

SISTEMAS DE PREVENCIÓN DE LAVADO DE ACTIVOS Y DE FINANCIACIÓN DEL TERRORISMO

FRANCISCO SINTURA - WILSON MARTÍNEZ - FERNANDO QUINTANA



BOGOTÁ • MÉXICO D.F. • BUENOS AIRES • CARACAS • LIMA • SANTIAGO

SEGUNDA EDICIÓN 2014

Primera edición 2011

© Francisco Sintura - Wilson Martínez - Fernando Quintana
© Legis Editores S.A., 2014

Queda prohibida la reproducción total o parcial de este libro,
por cualquier proceso reprográfico o fónico, por fotocopia, microfilme,
offset o mimeógrafo, sin previa autorización del editor.

LEGIS

Presidente (E): *Diego Barrero Castañeda*
Directora Editorial: *Martha Penen Lastra*
Diseño de Carátula: *Juan Felipe Ulloa*
Diagramación: *Preprensa Editorial*
Impresión: LEGIS S.A.

ISBN: 978-958-653-???-?

Impreso en Colombia / Printed in Colombia

AGRADECIMIENTOS

Los autores agradecen a sus familias el haberles permitido disponer de un tiempo precioso de convivencia para la elaboración del trabajo. Sin su ánimo y decidido respaldo, nada hubiera sido posible.

Al equipo editorial de Legis, por su orientación y consejo.

A Viviane Morales Hoyos y Eduardo A. Fabián Caparrós, quienes consideraron digno de su pluma el prologar esta obra, que no pretende más que llamar la atención sobre el elemento más valioso de una sana política de *buen gobierno corporativo* para la prevención y administración del riesgo de lavado de activos y financiación del terrorismo.

ÍNDICE GENERAL

PRÓLOGO DE VIVIANE MORALES HOYOS.....	<i>xvii</i>
PRÓLOGO DE EDUARDO A. FABIÁN CAPARRÓS.....	<i>xxiii</i>
INTRODUCCIÓN: LA PREVENCIÓN DEL LAVADO DE ACTIVOS COMO UNA POLÍTICA DE BUEN GOBIERNO CORPORATIVO Y DE RESPONSABILIDAD EMPRESARIAL	<i>xxix</i>

PRIMERA PARTE

Marco jurídico de la prevención del lavado de activos y la financiación del terrorismo

MARCO JURÍDICO DE LA PREVENCIÓN DEL LAVADO DE ACTIVOS Y LA FINANCIACIÓN DEL TERRORISMO	1
---	---

CAPÍTULO 1

Retrospectiva en el derecho colombiano

RETROSPECTIVA EN EL DERECHO COLOMBIANO	13
--	----

CAPÍTULO 2

Estándares internacionales en materia de prevención

1. PRINCIPIOS GENERALES DE PREVENCIÓN DEL COMITÉ DE BASILEA	30
1.1. Identificación del cliente.....	30
1.2. Aseguramiento y control del cumplimiento de la ley.....	31
1.3. Cooperación con las autoridades judiciales.....	31
1.4. Adopción formal de políticas para la prevención del lavado de activos	31
2. RECOMENDACIONES DEL GRUPO DE TRABAJO DE ACCIÓN FINANCIERA, GAFI	32

3. RECOMENDACIONES DE LA ONU	38
3.1. Convención de Viena de 1988	38
3.2. Convención de Palermo	43
4. RECOMENDACIONES DEL COMITÉ DE BASILEA PARA EL CONOCIMIENTO DEL CLIENTE	49
4.1. Política clara y expresa para la aceptación de clientes	50
4.2. Mecanismos para un adecuado y oportuno conocimiento del cliente	51
4.3. Seguimiento continuo de las cuentas de alto riesgo	52
4.4. Definición de la gestión de riesgos	53
5. RECOMENDACIONES DEL FORO CONJUNTO ENTRE EL COMITÉ DE BASILEA, EL IAIS Y LA IOSCO	53
6. CONVENIO DEL CONSEJO DE EUROPA SOBRE BLANQUEO DE CAPITALES ...	56
7. RECOMENDACIONES DEL GRUPO EGMONT	60
8. RECOMENDACIONES DE LA CICAD	63

CAPÍTULO 3

Normatividad colombiana vigente

1. ETAPAS DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO (SARLA/FT)	80
1.1. Identificación del riesgo	83
1.2. Medición del riesgo	84
1.3. Control del riesgo	86
1.4. Monitoreo del riesgo	92
2. ELEMENTOS DEL SARLA/FT	98
2.1. Políticas	99
2.2. Procedimientos	99
2.3. Documentación	101
2.4. Estructura organizacional	102
2.5. Órganos de control	106
2.6. Infraestructura tecnológica	108
2.7. Divulgación de información	109

CAPÍTULO 4

Características y alcances de la Lista Clinton

CARACTERÍSTICAS Y ALCANCES DE LA LISTA CLINTON	115
--	-----

CAPÍTULO 5

La prevención del lavado de activos en el sector real

1. CATÁLOGO DE SEÑALES DE ALERTA PARA ALGUNAS INDUSTRIAS DEL SECTOR REAL	136
1.1. Frente al cliente	136
1.2. Frente a los proveedores	139
1.2.1. Señales en proveedores personas jurídicas	139
1.2.2. Señales en proveedores personas naturales	140
1.3. Frente a empleados	142

SEGUNDA PARTE

Metodología para la gestión del riesgo de lavado de activos y financiación del terrorismo

1. INTRODUCCIÓN	143
2. APLICACIÓN DE LA METODOLOGÍA EN EL PROCESO PRODUCTIVO	145
3. FUENTES PARA LA IDENTIFICACIÓN DE POSIBLES IMPACTOS	148
4. PROPUESTA METODOLÓGICA	150

CAPÍTULO 1

Alcance del SARLA/FT y del SIPLA/FT

1. ALCANCE DEL SARLA/FT	166
— Marco normativo del SARLA/FT	168
2. ALCANCE DEL SIPLA/FT	168
— Marco normativo del SIPLA/FT	171

CAPÍTULO 2

Contexto organizacional

1.	ESTRUCTURA ORGANIZACIONAL	173
1.1.	Organigrama	174
1.1.1.	Junta directiva	174
1.1.2.	Representante legal	175
1.1.3.	Gerente de riesgos	176
1.1.4.	Oficial de cumplimiento	177
1.1.5.	Oficial de cumplimiento suplente	179
1.1.6.	Analista de operaciones inusuales y administrador de datos	180
1.1.7.	Comité evaluador de operaciones	180
1.1.8.	Empleados	183
1.2.	Órganos de control interno y revisión	185
1.2.1.	Revisor fiscal	185
1.2.2.	Auditoría interna	185
1.3.	Infraestructura tecnológica y consