilustración se va a proceder a desarrollar la matriz indicada, con la finalidad de obtener una valoración del riesgo en el análisis de transacciones inusuales con base a la *combinación de factores de clientes, transacciones y canales* que pueden estar relacionados a potenciales casos de LAFD. Los criterios de asignación de pesos y ponderaciones de los diversos factores de riesgo están dirigidos a ejemplos didácticos para registrar y completar esta matriz de riesgo utilizando una escala de valoración, que en el presente caso se utiliza la escala de 1 a 5 (0 a 1= bajo; 1,1 a 3,0= medio; 3,1 a 4,0= alto y de 4,1 a 5,0 = extremo).

- **Análisis de condiciones de vulnerabilidad**

Factor producto

Los productos más sensibles a este tipo de riesgo son las transferencias al exterior que tienen como origen o destino países o jurisdicciones sensibles, operaciones de compra y venta de divisas y las operaciones acreditadas en cuentas. En función de los productos, la matriz permite marcar las operaciones que cumplen tal condición.

Tabla 10
Sección: Análisis del factor producto

Productos y servicios					
Tipo	**Sub factor**	**Valor**	**Score**	**Ponderación**	**Resultado**
Cheque de gerencia		x	0,00	60%	0
Cuenta corriente	x	x	0,40	60%	0,24
Cuenta de ahorros	x	x	2,00	60%	1,2
Inversiones		x	0,00	60%	0
Operaciones de cambio		x	0,00	60%	0
Transferencias al / del exterior					
- Hacia o desde países sensibles	x	x	1,00	60%	0,6
- Hacia o desde otros países	x	x	0,50	60%	0,3
Otros	x	x	0,10	60%	0,06
TOTAL DEL FACTOR			**4,00**	**60%**	**2,40**

Fuente: Matriz de valoración de riesgos
Elaboración propia

La mayor ponderación se asigna a los productos más comunes de los bancos como son las cuentas de ahorro con un riesgo medio (2) y las transferencias enviadas y recibidas a países sensibles y otros países con una calificación de 1 y 1.50 respectivamente; las cuenta corrientes con un riesgo bajo del 0,4; y otros productos con un 0,10; todos estos productos en el presente ejemplo representan el 60% de ponderación del factor producto con relación a la condición de vulnerabilidad.

Factor canal de atención

La mayor ponderación en este factor puede ser asignada a aquellas operaciones que se realizan a través de ventanilla que es el canal físico más común utilizado por los

clientes que se la asigna con un riesgo medio (2), así como las efectuadas en cajeros automáticos que se le otorga un riesgo medio (1,50) que son los canales más importantes; sin dejar de considerar la actual tendencia de utilizar los servicios de los corresponsales no bancarios (CNB) como un canal de atención masiva de cobertura de clientes que se le asigna un riesgo bajo (1) debido a que en este canal las transacciones y montos son restringidos. La suma de la calificación de todos los canales de atención de clientes en el presente ejemplo representa el 40% de ponderación de este factor.

Tabla 11
Sección: Análisis del factor canal de atención

Canal de atención transaccional					
Tipo	**Sub factor**	**Valor**	**Score**	**Ponderación**	**Resultado**
Ventanilla de atención	x	x	2,00	40%	0,8
Puntos pago		x	0,00	40%	0
Ventanilla express		x	0,00	40%	0
Corresponsal no bancario (CNB)	x	x	1,00	40%	0,4
Banca electrónica personas		x	0,00	40%	0
Kioscos consultas y transacciones		x	0,00	40%	0
Cajeros automáticos	x	x	1,50	40%	0,6
Celular		x	0,00	40%	0
TOTAL DEL FACTOR			**4,50**	**40%**	**1,80**

Fuente: Matriz de valoración de riesgos
Elaboración propia

Esta matriz incorpora los diferentes tipos de canales (físico, internet, autoservicio) analizados en los factores de vulnerabilidad. Dependiendo de los canales transaccionales utilizados es posible marcar una o todas las opciones de este factor.

Una vez analizados las *condiciones de vulnerabilidad* de los factores: producto y canal de distribución, que obtuvieron la calificación de 2,40 y 1,80 respectivamente, se determina que el *análisis de vulnerabilidad* muestra el resultado de 4,20.

- **Análisis de condiciones de amenaza**

  Factor persona o cliente

El primer criterio es establecer si se trata de una persona natural o jurídica, o un cliente catalogado “sensible”, cada uno de ellos con ponderaciones de riesgo distintas. Se considera el cliente sensible, a una persona natural o jurídica que por su condición legal o características propias de exposición al riesgo de LAFD de entrada es identificado y marcado para su posterior análisis dentro de la matriz de riesgo en combinación y ponderación con el resto de factores.

En el presente ejemplo, para continuar con el desarrollo de la matriz de riesgo se considera el caso de un cliente sensible al cual se le asigna un riesgo extremo (5) por su exposición y condición inherente del riesgo, este factor cliente representa el 15% de

ponderación que está dentro de las condiciones de amenaza, debiendo recalcar que cada banco puede asignar o valorar el riesgo de acuerdo a su percepción propia del riesgo.

Tabla 12

Sección: Análisis del factor persona o cliente

Personas					
Tipo de cliente	**Sub factor**	**Valor**	**Score**	**Ponderación**	**Resultado**
Persona natural		x	0,00	15%	0
Persona jurídica		x	0,00	15%	0
Clientes sensibles (ONG, casas de cambio, extranjeros no residentes, PEPs, otros)	x	x	5,00	15%	0,75
TOTAL DEL FACTOR	**15% (5)**				**0,75**

Fuente: Matriz de valoración de riesgos
Elaboración propia

Tabla 13

Sección: Proceso de análisis del factor persona natural

Persona Natural	**Sub factor**	**Valor**	**Score**	**Ponderación**	**Resultado**
a) Edad					
De 18 a 25 años		x	0,00		0
De 26 a 35 años	x	x	4,00	40%	1,6
De 36 - 65 años		x	0,00		0
Mayor a 66 años		x	0,00		0
b) Tipo de documento					
Cédula de identificación		x	0,00		0
RUC		x	0,00		0
Carnet de extranjería		x	0,00		0
Pasaporte	x	x	5,00	20%	1
c) Antigüedad					
Menor a 1 año	x	x	5,00	10%	0,5
De 1 a 5 años		x	0,00		0
De 6 a 10 años		x	0,00		0
Mayor a 10 años		x	0,00		0
d) Actividad económica					
Relación de dependencia		x	0,00		0
Independiente					
- Formal		x	0,00		0
- Informal	x	x	5,00	15%	0,75
e) Condición del contribuyente -SRI					
Activo		x	0,00		0
Inactivo		x	0,00		0
Suspensión temporal	x	x	5,00	15%	0,75
Suspensión definitiva		x	0,00		0
TOTAL DEL FACTOR	**15% (4,6)**				**0,69**

Fuente: Matriz de valoración de riesgos
Elaboración propia

Respecto a los sub-factores la mayor calificación de riesgo alto (4) se le asigna a la edad del cliente en el rango de edad de 26 a 35 años, puesto que en este segmento según las estadísticas de ciertos bancos se da la mayor ocurrencia de transacciones inusuales que terminan siendo reportadas a la UAFE, cuya ponderación dentro del factor es del 40%; el tipo de documento de identificación del cliente tiene un riesgo extremo (5) y representa el 20%; la actividad económica y la condición del

contribuyente que son sub-factores interrelacionados tienen un riesgo extremo (5) y representa el 15%; y la antigüedad de la cuenta también con riesgo extremo (5) con el 10% que en el presente caso se trata de una cuenta nueva menor a un año.

El análisis contempla a personas naturales y jurídicas, quienes representan el elemento potencial de riesgo. En personas naturales se incluye sub-factores relacionados con: edad, tipo de identificación, antigüedad, actividad económica y la condición del contribuyente ante el Servicio de Rentas Internas (SRI) para conocer el grado de formalidad de la actividad económica. Estos criterios son determinantes, cuando una vez concluido el análisis del resto de factores se debe revisar la excepción de inusualidad en la transaccionalidad del cliente, en función de las señales de alerta y las características propias del mismo.

Para el análisis de las personas jurídicas además se considera la fecha de constitución de la empresa, domicilio fiscal, antigüedad como cliente y la condición del contribuyente ante el SRI.

Factor zona geográfica

La ponderación de este factor se establece con base a la frecuencia que el cliente acude a las oficinas del banco en la ciudad de residencia o al interior del país, así como las zonas donde es conocido circulan flujos de fondos producto de actividades ilegales (narcotráfico, trata de personas, tráfico de armas, extorsión, etc.) en busca de ingresar fondos a los bancos sin ser detectados para configurar el delito de lavado de activos.

Tabla 14
Sección: Análisis del factor zona geográfica

Zona geográfica o territorio	Sub factor	Valor	Score	Ponderación	Resultado
a) Oficinas ubicadas en Quito					
El Recreo	x	x	2,00	30%	0,60
Atahualpa	x	x	1,50	30%	0,45
Panamericana Sur	x	x	0,50	30%	0,15
Alameda	x	x	0,50	30%	0,15
El Condado	x	x	0,50	30%	0,15
b) Oficinas ubicadas en provincias					
Zona de fronteras (norte y sur)	x	x	2,00	70%	1,40
Zonas francas	x	x	1,50	70%	1,05
Zonas afectadas por actividad ilegal	x	x	0,50	70%	0,35
Zonas de región oriental	x	x	0,50	70%	0,35
Otros	x	x	0,50	70%	0,35
TOTAL DEL FACTOR	**10% (5)**				**0,50**

Fuente: Matriz de valoración de riesgos
Elaboración propia

Para el presente ejemplo se asigna la calificación del riesgo del componente de acuerdo a la categoría o nivel de riesgo de cada agencia bancaria local definida por el

banco cuya ponderación de este sub-factor representa el 30%; en tanto que a las oficinas ubicadas en provincia se las asigna con un 70% por el mayor riesgo que representa en especial aquellas zonas de frontera y las afectadas por actividad ilegal.

Factor transacciones

Este factor es importante para la determinación de potenciales casos de LAFD al interior de las entidades bancarias, ya que estas transacciones son los mecanismos utilizados para el ingreso (colocación) y diversificación de fondos de origen ilícito en la operatividad del flujo de fondos de los bancos.

Tabla 15
Sección: Análisis del factor transacciones

Transacciones	Sub factor	Valor	Score	Ponderación	Resultado
a) Moneda transada					
Dólares	x	x	3,00	30%	0,9
Euros	x	x	2,00	30%	0,6
Otros		x			
b) Medio de ingreso y/o pago					
Efectivo	x	x	3,00	20%	0,6
Cheque	x	x	1,50	20%	0,3
Cargo / Abono en cuenta	x	x	0,50	20%	0,1
c) Monto total transado (12 meses)					
Menos de U$ 10.000		x	0,00	50%	0
De U$ 10.000 a U$ 50.000		x	0,00	50%	0
De U$ 50.001 a U$ 100.000		x	0,00	50%	0
De U$ 100,001 a U$ 250.000		x	0,00	50%	0
De U$ 250.001 a U$ 500.000		x	0,00	50%	0
Más de U$ 500.000	x	x	5,00	50%	2,5
TOTAL DEL FACTOR	**30% (5)**				**1,50**

Fuente: Matriz de valoración de riesgos
Elaboración propia

Para el ejemplo, la calificación para el tipo de moneda dólares y euros se le asigna un riesgo medio (3 y 2) con un 30% de ponderación; los valores acreditados en cuenta como efectivo, cheque calificados con riesgo medio (3 y 1,50) y otros cargos con riesgo bajo (0,50) con una ponderación del 20%; y los montos tranzados con calificación de riesgo extremo (5) ya que para el caso es un monto significativo superior a U$ 500.000 con una ponderación del 50%. La suma de la calificación de estos sub-factores representa el 100% de este factor de amenaza.

El tipo de moneda, medios de ingreso y salida, así como los montos transados por el cliente deben estar acorde con su actividad económica y pueden ser analizados en montos acumulados en períodos definidos que puede ser mensual, trimestral, semestral, anual, o en función de las necesidades particulares de cada entidad con base a los

controles definidos. Tanto la información de la moneda, el medio de ingreso y/o pago y los montos transados son datos históricos disponibles en los sistemas internos del banco.

Factor conducta inusual observada

Este factor otorga una valoración basada en la cantidad de alertas sobre operaciones inusuales que salen fuera del perfil del cliente y que son generadas por el sistema de monitoreo sobre un mismo cliente. También se considera las relaciones que pueden existir entre el cliente objeto de análisis y otras personas (naturales o jurídicas) en proceso de revisión, pedidos de información por parte de autoridades judiciales, reportadas a la UAFE o que constan en la lista restrictiva interna de personas investigadas y sancionadas por actividades ilícitas, o clientes con quienes el banco canceló la relación comercial por falta de justificación de transacciones inusuales.

Tabla 16
Sección: Análisis del factor conducta inusual observada

Conducta inusual observada	Sub factor	Valor	Score	Ponderación	Resultado
a) Cantidad de alertas generadas					
De 1 a 3 alertas	x	x	1,00	30%	0,3
Más de 3 y menos de 5 alertas		x	0,00	30%	0
De 5 o más		x	0,00	30%	0
b) Relaciones identificadas					
Con otros reportados	x	x	0,50	30%	0,15
Con otros en listas restrictivas		x	0,50	30%	0
Con otros en proceso de investigación	x	x	3,00	30%	0,9
c) Otras condiciones de riesgo					
Operaciones estructuradas	x	x	1,50	40%	0,6
Señales de alerta identificadas	x	x	3,00	40%	1,2
Pedidos de autoridades judiciales		x	0,00	40%	0
Pedidos de bancos corresponsales		x	0,00	40%	0
TOTAL DEL FACTOR	**30% (3,15)**				**0,95**

Fuente: Matriz de valoración de riesgos
Elaboración propia

El sub-factor de condiciones de riesgo sobre señales de alerta y las operaciones estructuradas se califica con un riesgo medio (3 y 1,50) con una ponderación del 40%; las relaciones identificadas con personas en proceso de investigación se califica con un riesgo medio (3) y las relaciones del cliente con otras personas reportadas y en listas restrictivas se asigna un riesgo medio y bajo (3 y 0,50) sub-factores con una ponderación del 30%; y la cantidad de alertas generadas por el sistema de monitoreo en el rango de 1 a 3 alertas con una calificación baja (1) con una ponderación dentro del factor global de 30%. Muchas veces las alertas se generan por cuanto los clientes no cuentan con un perfil económico o financiero ingresado en el software de monitoreo.

4) Consolidación de resultados de la matriz de valoración de riesgos

El resultado combinado es producto de la convolución (combinación de 2 funciones para obtener una tercera función) tanto de las condiciones de vulnerabilidad y las condiciones de amenaza, que en el presente caso son de 4,20 y 4,39 respectivamente, que representa un riesgo alto y la acción sugerida es informar al oficial de cumplimiento.

Tabla 17
Consolidación de resultados de la matriz de valoración de riesgos

Secciones de la matriz	Ponderación	Resultado
Condiciones de vulnerabilidad		
Productos y servicios	60%	2,40
Canal de atención	40%	1,80
a) Subtotal vulnerabilidad	100%	4,20
Condiciones de amenaza		
Tipo de cliente	15%	0,75
Persona natural	15%	0,69
Zona geográfica	10%	0,50
Transacciones	30%	1,50
Conducta inusual observada	30%	0,95
b) Subtotal amenaza	100%	4,39
RESULTADO COMBINADO (a + b)		**4,20 – 4,39**

Fuente: Matriz de valoración de riesgos
Elaboración propia

5) Interpretación de resultados

Los resultados generados y totalizados en las diferentes secciones de la "matriz de valoración de riesgos en el análisis de operaciones inusuales", se procede a comparar con una tabla de valoración para determinar el nivel de riesgo definido en: bajo, medio, alto y extremo, de acuerdo a la combinación de la "vulnerabilidad y la amenaza" de los diversos factores del riesgo analizados en un caso (sobre un cliente).

Los resultados que se obtenga de la matriz de riesgo sirven de base para la ejecución del monitoreo de transacciones permanente, adoptando las medidas de debida diligencia que corresponda (JBE 2012, 8).

Para el presente caso, el resultado así obtenido se compara con la tabla de calificación de riesgos que se detalla más adelante, de donde se deriva el plan de acción a seguir con base a la calificación de riesgo obtenida. En función de las políticas sobre el nivel de aceptación del riesgo tolerable, cada banco puede definir los procedimientos internos propios sobre las acciones a realizar una vez que se obtiene el resultado de la medición del riesgo.

Tabla 18
Calificación de riesgos

Vulnerabilidad	Amenaza	Resultado	Calificación	Acción
1	1	11	RIESGO BAJO	Finalizar
1	2	12	RIESGO BAJO	Finalizar
1	3	13	RIESGO BAJO	Finalizar
1	4	14	RIESGO MEDIO	Revisar
1	5	15	RIESGO MEDIO	Revisar
2	1	21	RIESGO BAJO	Finalizar
2	2	22	RIESGO MEDIO	Revisar
2	3	23	RIESGO MEDIO	Revisar
2	4	24	RIESGO MEDIO	Revisar
2	5	25	RIESGO MEDIO	Revisar
3	1	31	RIESGO BAJO	Finalizar
3	2	32	RIESGO MEDIO	Revisar
3	3	33	RIESGO MEDIO	Revisar
3	4	34	RIESGO ALTO	Informar al OC
3	5	35	RIESGO ALTO	Informar al OC
4	1	41	RIESGO MEDIO	Revisar
4	2	42	RIESGO MEDIO	Revisar
4	3	43	RIESGO ALTO	Informar al OC
4	4	44	RIESGO ALTO	Informar al OC
4	5	45	RIESGO EXTREMO	Reportar Comité
5	1	51	RIESGO MEDIO	Revisar
5	2	52	RIESGO MEDIO	Revisar
5	3	53	RIESGO ALTO	Informar al OC
5	4	54	RIESGO EXTREMO	Reportar Comité
5	5	55	RIESGO EXTREMO	Reportar Comité

Fuente: Matriz de valoración de riesgos
Elaboración propia

Finalizar *(riesgo bajo)*. Se puede finalizar el análisis puesto que estos casos no demandan trabajo adicional, se puede registrar un comentario en el sistema de monitoreo sobre el motivo del descarte y cualquier observación adicional que el caso amerite y su archivo respectivo.

Revisar *(riesgo medio)*. Se debe profundizar la revisión, con apoyo de la información de los movimientos bancarios del cliente, ya que no se tiene la certeza para justificar y finalizar el caso, sino que amerita revisar el contexto y antecedentes del nivel de riesgo del cliente. Dependiendo del caso se puede requerir al Ejecutivo de Cuenta que en un plazo prudencial solicite la información y justificativos de una o varias transacciones para descartar la alerta y finalizarla.

Informar al oficial de cumplimiento *(riesgo alto)*. Se debe requerir al Ejecutivo de Cuenta que en un plazo prudencial solicite información y justificativos de la(s) transacción(es) al cliente y dependiendo de la razonabilidad de la justificación se puede presentar un informe de operaciones inusuales injustificadas para revisión y aceptación del oficial de cumplimiento.

Reportar a comité de cumplimiento *(riesgo extremo).* Se debe proceder a reportar el caso al Comité de Cumplimiento con el respectivo informe de operaciones inusuales e injustificadas preparado por la Unidad de Cumplimiento, puesto que si se establece un riesgo extremo de LAFD puede poner en un riesgo inminente a la entidad.

El resultado también puede ser apreciado en la matriz de riesgo gráfica, que permite observar el nivel de riesgo en un plano cartesiano donde se visualiza todas las categorías del riesgo global en función de la vulnerabilidad (impacto), la amenaza (probabilidad) y el plan de acción respectivo.

Gráfico 9
Matriz gráfica de riesgo

VULNERABILIDAD						
	5 Muy alta	MEDIO (Revisar) 5	MEDIO (Revisar) 10	ALTO (Informar OC) 15	EXTREMO (Reportar) 20	EXTREMO (Reportar) 25
	4 Alta	MEDIO (Revisar) 4	MEDIO (Revisar) 8	ALTO (Informar OC) 12	ALTO (Informar OC) 16	EXTREMO (Reportar) 20
	3 Media	BAJO (Finalizar) 3	MEDIO (Revisar) 6	MEDIO (Revisar) 9	ALTO (Informar OC) 12	ALTO (Informar OC) 15
	2 Baja	BAJO (Finalizar) 2	MEDIO (Revisar) 4	MEDIO (Revisar) 6	MEDIO (Revisar) 8	MEDIO (Revisar) 10
	1 Muy baja	BAJO (Finalizar) 1	BAJO (Finalizar) 2	BAJO (Finalizar) 3	MEDIO (Revisar) 4	MEDIO (Revisar) 5
		1 Raro	2 Posible	3 Probable	4 Ocasional	5 Inminente
		AMENAZA (PROBABILIDAD)				

Fuente: EALDE Business School, Programa de Gestión de Riesgos
Elaboración propia

En la anterior ilustración se establece dos aspectos a tomar en cuenta en los riesgos identificados; *la probabilidad que puede ser medida con criterios de frecuencia* si se ha materializado, y *el impacto que se pueden entender como las consecuencias*. La evaluación de riesgo se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la ocurrencia del riesgo (Cubillos 2011, 24), conforme fue desarrollada la matriz de valoración de riesgos, donde con base a la convolución de las condiciones de amenaza y probabilidad se obtiene una valoración cuantificable del riesgo (Tabla 18) para los bancos locales.

Riesgo inherente

Por más que se implementen controles, por la naturaleza del negocio bancario, siempre va a existir el riesgo inherente a sus operaciones. Las entidades bancarias

pueden gestionar una mayor o menor cantidad de riesgo, y puede variar con base al riesgo que están dispuestas a aceptar. La valoración del riesgo inherente de los factores de riesgo, se obtiene a través del producto de las variables: impacto (vulnerabilidad) y probabilidad (amenaza) de ocurrencia del evento, durante un periodo determinado.

Riesgo Inherente = Factor Vulnerabilidad x Factor de Amenaza

Como resultado de este producto, para el presente caso se puede establecer la valoración de rangos del riesgo inherente, según el siguiente detalle:

Tabla 19
Rango de riesgo inherente

Rangos	Riesgo	Rangos	Riesgo
20 - 25	Extremo	4 - 10	Medio
12 - 16	Alto	1 - 3	Bajo

Fuente: Matriz gráfica del riesgo
Elaboración propia

Riesgo residual

El riesgo residual hace referencia a aquel que permanece después de haber ejecutado las respuestas o acciones de control a esos riesgos, es decir a pesar de que la entidad ha implementado determinados controles el riesgo subsiste, teniendo en cuenta que siempre va a existir un nivel de riesgo, procurando de que ese nivel sea aceptable, para crear planes de contingencia y planes alternativos (Ealde 2017, 6).

Partiendo del hecho de que el riesgo residual es el resultado del riesgo inherente menos el valor de control, es importante destacar *que la efectividad del control juega un papel preponderante en la prevención* de LAFD. Cuando se realiza un diagnóstico inicial para establecer el riesgo residual, el valor de control original es cero (0) con los controles implementados actuales a una determinada fecha, o en su defecto si no existe control (0) el riesgo inherente es igual al riesgo residual.

Riesgo Inherente (-) Valor del Control = Riesgo Residual

Expectativa { Efectividad del control / Promesa

Control sub-estándar	=	- 1	Falla el control, no funciona
Control original	=	0	Con los controles actuales
Control reforzado	=	+ 1	Aumenta expectativa
Control adicional	=	+ 2	Refuerza expectativa

Para el caso en que el control falla por una acción o ausencia de acción que genera que un control se debilite o anule (condición sub-estándar) el valor del control se reduce lo que provoca que el riesgo residual se incremente.

Para reforzar el valor del control se puede realizar acciones para fortalecer los controles existentes, esta tarea es dinámica y continua, puesto que el análisis, evaluación y tratamiento del riesgo está bajo la administración de la propia organización, así como su diseño e implementación. Si se fortalece el control se refuerza y aumenta la expectativa, pero ésta debe ser efectivizada con el reforzamiento del control para poder disminuir el riesgo residual y se cumpla la condición: "a mayor valor del control menor valor residual", que es el escenario que se espera lograr con un eficiente sistema de administración de riesgos.

6) Riesgo tolerable

En esta fase se realiza la comparación del *nivel real de riesgo* identificado durante el proceso de análisis obtenidos con base a las condiciones de vulnerabilidad y amenaza, con los *criterios de riesgo establecidos* cuando se consideró el contexto total de la naturaleza del riesgo (bajo, medio alto y extremo).

El principio de ALARP (riesgo residual tan bajo como sea razonablemente factible) del autor Des Plainess, se adapta plenamente a la aceptación del riesgo de LAFD y está dividido en tres niveles:

- *Nivel intolerable.* En el cual el "riesgo extremo" es intolerable cualesquiera sean los beneficios que pueda traer la actividad y las medidas de reducción del riesgo son esenciales a cualquier costo. Bajo el enfoque de prevención de LAFD la expectativa es que se reducirá el riesgo, a menos que el costo en reducirlo sea desproporcionado a los beneficios a obtener o por política interna no se acepta la coexistencia de dicho nivel de riesgo. Por el contrario, si se decide convivir con este riesgo, el costo de aplicar controles en este nivel debe evaluarse en función de la rentabilidad que se pueda obtener de un producto o servicio bancario.
- *Nivel tolerable.* Se pueden ubicar al "riesgo alto" y "riesgo medio", en el cual los costos y los beneficios, son aceptados y tomados en cuenta, así como las oportunidades son comparadas y analizadas contra las consecuencias potenciales adversas. En esta banda se encuentran los riesgos (nivel alto y medio) que demandan acciones de mitigación como el monitoreo transaccional con apoyo del software, revisión y análisis continuo de los factores de riesgo, acciones de debida diligencia practicada a clientes, entre otros.
- *Nivel inferior o aceptable.* Se ubica el "riesgo bajo", en el cual los riesgos son inmateriales y no es imprescindible aplicar medidas de tratamiento, cuando los

riesgos están próximos a un nivel inmaterial se debe tomar acciones para reducir el riesgo si los beneficios exceden el costo de reducción, caso contrario se puede coexistir y aceptar este riesgo que es inherente a la actividad bancaria.

Gráfico 10
Manejo del riesgo

Fuente: Principio ASSE org - Gestión de Riesgos del autor Des Plainess
Elaboración propia

Los criterios para decidir si un riesgo necesita ser tratado por lo general se basa en los datos históricos o eventos similares ocurridos en el pasado relacionados a operaciones inusuales identificadas y reportadas, tipologías de operaciones, señales de alerta, montos acumulados, reportes y estructuras de información remitidos al organismo de control, entre otros.

1.7 Tratamiento del riesgo

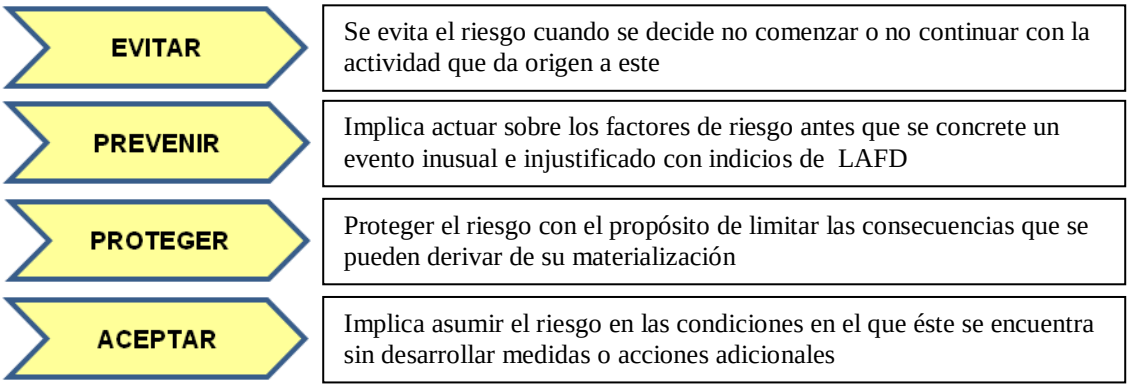
Para tratar el riesgo en la práctica se debe decidir sobre diferentes opciones estratégicas que se pueden aplicar en un sistema de gestión de riesgos, es decir, se puede decidir por evitar el riesgo, por prevenir su ocurrencia, por proteger el riesgo una vez que este se vuelve activo para limitar su capacidad de daño o perjuicio a la entidad, o por aceptar el riesgo en las condiciones en que éste se encuentre (López 2016, 104).

El esquema general para el tratamiento del riesgo, según la normativa local menciona: “Las instituciones del sistema financiero están obligadas a adoptar medidas de control, orientadas a prevenir y mitigar los riesgos que en la realización de sus transacciones, puedan ser utilizadas como instrumento para lavar activos y/o financiar delitos” (JBE 2012, 5). Para esto debe existir un *pre-evento* que origina una causa de error o debilidad sea por un factor humano, tecnológico o material que lo provoque.

Para las *fases de evento y post-evento* la normativa establece: “Implementar metodologías y procedimientos para detectar transacciones económicas inusuales e injustificadas, así como su oportuno y eficiente reporte a la UAF” (JBE 2012, 7), que da lugar a la ocurrencia de un evento donde existe la elaboración de un informe de análisis del pre-evento y un reporte de operaciones inusuales e injustificadas (ROII) remitido a las autoridades y demás acciones complementarias internas como parte del post-evento.

La “*estrategia para la gestión del riesgo”* está en función de formular las estrategias de la entidad bancaria para establecer los controles necesarios sobre la base del grado de exposición y *nivel de aceptación* del riesgo.

Gráfico 11
Alternativas de estrategias de gestión del riesgo



Fuente: Sistemas de gestión de riesgos de LAFD
Elaboración propia

El apetito al riesgo, la tolerancia y los límites son el punto de partida y conforman el primer paso para gestionar los riesgos. Todo comienza por conocer los objetivos estratégicos de la entidad obtenidos en el establecimiento del contexto. Los objetivos de la empresa, sus políticas y sus procedimientos están planteados por la alta dirección, que están recogidos en los manuales elaborados y van a condicionar el apetito de riesgo de la organización (Ealde 2017, 5).

a) Evitar

La estrategia de evitar se utiliza básicamente cuando se tratan de riesgos inaceptables o inadmisibles (riesgo extremo), que su ocurrencia va a tener un impacto negativo en el banco. Desde el punto de vista de LAFD existen variados riesgos de este tipo mencionados en las regulaciones para evitar su ocurrencia, tales como:

- Las instituciones del sistema financiero deben contar con un manual de prevención del lavado de activos y financiamiento de delitos, que establezca

políticas, procesos y procedimientos que deben ser aplicados para *evitar* que se las utilice para lavar activos o financiar delitos (JBE 2012, 9).

- Las instituciones deben evitar establecer relaciones comerciales con sociedades o empresas comerciales constituidas al amparo de legislaciones extranjeras que permitan o favorezcan el anonimato de los accionistas o administradores, incluyendo en esta categoría a sociedades anónimas cuyas acciones sean emitidas al portador; o, que dichas legislaciones impidan la entrega de información (JBE 2012, 10).
- Toda institución del sistema financiero una vez aplicada la política "Conozca a su cliente" deberá categorizar y ponderar el riesgo de cada uno de ellos. Esto permitirá en algunos casos tomar decisiones de *no vinculación* o de someterlos a una debida diligencia ampliada (JBE 2012, 11).

El incumplimiento de las acciones preventivas y la consecuente materialización del riesgo como se mencionó anteriormente pueden dar lugar a sanciones por parte de la Superintendencia de Bancos, que pueden llegar hasta la suspensión temporal o definitiva del permiso de operación de la institución bancaria.

b) Prevenir

La prevención implica actuar y gestionar los factores de riesgo antes que se materialice un caso o evento relacionado con la ejecución de operaciones inusuales e injustificadas a fin de disminuir su probabilidad de ocurrencia, transferir o desplazar la amenaza. Para que exista indicios de LAFD, debe existir la condición concomitante de "inusual e injustificada", puesto que no toda operación inusual puede ser calificada como injustificada sin un previo análisis, por lo que parte de la labor de la Unidad de Cumplimiento con apoyo del área comercial es la de descartar transacciones inusuales; si una vez realizado el proceso de acercamiento con el cliente no es factible descartar la alerta, la operación en cuestión se convierte además en injustificada.

La amenaza desplazada no desaparece, sino busca a otras entidades bancarias, financieras o de la economía popular y solidaria (cooperativas de ahorro y crédito, cajas de ahorro) con controles menos exigentes que faciliten la colocación de recursos producto de actividades ilícitas, e inclusive las organizaciones delictivas buscan otros sectores afines como el inmobiliario, construcción, comercio de arte, explotación de minería, entre otros, para tales fines de ocultamiento de los activos ilícitos, conformándose un círculo vicioso y de alto riesgo, ya que estos actores descritos son también clientes de los propios bancos.

Dentro de la estrategia de prevención del riesgo que menciona la normativa local, juega un rol fundamental la Unidad de Cumplimiento, puesto que es la encargada de prevenir y proteger a la entidad del LAFD, además la norma hace énfasis en:

- Las medidas de *prevención* deben cubrir toda clase de servicios o productos financieros, sin importar que se realicen en efectivo o no, así como a toda clase de clientes permanentes u ocasionales, accionistas, directivos, funcionarios, empleados, proveedores y usuarios de la institución del sistema financiero (JBE 2012, 5).
- Las políticas que adopten las instituciones del sistema financiero y que deben constar en el "código de ética", deben permitir la adecuada aplicación de medidas para *prevenir* de lavado de activos y el financiamiento de delitos y traducirse en reglas de conducta y procedimientos que orienten la actuación de los accionistas, miembros del directorio u organismo que haga sus veces, administradores, funcionarios y empleados (JBE 2012, 6).

Controles de mitigación

Los tipos de control que se aplican para la mitigación de riesgos pueden ser manuales, automáticos y semiautomáticos, generalmente son los controles de tipo preventivo, detectivo y correctivo. Para administrar y mitigar los riesgos, los procesos y productos ofrecidos por el banco deben estar respaldados por procedimientos en los que se describen los controles de prevención de cada uno de ellos, que pueden estar contenidos y documentados en el manual de prevención de LAFD, código de ética, autorizaciones y aprobaciones por niveles superiores, visitas in situ a clientes, debida diligencia ampliada para clientes con riesgo alto y extremo, informes sobre suficiencia de controles de PLFD en la salida de productos nuevos, análisis de registros de información, conocimiento del mercado y su segmentación, programa de cumplimiento, condiciones contractuales, formularios de control, capacitaciones para comprender la exposición del banco, tipologías o señales de alerta en transacciones, entre otros.

c) Proteger

Se actúa protegiendo el riesgo cuando se responde después de ocurrido un evento, con la finalidad de limitar las consecuencias negativas que se puedan derivar de su ocurrencia. La protección se activa cuando la prevención falla o no resulta suficiente como barrera de prevención del riesgo del sistema o subsistema vulnerado.

La acción más eficaz es el reporte de operaciones inusuales e injustificadas (ROII) a la UAFE, puesto que este reporte a la autoridad con carácter confidencial y

reservado cubre la responsabilidad del banco de actuar con diligencia y oportunidad de acuerdo a la normativa establecida, la misma que hace énfasis en:

- Las instituciones del sistema financiero están obligadas a adoptar medidas de control, orientadas a prevenir y mitigar los riesgos que en la realización de sus transacciones, puedan ser utilizadas como instrumento para lavar activos y/o financiar delitos (JBE 2012, 5).
- Implementar metodologías y procedimientos para detectar transacciones económicas inusuales e injustificadas, así como su oportuno y eficiente reporte a la Unidad de Análisis Financiero (JBE 2012, 7). Es en este punto, el presente sistema de administración del riego basado en la norma ISO 31000 es el que aporta con una metodología eficiente e innovadora para la gestión del riesgo.
- Los procedimientos para el oportuno reporte interno y externo de transacciones con montos sobre los umbrales y con transacciones inusuales e injustificadas (JBE 2012, 9). Esta acción de control se refiere a los procedimientos para elaborar los reportes de información mensual que los bancos deben remitir sobre transacciones que individual o acumuladas de clientes superen los US $ 10.000; y además hace referencia al reporte de operaciones inusuales e injustificadas.

d) Aceptar

Al asumir un riesgo se debe definir y parametrizar en el sistema de monitoreo umbrales en donde la probabilidad de ocurrencia de un evento de LAFD es mínima, o la cuantía comprometida de una pérdida es inmaterial. La decisión de asumir un nivel de riesgo se fundamenta en la necesidad de emplear los recursos disponibles para aquellas actividades de control preventivo relacionadas a casos de alertas de transacciones con valoración de riesgos medio, alto y extremo, sujetas a una mayor probabilidad de ocurrencia de un evento de riesgo (López 2016, 107).

Desde el punto de vista de la administración de riesgo, la normativa establece por ejemplo que para *aceptar un riesgo*, se debe tomar en cuenta que:

- La singularización del funcionario que tiene como responsabilidad excepcionar a los clientes de la obligación de suscribir el formulario de licitud de fondos (JBE 2012, 10). Por la dinámica y volumen de transacciones la norma establece que las instituciones financieras exigirán a sus clientes llenar el formulario de licitud de fondos en los depósitos individuales que igualen o superen los US $ 5.000 en efectivo; en tal sentido, esta excepción del formulario representa una *aceptación*

implícita del riesgo de omitir el control que representa contar con la información otorgada por el cliente sobre el origen y destino de los fondos de la transacción.

- Designar las instancias autorizadas para exceptuar clientes del diligenciamiento del formulario de licitud de fondos (JBE 2012, 22). Al constituir la aceptación de un riesgo una alta responsabilidad, la entidad debe designar un funcionario de jerarquía que apruebe tal excepción, que usualmente es el oficial de cumplimento en coordinación y por solicitud del Ejecutivo de Cuenta, quien conoce razonablemente la actividad económica del cliente, su entorno y su fuente de ingresos. Por lo general esta excepción aplica a clientes conocidos que por la naturaleza de su negocio manejan grandes cantidades de efectivo (gasolineras, supermercados, establecimientos educativos, tiendas de retail, entre otros) y que han sido objeto de un proceso previo de debida diligencia avanzada que se encuentra documentado en el file del cliente.

En función de la matriz gráfica del riesgo (Gráfico 9), el tratamiento del riesgo obtenido con base a la combinación de las Condiciones de Vulnerabilidad y Amenaza, debe estar enfocado en: “Evitar o reducir el Riesgo Extremo”; “Reducir, prevenir y proteger el Riesgo Alto y Riesgo Medio”; y “Aceptar el Riesgo Bajo”.

1.8 Monitorear y revisar

Los procesos de gestión de riesgos deben ser incorporados a los procesos organizacionales y además al plan estratégico de la entidad para ser monitoreados, dado que la gestión de riesgos es dinámica y debe adaptarse a los cambios de la entidad ya sea por el lanzamiento de un nuevo producto, la apertura de un canal de servicio o de una agencia en una nueva zona geográfica, todos estos nuevos cambios del negocio deben ser notificados al oficial de cumplimiento desde el inicio de su desarrollo para asegurar un acompañamiento oportuno del enfoque de gestión del riesgo.

En la práctica, el monitoreo y revisión del sistema de administración de riesgos puede ser ejecutado con el apoyo de indicadores de gestión y umbrales de control, tarea que es realizada por las Áreas de Riesgos, Unidad de Cumplimiento, Operaciones, Auditoría interna o externa. Para este efecto los indicadores deben ser medibles, tener una definición, un alcance, y un responsable a cargo de esta medición periódica.

Con la finalidad de evaluar el desempeño de la implementación del sistema de administración de riesgos de LAFD con base a la norma ISO 31000 y realizar el

monitoreo de los resultados de los procedimientos y actividades que optimizan al proceso de administración del riesgo, se va a proceder a desarrollar la documentación de los indicadores de gestión y evaluación propuestos y definidos para este efecto. .

1) Indicador de reporte de operaciones inusuales injustificadas a la UAFE

Este indicador muestra la eficacia del monitoreo reflejada a través del número de casos de operaciones inusuales e injustificadas de clientes remitidas a la UAFE a través del ROII, a la vez que ayuda a establecer la efectividad de la gestión del Ejecutivo de Cuenta para gestionar el descarte y justificación de las alertas de inusualidades de las transacciones de la cartera de sus clientes.

Este indicador debe ser analizado de una manera objetiva, puesto que pueden darse discrepancias con los organismos reguladores cuando ejerzan su facultad de revisión; ya que el hecho de contar con un software de monitoreo per se no garantiza una cantidad determinada de reportes de operaciones sospechosas, sino que está en función de la parametrización del sistema con base a la evaluación del riesgo (Anexo 4).

2) Indicador de requerimientos de corresponsales locales y del exterior

Estas alertas recibidas por parte de los bancos corresponsales, sirven de insumo e información histórica para la evaluación de riesgos dentro del factor producto (transferencias del y al exterior) y el factor de transacciones (pedidos de bancos corresponsales), que ayudan a incluir estas variables en la ponderación del riesgo.

Los servicios que implican la intervención de estas cuentas corresponsales del banco titular local para atender y brindar servicio a sus clientes ya sea por operaciones de comercio exterior, tesorería, transferencias enviadas y recibidas desde y al exterior, son objeto de procesos de debida diligencia por parte de los bancos del exterior para conocer el origen y destino de fondos de las transacciones que se ejecutan con su intermediación en la cadena de procesamiento de dichas operaciones (Anexo 5).

3) Indicador de atención de pedidos de información

Los organismos de control y autoridades judiciales dentro de su alcance y ámbito de acción solicitan continuamente información a los bancos sobre los movimientos transaccionales de personas que se encuentran en procesos de investigación.

Estos pedidos de información solicitados por las autoridades constituyen un insumo de información de la etapa de evaluación dentro del factor de riesgo conducta inusual observada (pedidos de autoridades judiciales), sobre todo si la Unidad de Cumplimiento o el área encargada de la atención de estos requerimientos mantiene un

registro histórico de los pedidos de información de clientes por parte de las autoridades o en su defecto pueden ser ingresados e identificados en una lista interna de control y seguimiento o proceder a la cancelación comercial con dichos clientes, con base a las políticas internas definidas (Anexo 6).

4) Indicador de gestión de control de listas restrictivas

La administración de la gestión operativa de las listas restrictivas corresponde a la Unidad de Cumplimiento, esta tarea es continua y la lista restrictiva debe estar conectada en línea a todos los aplicativos operativos que procesan transacciones para clientes con apoyo del software de control definido para el efecto (Anexo 7).

Conclusiones y recomendaciones

1. Conclusiones

- El objetivo general de la presente investigación respecto a mejorar el sistema de administración y gestión de riesgo de prevención LAFD de los bancos privados del país, se cumple de forma parcial, puesto que una de las principales limitaciones es que el modelo integral de la norma ISO 31000:2009 no ha sido desarrollado e implantado en todo su alcance y contexto por los bancos. Gran parte del enfoque de esta norma internacional, de forma empírica se está aplicando en los actuales sistemas de gestión de riesgos –básicamente el proceso de gestión de riesgo– de los bancos privados locales y del exterior, producto de lo cual la labor de monitoreo muestra una mejora sustancial sobre la calidad de las alertas de operaciones inusuales bajo un enfoque de administración de riesgo integral.
- Respecto a los objetivos específicos, los resultados cuantitativos obtenidos del estado actual de la suficiencia y eficacia del sistema de administración de riesgos de los bancos privados, ratifican los puntos divergentes que existe con los resultados de las revisiones in situ del regulador sobre varios puntos de mejora de dicho sistema, que justamente pueden ser optimizados mediante el enfoque integral que incluya el análisis de las variables cualitativas y cuantitativas de los factores de riesgo que se refleje en una labor de monitoreo más eficiente con base a la implementación de la norma ISO 31000:2009, cuyos resultados obtenidos en las entidades bancarias donde se aplica la norma son el incremento de alertas a gestionar y mayor reportes de inusualidades al organismo de control.
- Los resultados en aquellos bancos que están utilizando el enfoque de la norma ISO 31000:2009 son positivos, puesto que han optimizado sus recursos con la gestión y análisis de alertas o excepciones de mayor calidad y certeza de operaciones inusuales que salen fuera del perfil transaccional de los clientes. La aplicación del proceso de gestión de riesgo que establece esta norma per se, no garantiza el mejoramiento del actual sistema de gestión, sino la manera de identificar, evaluar y tratar los riesgos con base al modelo integral y esquema de trabajo que propone la norma, esto es los principios, el marco de trabajo y el

proceso de gestión del riesgo, todos se interrelacionan y retroalimentan entre sí. Los resultados que se esperan obtener con la aplicación de la norma ISO 31000:2018 toda vez que los principios de gestión buscan crear valor para la organización y van a ser apoyada por la alta dirección se proyectan ser muy alentadores y más efectivos en la labor de administración de estos riesgos.

- No se gana dinero con la gestión del riesgo, sino que se evita perderlo. Es más las pérdidas que puede suponer una sanción por multa, cierre temporal o cancelación de la licencia de operación por un tema de LAFD, un ciberataque o una actuación de mala fe desde dentro de una empresa pueden ser determinantes para la continuidad del negocio. Con esta norma se pretende tratar y minimizar el riesgo reputacional de una entidad, los beneficios intangibles está en la creación de valor para la organización y hasta alinearse a la responsabilidad social empresarial para abordar los riesgos sociales y ambientales dentro del modelo.
- A nivel mundial las investigaciones relativas a la integración de sistemas de gestión de riesgo de esta norma han sido significativa en número y han cubierto diferentes sectores y actividades susceptibles a la exposición al riesgo, estas se han llevado a cabo principalmente en los países europeos. Al revisar estudios e investigaciones sobre el tema en Latinoamérica el número se reduce y al limitarlo puntualmente a la aplicación en sistemas de prevención de LAFT en la región y el Ecuador el número de referencias es muy escaso, estando enfocadas únicamente a propuestas de diseño de sistemas integrados en estudio de caso particulares no relacionados a sistemas de prevención de LAFD.
- En la actualidad los bancos privados del país cumplen con el sistema de administración de riesgos de LAFD, que lo gestionan a través del programa de cumplimiento que contempla la identificación, medición, evaluación, control y monitoreo de estos riesgos; sin embargo, en la práctica la Superintendencia de Bancos en su proceso de revisión del periodo 2014 identificó debilidades materiales en dicho programa por la *falta de un enfoque integral* para una adecuada identificación y evaluación del riesgo, que considere las variables cuantitativas y cualitativas de los diferentes factores de riesgo. Por lo que la presente propuesta basada en la norma ISO 31000 está dirigida a solventar las observaciones del organismo supervisor derivadas de esta deficiencia, para obtener un sistema de gestión con un enfoque integral del riesgo.

- Un aspecto fundamental para el éxito del presente sistema de administración de riesgo propuesto, es el verdadero compromiso de la alta gerencia para apoyar la eficaz y eficiente ejecución del proyecto de fortalecimiento del actual sistema de administración de riesgos con el enfoque de la norma ISO 31000, ya que la falta de apoyo o desinterés puede debilitar el fortalecimiento del programa de cumplimiento y no llegar a satisfacer los requerimientos y expectativas del ente de supervisión en sus próximas revisiones.
- La gestión de riesgos con base a la norma ISO 31000 persigue la disminución de las probabilidades de los impactos negativos referentes a la ocurrencia directa o indirecta de eventos de lavado de activos y al contrario busca generar más negocios seguros para los bancos mediante el incremento de operaciones con sujeción al cumplimiento de la normativa para obtener mayores márgenes de rentabilidad para los accionistas.
- Los aspectos teóricos y conceptuales desarrollados en la presente investigación representan guías de carácter referencial para el soporte y fuente de consulta para las instituciones financieras y demás sujetos obligados, ya que el mismo riesgo podría parecer insignificante para una entidad y muy alto para otra, en función de sus percepciones y aceptación del riesgo de LAFD, en consecuencia los criterios deben representar una visión objetiva, tomando en cuenta las necesidades e intereses reales y particulares de cada institución.

2. Recomendaciones

Producto de la evaluación de la situación actual del modelo de gestión de riesgos de los bancos privados y la propuesta de implementación del nuevo modelo de gestión con base a la norma ISO 31000, se recomienda:

- Los criterios y valores de las diferentes matrices de riesgo desarrolladas en la presente investigación, están expresadas de manera didáctica para la comprensión visual de los lectores; sin embargo, en la práctica estos diversos criterios de valoración y ponderación de los riesgos, deben ser entendidos, automatizados e incorporados en el software de monitoreo. La clave está en la comprensión y evaluación de los factores de riesgo con un enfoque integral, para poder bajar dicho criterio experto al sistema de monitoreo de alertas de operaciones que salen fuera del perfil demográfico y transaccional de los clientes.

- La presente investigación pretende servir de guía para el establecimiento de los procedimientos básicos de control que una entidad bancaria deberá implementar para el desarrollo de sus actividades en el marco del ordenamiento legal y sentar las bases para la elaboración de mapas de riesgo que permitan evaluar los riesgos potenciales por tipo de factores (cualitativos y cuantitativos) con el fin de mantener la competitividad en el mercado.
- Se deben analizar los efectos devastadores efectos del de-risking en la inclusión financiera del sector bancario local, regional y mundial; los supervisores deben estar conscientes de los impactos de este fenómeno en la estabilidad financiera transnacional, si el sector financiero formal no se encuentra en capacidad de ofrecer los servicios de corresponsalía que demandan diversos sectores económicos, ello podría generar demanda de los mismos a través de canales informales o no regulados. De esta forma se estaría acentuando la problemática de prevención de LAFD que precisamente se busca solucionar a nivel internacional.
- La tendencia creciente de la materialización de estos riesgos a nivel mundial, ha obligado que ciertas entidades del exterior –principalmente bancos– aparte de requerir periódicamente información documentaria sobre la aplicación de controles de lavado de activos a los bancos extranjeros que mantienen cuentas de corresponsalía en su institución sustentados en un convenio, inclusive pueden ser objeto de visitas in situ locales para corroborar y verificar dichos controles. Por lo que los bancos nacionales deben disponer de todos los documentos, procedimientos y sistemas de gestión para demostrar y sustentar las acciones de control preventivo en esta materia.
- El gran desafío del sector bancario es pasar de la banca tradicional a la digital, en consecuencia, los esfuerzos a ejecutarse en el futuro tienen que ir dirigidos en ese sentido. El avance de la revolución digital es un hecho económico y cultural que no tiene reversa y el sector bancario tiene la oportunidad de abrir nuevos mercados, ampliar la inclusión financiera y reducir costos, siempre y cuando realice una adecuada administración de la gestión de riesgo, en especial identificar y mitigar los riesgos del lavado de activos y financiamiento de delitos.

Obras citadas

Alba, Ricardo. *Programa y Manual Uniforme para la Prevención de Lavado de Activos en América Latina*, Panamá: Agrica Lex Corp., Inc., 2003, 21.

------, *Programa y Manual Uniforme para la Prevención de Lavado de Activos en América Latina*, Panamá: Agrica Lex Corp., Inc., 2003, 172.

Albanese, Diana. "*Análisis y evaluación de riesgos: aplicación de una matriz de riesgos en el plan de prevención contra el lavado de activos*". Revista de Administración y Contabilidad de Universidad Nacional del Sur, Argentina, Departamento de Ciencias de la Administración. 2012, vol. 9, No. 3. http://repositoriodigital.uns.edu.ar/bitstream/123456789/4099/3/An%C3%A1lisis%20y%20Evaluaci%C3%B3n%20de%20riesgos.pdf

Banco Central de la República Dominicana (BCRD). "Evaluación cierre del plan estratégico institucional 2014-2017". Informe ejecutivo. 15 de octubre del 2018 https://gdc.bancentral.gov.do/Common/public/transparencia/documents/Informe_Cierre_PEI_2014-2017.pdf

------, (BCRD) "*Informe del cierre del Plan Estratégico Institucional 2014-2017*", Departamento de Planificación y Presupuesto, enero 2018. https://gdc.bancentral.gov.do/Common/public/transparencia/documents/informe_evaluacion_plan_estrategico_2014-2017_diciembre17.pdf

Banco Pichincha (BP).*"Oficiales de Cumplimiento se reúnen para compartir buenas prácticas de control*". Revista Impacto, No, 21 publicada por Banco Pichincha, Quito, 2013.

Bank for International Settlements (BIS). "*Reformas de Basilea III*" Comité de Supervisión Bancaria de Basilea, 2010. https://www.bis.org/bcbs/basel3/b3_bank_sup_reforms_es.pdf

Barba, Antonio. "*Cambio organizacional y cambio en los paradigmas de la administración"*. Iztapalapa 48, México. 2000. http://148.206.53.234/revistasuam/iztapalapa/include/getdoc.php?id=648&article=659&mode=pdf

Béjar Ramón. "*La importancia de implementar un Plan de Continuidad de Negocios*". Colegio de Contadores Públicos de México A. C. 1 de julio de 2013. https://www.dineroenimagen.com/2013-07-01/22403

Belacha et al, "*Gestión del riesgo crediticio y su efecto en la morosidad en una entidad bancaria en la ciudad de Trujillo*" Gerencia de Riesgos, 2014. https://es.slideshare.net/kathytenorio/trabajo-final-iso-31000-scotiabank-gerencia-de-riesgos

Bolaños, Martha. "*Diseño de un modelo de gestión de riesgo de crédito para el sistema mutual ecuatoriano basado en ISO 31000*". 2016. **URI:** http://repositorio.puce.edu.ec/handle/22000/10746

Bueno, Gastón et al. "*Administración de riesgos – una visión global y moderna*". Universidad de la República. Uruguay. 2010. https://www.colibri.udelar.edu.uy/jspui/bitstream/123456789/201/1/M-CD4026.pdf

Castro, Mauricio. "El Nuevo Estándar ISO para la Gestión de Riesgos*". Surlatina Consultores.* Accedido 22 de noviembre del 2017. https://capacitacion.gestionderiesgos.gob.ec/courses/40/files/3782/download

Centro de Estudios Sociales y de Opinión Pública. "*Lavado de dinero: indicadores y acciones de gobierno binacionales"*. Carpeta de indicadores y tendencias sociales, No. 17, México, marzo de 2012, 16. http://www3.diputados.gob.mx/camara/content/download/274232/852053/file/Carpeta-17-lavado-de-dinero.pdf.

Chiavenato, Idalberto. Introducción a la Teoría General de la Administración. Séptima edición. McGraw-Hill Interamericana 2004.

Cubillos, Myrian et al. 2011. *Guía para la Administración de Riesgo*, cuarta edición, Bogotá DC, p. 25.

Cuello; Roberto et al. 2008. "*Aplicación el estándar australiano de Administración de Riesgos AS/NZS 4360:1999"*. Pensamiento & Gestión No. 25, Colombia, edición digital. Julio / Diciembre 2008. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-62762008000200006

Deming, William. *Calidad, Productividad y Competitividad. La salida de la crisis*. Ediciones Díaz de Santos S. A. Madrid, España. 1986.

De Juan, Aristóbulo. "*Basilea II en los sistemas financieros frágiles*" Revista de temas financieros. 2005. http://www.sbs.gob.pe/Portals/0/jer/EDIPUB_VOLUMEN2/3DE%20JUAN.pdf

De Sena, Alcina. *¿Auditoría más efectiva después de COSO ERM 2017 o de ISO 31000:2009?".* Revista Perspectiva Empresarial ISNN: 2389-8194. Septiembre de 2017 file:///C:/Users/PC/Downloads/134-444-1-PB.pdf

Ealde, Business School. *Gestión de Riesgo y Control del Riesgo*. Accedido 5 de noviembre del 2017, 6. https://es.scribd.com/document/343222999/White-Paper-Gestion-de-Riesgos-y-Control-Interno-0916

EC. *Código Orgánico Integral Penal*. Registro Oficial 180, 10 de febrero del 2014. Delitos económicos, 22-4.

------, *Código Orgánico Integral Penal*. Registro Oficial 180, 10 de febrero del 2014. Delitos contra la humanidad, 55-9.

------, *Código Orgánico Integral Penal*. Registro Oficial 180, 10 de febrero del 2014. Delitos contra el derecho a la salud, 91-2.

EC.2014. *Código Orgánico Monetario y Financiero.* Registro Oficial 332, 12 de septiembre del 2014, De las entidades, 5. Art. 6.

------. *Código Orgánico Monetario y Financiero.* Registro Oficial 332, 12 de septiembre del 2014, Del Banco Central del Ecuador, 11. Art. 36.

EC.2016. *Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y Financiamiento de Delitos*. Registro Oficial 802, 21 de julio del 2016, arts. 317-320.

Ecuador JBE, *Resolución No. JB-2012-2146, Glosario de términos*, Registro Oficial 709, 23 de mayo de 2012, 3.

------, JBE, *Resolución No. JB-2012-2146, De las Políticas y Procedimientos de Control*, Registro Oficial 709, 23 de mayo de 2012, p. 5-8.

------, JBE, *Resolución No. JB-2012-2146, Del Manual de Prevención de Lavado de Activos y Financiamiento de Delitos*, Registro Oficial 709, 23 de mayo de 2012, p. 9.

------, JBE, *Resolución No. JB-2012-2146, De la Debida Diligencia y sus Procedimientos*. Registro Oficial 709, 23 de mayo de 2012, págs.10, 11, 17.

------, JBE, *Resolución No. JB-2012-2146, De la Estructura Organizacional*, Registro Oficial 709, 23 de mayo de 2012, p. 22, 28.

Ecuador Junta de Política y Regulación Monetaria y Financiera. *Resolución No. 380-2017-F Política para la Gestión Integral y Administración de Riesgos de las Entidades de los Sectores Financieros Público y Privado,* Registro Oficial 22, Suplemento, 26 de junio de 2017, 2-4.

Encalada, Ingrid. "*Propuesta de un sistema de gestión de riesgo para la compañías del sector de seguros en el Ecuador*". Universidad del Azuay, 2018. http://dspace.uazuay.edu.ec/bitstream/datos/7669/1/13498.pdf

Escorial, Ángel. "Nuevo marco de gestión de riesgos para las organizaciones" ISO 31000, Asociación Española de Normalización (AENOR). 2012. https://portal.aenormas.aenor.com/revista/pdf/ene18/38ene18.pdf

Espinosa, David. "Teoría general de sistemas de Ludwing von Bertalanffy" 2009. https://www.gestiopolis.com/teoria-general-de-sistemas-ludwig-von-bertalanffy/

Fayol, Henry. Administration industrielle et générale. París, Francia 1916.

Federación Latinoamericana de Bancos (FELABAN), *"Acuerdos de supervisión bancaria a la luz de los acuerdos de Basilea"* Convención bancaria, 2018. https://www.felaban.net/archivos_noticias/Noticia-2018-08-24.pdf

FFIEC. Federal Financial Institutions Examination Council. *Manual de Inspección Antilavado de Dinero / Ley de Secreto Bancario BSA/AML*, 2007, 152-4.

FLACSO. Facultad Latinoamericana de Ciencias Sociales. "Las cifras del Lavado de Activos", Perfil criminológico No. 14, junio del 2015, 15. https://www.fiscalia.gob.ec/images/perfil/criminologico14.pdf

GAFILAT. Grupo de Acción Financiera de Latinoamérica. *Recopilación de tipologías regionales de GAFILAT 2009-2016*, Buenos Aires, Argentina, 2016, 11-186.

------. Grupo de Acción Financiera de Latinoamérica. *Estándares Internacionales sobre la lucha contra el Lavado de Activos y el Financiamiento del Terrorismo y de la Proliferación*, Las recomendaciones del GAFI, OCDE, 2015, 4-5. www.uiaf.gov.co/index.php?idcategoria=28433

GAFISUD. Grupo de Acción Financiera de Sudamérica. *Notas interpretativas y mejores prácticas de las 9 recomendaciones especiales contra el financiamiento del terrorismo*. CADECAC, Buenos Aires, Argentina, 2012.

Galdo, María. "Multicanalidad y digitalización bancaria, innovación y tendencias", Universidad Pontificia. ICADE Business Scholl, Madrid 2015. https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/6338/TFM000186.pdf?sequence=1&isAllowed=y

González, Hugo. "Gestión del riesgo – ISO 31000", Calidad & Gestión, Buenos Aires, Argentina, 28 de octubre del 2016. https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/.

Hernández, Abigail. Escuela estructuralista. 2009. https://www.monografias.com/trabajos69/escuela-estructuralista-max-weber/escuela-estructuralista-max-weber2.shtml

Idrovo, Efraín. "*Disminución del riesgo operativo en las compañías de seguros mediante la implementación de ISO 31000*", Universidad de Guayaquil, 2015. http://repositorio.ug.edu.ec/bitstream/redug/9596/1/Tesis%20Efra%C3%ADn%20Idrovo%20oficial%2007-01-2016.pdf

ISO. International Organization for Standarization, Norma Internacional ISO 31000 versión 2009 Gestión de Riesgos Principios y Guías, Primera Edición, Noviembre 15, 2009.

ISOTools. "Principales cambios de la norma ISO 31000:2018 de Gestión de Riesgos". Plataforma tecnológica para la gestión de la excelencia, 6 de junio del 2018. https://www.isotools.org/2018/06/06/principales-cambios-norma-iso-310002018-gestion-riesgos/

------; "Gestión de Riesgos: Cómo ha cambiado el nuevo COSO ERM 2017?". Plataforma tecnológica para la gestión de la excelencia, 7 de febrero del 2018. https://www.isotools.org/2018/02/07/ha-cambiado-nuevo-coso-erm-2017

Lara, Antonio. *Lavado de dinero, paraísos fiscales y transacciones dudosas*, Primera edición, West Houston Reprographics, Inc., Houston Texas, 2002, 29-32.

López, Orlando. "Sistema de Gestión de Riesgo 2016, Norma Técnica Internacional ISO 31000:2009". Ponencia en el Programa de Capacitación en Sistemas de Gestión de Riesgos de Lavado de Activos, Quito, 27 de febrero del 2016.

------, 2006. Marco Conceptual y Metodológico de la Gestión de Riesgo del Lavado de Activos y Financiamiento del Terrorismo.

Maslow, Abraham. Motivation and Personality. Harper Taw Publisher. 1954.

Meyers, Fred. Estudios de tiempos y movimientos para la manufactura. Prentice Hall, Segunda edición, México, 2000. https://es.scribd.com/document/310518841/Estudio-de-Tiempos-y-Movimientos-Para-La-Manufactura-Agil-Meyers

Morales, Jessica. Evolución de la administración y el pensamiento administrativo. 2015. https://www.gestiopolis.com/evolucion-de-la-administracion-y-el-pensamiento-administrativo/

Morillo et al, "*Viabilidad y efectos de la aplicación del estándar australiano como sistema de administración del riesgo de lavado de activos y financiamiento del terrorismo-SARLAFT en el sector cooperativo ecuatoriano*", Revista Publicando indexada a Latindex. Quito. 2017. https://www.rmlconsultores.com/revista/index.php/crv/article/view/484

Münch, Lourdes. Administración: *Gestión Organizacional, enfoques y proceso administrativo*. Pearson Educación. ISBN 978-607-442-389-1. México. 2010. https://issuu.com/jassiorojo01/docs/administracion_gestion_organizacion

Padilla, Avigail et al. "*Diseño de un sistema de gestión y administración del riesgo de lavado de activos basado en la ISO 31000 para la Cooperativa de Ahorro y Crédito Riobamba Ltda., de la ciudad de Riobamba, provincia de Chimborazo*". Escuela Superior Politécnica del Chimborazo, 2016. http://dspace.espoch.edu.ec/bitstream/123456789/5817/1/82T00574.pdf

Quezada, Gilberto. "Administración de riesgos empresariales: definición y proceso" GestioPolis, 2010. https://www.gestiopolis.com/administracion-de-riesgos-empresariales-definicion-y-proceso/

Ramírez; Alexandra et al. "*Gestión de riesgos tecnológicos basados en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocio*". Sistema de información científica Redalyc, Universidad Autónoma del Estado de México (UAEM). 2011. http://www.redalyc.org/html/4988/498850173005/

Rendón, Lina. School of Human Relations. Universidad Nacional de Colombia. 2011. http://bdigital.unal.edu.co/3838/1/linamariarendongiraldo.2011.pdf

Rojas, Jairo. *"Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del Ecuador"* Universidad de Las Américas, Facultad de Posgrados, Quito, 2017.

SBE. "Normas Generales para la Instituciones del Sistema Financiero". *Superintendencia de Bancos del Ecuador*. 11 abril del 2013. 819. http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_XIII_cap_IV.pdf

------, "*Metodología de Gestión de Riesgos de Seguridad de la Información*", Resolución No. SB-CGPyCG-2017-016, 11 de octubre de 2017.

http://oidprd.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2017/Otras_resoluciones/resolucion_SB-CGPyCG-2017-016.pdf

------, "Política General de Seguridad de la Información". *Superintendencia de Bancos del Ecuador*. 4 abril del 2018. https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2018/05/resol_SB-CGPMC-2018-004.pdf

Stuart, Gulliver. "HCBS Multa récord en caso de lavado de dinero, Perú". *Gestión, Economía y Negocios.* 11 de diciembre de 2012 http://gestion.pe/empresas/hsbc-pagara-multa-record-us-1900-millones-caso-lavado-dinero-2053942.

Torres, María. "El rol del Organismo de Control de las instituciones del sistema financiero". Superintendencia de Bancos del Ecuador. Ponencia presentada en el Segundo Congreso Internacional de Prevención de Lavado de Activos – CIRPLA, Quito, 4 de junio del 2014.

UAFE. "Infórmate y evita involucrarte en el lavado de activos y en el financiamiento de delitos". *Unidad de Análisis Financiero y Económico*. 21 de octubre del 2017. http://www.uafe.gob.ec/index.php/informate-sobre-el-lavado-de-activos.

------, "Tipología basadas en información conocida por la UAF". *Unidad de Análisis Financiero y Económico*. Accedido 21 de octubre del 2017. http://www.uafe.gob.ec/index.php/tipologias-y-senales-de-alerta-sobre-el-lavado-de-activos-en-el-ecuador

USDT. "The 2001National Money Laundering Strategy". U.S. *Department of Treasury*, september 2001, http://www.treasury.gov/offices/enforcement/ml2001.pdf

Vaca, Denisse. "*Diseño de formatos para implementar un sistema de gestión de riesgos dentro de una empresa siguiendo los lineamientos de COSO –ERM"*, 2017. **URI:** http://repositorio.puce.edu.ec/handle/22000/12923

Valdivia, Dan. "*Implementación de la norma ISO 31000:2009 como un sistema de gestión de riesgo crediticio: caso instituciones especializadas en microcrédito*"; Universidad Andina Simón Bolívar, Bolivia 2015. http://104.207.147.154:8080/bitstream/54000/198/1/TE-213.pdf

Vásquez Fredy et al. "*Información y ventaja competitiva. Coexistencia exitosa en las organizaciones de vanguardia*". Revista Internacional, Científica y Profesional El Profesional de la información. (págs.149-156). 2015. Vol. 24, Número 2 http://www.elprofesionaldelainformacion.com/contenidos/2015/mar/08.html

Anexos

Anexo 1: Hallazgos de Superintendencia de Bancos sobre Grupo Pichincha

Condición	Criterio	Causa	Efecto
1) El volumen de monitoreo puntual de operaciones no es significativo con relación al total de transacciones procesadas por los bancos privados	Implementar metodologías y procedimientos para detectar transacciones económicas inusuales e injustificadas, así como su oportuno y eficiente reporte a la UAFE	Al no considerar todos los factores de riesgo de las variables cualitativas y cuantitativas dentro de las transacciones, no se obtiene alertas de operaciones inusuales con características de riesgo integral	Operaciones injustificadas y de origen ilícito han sido procesadas sin levantar alertas ni reportes de inusualidad (ROII) a las autoridades competentes
2) No se realiza monitoreo de ciertas áreas internas (comercio exterior) y/o productos (cash management, tarjetas de crédito: consumos, pagos) de las entidades bancarias	Efectuar de forma permanente los procesos de monitoreo a todas las transacciones, de manera tal que se determine si la transaccionalidad del cliente se ajusta a los perfiles transaccional y de comportamiento establecidos	a) No se manejan sistemas centralizados para consolidar y procesar la información transaccional de clientes b) Falta de revisión e inclusión de las políticas de prevención de LAFD en productos nuevos	Se deja de monitorear y revisar parte de las operaciones con un alto riesgo inherente de LAFD por la naturaleza propia de dichas áreas internas y tipo de transacciones. No hay integridad de la revisión
3) El enfoque principal actual de riesgo para el monitoreo de operaciones está direccionado a variables cuantitativas, sin considerar mayormente las variables cualitativas	La consolidación de criterios y factores de riesgos, mediante categorías previamente definidas, permitirán a través de matrices de riesgos, segmentar a los clientes y obtener su perfil de riesgo y combinar el riesgo de cada uno de los factores diseñados	a) Falta de observancia de la normativa por cumplir los tiempos de implementación de controles que exige dicha norma b) No existe un análisis de riesgo integral considerando los factores demográficos y transaccionales	a) Generación de un número reducido de alertas de clientes b) No se generan alertas de transacciones que salen fuera del perfil de riesgo del cliente con base a factores cualitativos y cuantitativos
4) Conocimiento débil de las actividades económicas y de origen de fondos de clientes de alto riesgo, que operan con transacciones por encima de los umbrales de reporte (US $ 10.000)	Los mecanismos de control serán aplicados a todas las transacciones y de manera reforzada a aquellas cuyas cuantías individuales sean iguales o superiores a U$ 10.000, así como a las transacciones múltiples cuyo monto, en conjunto, dentro de un periodo de 30 días igualen o superen los U$ 10.000, cuando sean transacciones únicas, es decir, sean realizados en beneficio de una misma persona	a) Falta de segmentación de la base de clientes para identificar perfiles de riesgo y montos acumulados de transacciones b) Ausencia parcial o total de procedimientos de debida diligencia reforzada para segmentos de clientes que representan un alto riesgo para la entidad	a) Incumplimiento de la Política Conozca a su Cliente b) Aumenta el riesgo de procesar operaciones relacionadas al LAFD c) Observaciones por parte de las autoridades judiciales al no contar con información suficiente de clientes
5) No se cuenta en los archivos físicos de clientes toda la información que exige la normativa local en la apertura de cuenta de clientes	Las instituciones del sistema financiero deben diseñar y adoptar el formulario de solicitud de inicio de relación comercial en el que se incorporará toda la información y documentación	Por optimizar y reducir tiempos en la instancia de apertura de cuentas, no se obtiene toda la documentación e información mínima requerida por la normativa local	No se cuenta con información de respaldo que sustente un conocimiento del cliente en función de la normativa establecida para el efecto

Fuente: Informes de revisión in situ de Superintendencia de Bancos
Elaboración propia

Anexo 2: Matriz de principales partes interesadas (stakeholders)

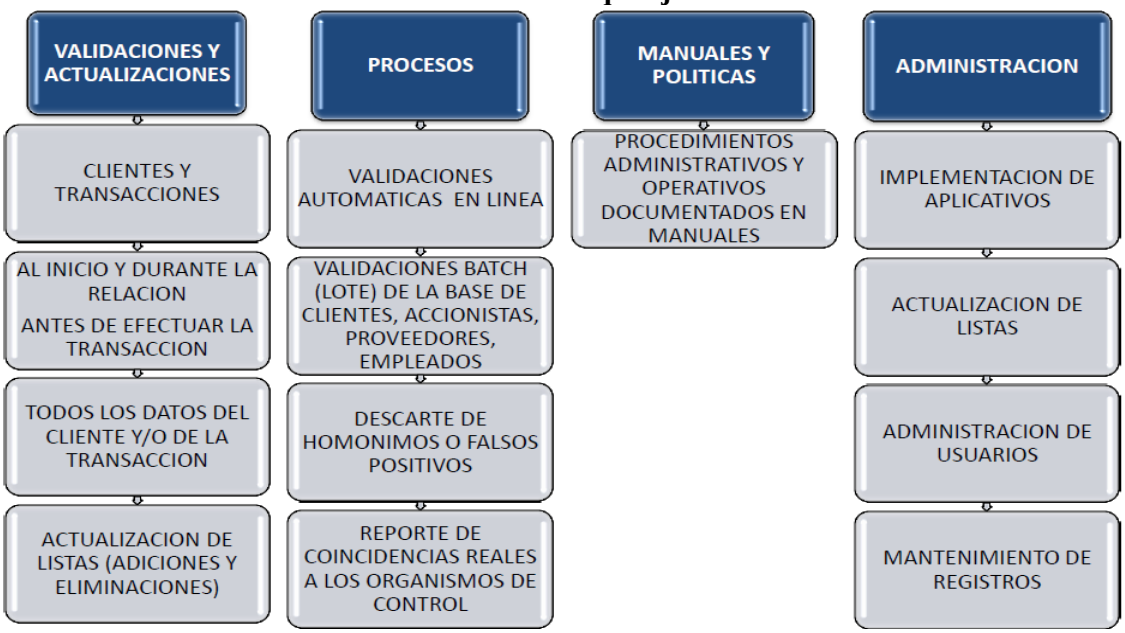
Stakeholders	Funciones y roles generales	Importancia del tema	Cómo contribuye a la gestión	Cómo puede retrasar la gestión	Estrategia de colaboración
Accionistas	* Aportar capital inicial * Definir los objetivos anuales * Decisiones sobre oportunidades de negocio * Reinversión de utilidades	* Maximizar las utilidades apoyando las políticas de prevención de LAFD * Obtener mayor captación del mercado financiero	* Alinearse a los postulados de prevención de LAFD * Proveer los recursos necesarios para prevención de LAFD	* No dar la importancia verdadera al proyecto de prevención LAFD * Interponer el interés económico al de control de prevención LAFD	Reuniones de sensibilización en la Sesión de Directorio para obtener el apoyo a las acciones del proyectos de prevención
Empleados	* Aporte de know how en controles * Potencia el negocio cumpliendo las normas * Ejecución de tareas asignadas dentro del proyecto de PLAFD	* Mantenimiento de condiciones estables de trabajo * Inclusión en programas de capacitación en PLAFD	* Compromiso y apoyo a las actividades de PLAFD * Aporte de ideas y sugerencias para optimizar al programa de prevención	* Falta de compromiso e incumplimiento de las acciones que demanda el proyecto * Conformar sindicatos y realizar huelga laboral	Capacitación semestral para difundir y sensibilizar el fenómeno de LAFD que es parte del entrenamiento que exige la normativa
Superintendencia de Bancos del Ecuador (SBS)	* Supervisar al sistema bancario a través del cumplimiento de la ley * Emitir informes de revisión del cumplimiento de la normativa * Imponer sanciones a las entidades bancarias en caso de observaciones, conforme la ley	* Verificar el cumplimiento de los aspectos normativos en materia de control de LAFD * Emitir recomendaciones para el mejoramiento del sistema de administración de riesgos	* Efectuar una revisión objetiva del programa de cumplimiento * Realizar el seguimiento de las recomendaciones efectuadas para su implementación	* Emisión de informes desfavorables sobre el cumplimiento del programa de prevención LAFD * No validar con la oportunidad del caso la inclusión de las recomendaciones emitidas	Reuniones trimestrales para presentación de avances de implementación de recomendaciones, producto de las revisiones in situ
Asociación de Bancos Privados del Ecuador - ABPE	* Agrupar las inquietudes y requerimientos de los bancos privados * Promover como asociación el acercamiento con los organismos de supervisión y control	Una entidad individual no logra una fuerza significativa para plantear temas de interés en materia de PLAFD	La asociación gremial es una estrategia de conjunto para expresar con mayor injerencia puntos de vista ante los reguladores	No lograr consenso en los puntos de vista y necesidades de asociación y apoyo de sus agremiados	Alinear objetivos comunes entre las entidades bancarias asociadas, a través de reuniones mensuales
Unidad de Análisis Financiero (UAFE)	* Normar las estructuras de información * Requerir información de cuentas de clientes * Receptar los reportes de operaciones inusuales * Reportar a Fiscalía casos de transacciones inusuales injustificadas	Receptar y consolidar la información mensual de cuentas de clientes de todas las entidades financieras, para reportar casos de operaciones injustificadas a la autoridad judicial	* Informa sobre tipologías de casos de LAFD * Planifica y aprueba planes de capacitación de PLAFD de las entidades financieras * Da soporte de consultas técnicas en esta materia	* Imposición de amonestaciones por falta de entrega de información en los plazos previstos, sin considerar problemas tecnológicos de las entidades y sujetos obligados	Reuniones trimestrales para abordar temas de procesamiento de información mensual a reportar y demás temas técnicos relacionadas al control de LAFD
Fiscalía General del Estado	* Representación de la sociedad en la acusación, investigación y persecución del delito.	Es el órgano judicial acusador para obtener la aplicación de sanciones por estos delitos tipificados en el COIP	Aporta con el desarrollo de la investigación de campo para establecer responsabilidades de estos delitos	No cumplir con una investigación objetiva para establecer responsabilidades, por cumplir con plazos de las etapas	Lograr acuerdos para la entrega oportuna de la información de los clientes objetos de investigación
Banca corresponsal del exterior	* Prestación de servicios de cuentas de corresponsalía * Requerimientos de debida diligencia para justificar transacciones	Acciones de colaboración para justificar el origen de fondos de las operaciones procesadas de clientes a través de cuentas de corresponsalía	Proporciona alertas de transacciones que fueron alertadas por los sistemas de monitoreo de los bancos corresponsales del exterior	Falta de retroalimentación sobre las razones de las transacciones alertadas objeto de los procesos de justificación y debida diligencia	Asistencia y colaboración mutua con la información de justificación de transacciones de clientes en los plazos definidos

Fuente y elaboración propia

Anexo 3: Control de listas restrictivas

Para este efecto los bancos cuentan con un software de listas restrictivas locales e internacionales (OFAC, ONU, FBI, entre otras) que controla y verifica en línea los nombres e identificaciones de clientes, previa a la prestación de un servicio bancario determinado, como: la apertura de cuentas, envío de transferencias, operaciones de crédito, emisión de cheques de gerencia, inversiones, entre otros. En cuanto a listas locales, éstas contienen las que proporciona la UAFE y la Secretaría Técnica de Drogas, a la cual se las puede complementar con lista restrictivas propias de cada institución (clientes sancionados por comité de cumplimiento, reportados a la UAFE, clientes activos controlados).

Gráfico
Control de listas restrictivas que ejecutan los bancos



Fuente: Procesos de control de listas restrictivas
Elaboración propia

Dependiendo del tipo de coincidencia en la lista restrictiva que maneje cada banco, por lo general se debe gestionar los siguientes casos sobre estas listas:

***Falso positivo*.** Es una coincidencia que al ser evaluada no corresponde al registro del cliente del banco.

Homónimo. Es una coincidencia en la que los nombres y apellidos encontrados son los mismos del cliente, pero el número de identificación es diferente.

Coincidencia real. Son los casos de los clientes que al ser alertados por la lista restrictiva se trata de la misma persona ya que coincide nombres, apellidos e

identificación, en cuyo caso se deben adoptar definiciones internas, que usualmente es la desvinculación como clientes de este grupo de personas, siguiendo el respectivo proceso de cancelación de cuentas.

Anexo 4: Indicador de reporte de transacciones inusuales a la UAFE

Concepto	Descripción
PROCESO	MONITOREO DE TRANSACCIONES DE CLIENTES
SUBPROCESO	Reportes de operaciones inusuales e injustificadas (ROII) remitidos a la UAFE
DEFINICION	Representa el nivel de operaciones inusuales realizadas por los clientes en la entidad identificadas en el monitoreo, sin justificación y reportadas a la UAFE
MEDICIÓN	Mensual
META	Lograr identificar, gestionar y evaluar las transacciones que exceden el perfil de riesgo asignado al cliente, para someterlas a un proceso de revisión y debida diligencia para justificar la excepción alertada por el sistema de monitoreo y que NO fueron justificadas por el cliente
VERIFICAR	Realizar el seguimiento que todas las operaciones inusuales alertadas sean gestionadas con apoyo del Ejecutivo de Cuenta y que exista una respuesta del cliente, y reportar a la UAFE aquellos casos que no fueron justificadas por el cliente
FORMA DE CÁLCULO	$\frac{\text{Número de ROII de clientes reportados a la UAFE}}{\text{Número de alertas gestionadas con el Negocio para descarte}} \times 100$
	$\frac{\text{Número. de alertas gestionadas con el Negocio para descarte}}{\text{Número total de clientes alertados por sistema de monitoreo}} \times 100$
RESPONSABLE	Unidad de Cumplimiento / Ejecutivos de Negocio
FINALIDAD	Mide el nivel porcentual de las transacciones inusuales e injustificadas reportadas a la UAFE con relación al total de transacciones alertadas y gestionadas con el Negocio para descarte
FUENTE DE INFORMACIÓN	Base de datos del software de monitoreo, tanto de los casos alertados de transacciones inusuales, como los casos injustificados y reportados a la UAFE
NIVEL DE REPORTE	Comité de Cumplimiento y Comité Integral de Riesgos
FUENTE DEL INDICADOR	Indicador requerido por la Superintendencia de Bancos y Comité de Riesgos

Fuente y elaboración propia

Anexo 5: Indicador de atención de requerimientos de corresponsales

Concepto	Descripción
PROCESO	ATENCIÓN DE REQUERIMIENTOS DE CORRESPONSALES
SUBPROCESO	Debida Diligencia para Justificación Transacciones de clientes
DEFINICIÓN	Procedimiento de debida diligencia para justificar transacciones de clientes, solicitados por bancos del exterior
MEDICIÓN	Mensual
META	Atender los requerimientos de información y debida diligencia solicitados por bancos del exterior para justificar transacciones realizadas por clientes del banco con intervención de corresponsales del exterior, en los plazos y condiciones definidas para el efecto
VERIFICAR	Revisión de la pertinencia de la información y los soportes que justifican el origen y destino de los fondos involucrados en la transacción objeto de la debida diligencia
FORMA DE CÁLCULO	No. de pedidos de debida diligencia de clientes atendidos al mes / No. de debida diligencia requeridas por corresponsales en un mes x 100
RESPONSABLE	Unidad de Cumplimiento / Oficial de Cumplimiento
FINALIDAD	Mide el nivel porcentual de los requerimientos atendidos de justificación de transacciones requeridos por los corresponsales del exterior en un periodo determinado
FUENTE DE INFORMACIÓN	Base de datos del software de monitoreo, que almacena las operaciones de la base de clientes o en su defecto la extracción de las transacciones de la base central de datos
NIVEL DE REPORTE	Comité de Cumplimiento y Comité Integral de Riesgos
FUENTE DEL INDICADOR	Indicador requerido por el Comité de Cumplimiento y Comité Integral de Riesgos

Fuente y elaboración propia

Anexo 6: Indicador de atención de pedidos de información

Concepto	Descripción
PROCESO	ATENCIÓN DE PEDIDOS DE ORGANISMOS DE CONTROL
SUBPROCESO	Envío de información de clientes solicitado por organismos de control
DEFINICIÓN	Procedimiento de atención de pedidos de información de clientes, solicitados por organismos de control y autoridades judiciales para los procesos de investigación de casos de LAFD
MEDICIÓN	Mensual
META	Atender los requerimientos de información relacionada a los clientes del banco solicitados, dentro de los plazos legales definidos por las autoridades
VERIFICAR	Revisión previa de la integridad y exactitud de la información requerida del cliente, antes del envío, puesto que si la misma no es consistente y completa, la entidad puede ser objeto de sanciones
FORMA DE CÁLCULO	No. de pedidos información de clientes atendidos al mes / No. de pedidos de información de clientes solicitados en un mes x 100
RESPONSABLE	La consolidación y envío corresponde a la Unidad de Cumplimiento, la integridad de la información histórica de transacciones es responsabilidad de las áreas de tecnología y los soportes de las áreas de negocio, operativas y archivo central
FINALIDAD	Mide el nivel porcentual de cumplimiento de los requerimientos atendidos de información solicitada por las autoridades judiciales en un periodo determinado

FUENTE DE INFORMACIÓN	Los movimientos transaccionales son extraíbles de la base de datos de las operaciones bancarias, en tanto que los documentos soporte se encuentran en el file del cliente, áreas operativas y comerciales
NIVEL DE REPORTE	Comité de Cumplimiento y Comité Integral de Riesgos
FUENTE DEL INDICADOR	Indicador requerido por el Comité de Cumplimiento y Comité Integral de Riesgo

Fuente y elaboración propia

Anexo 7: Indicador de gestión de control de listas restrictivas

Concepto	Descripción
PROCESO	GESTIÓN DE CONTROL DE LISTAS RESTRICITVAS
SUBPROCESO	Proceso de cruce de listas restrictivas con la base de clientes
DEFINICIÓN	Procedimiento de validación y cruce de las base de datos de clientes con la base de las listas restrictivas locales e internacionales
MEDICIÓN	Semanal
META	Realizar el cruce de las bases de datos de clientes del banco para identificar las coincidencias reales y casos de personas con nombres homónimos
VERIFICAR	Identificar y gestionar los casos de clientes con coincidencias reales para gestionar la desvinculación como cliente de la entidad, así como aceptar y regularizar a los clientes con nombres homónimos previa gestión de comprobación documental
FORMA DE CÁLCULO	$\frac{\text{No. de clientes homónimo regularizados}}{\text{No. total de base de personas en listas restrictivas}} \times 100$
	$\frac{\text{No. de personas en listas con coincidencias reales}}{\text{No. total de base de personas en listas restrictivas}} \times 100$
RESPONSABLE	Unidad de Cumplimiento / Oficial de Cumplimiento
FINALIDAD	Desvincular a clientes activos e inactivos que consten en las listas restrictivas, y realizar un proceso de regularización para la aceptación de casos de clientes con nombres homónimos
FUENTE DE INFORMACIÓN	La base de listas restrictivas se encuentra centralizadas en el software de los proveedores de estas listas negativas, que contienen la base de personas locales e internacionales con antecedentes negativos
NIVEL DE REPORTE	Comité de Cumplimiento y Comité Integral de Riesgos
FUENTE DEL INDICADOR	Indicador requerido por el Comité de Cumplimiento y Comité Integral de Riesgos

Fuente y elaboración propia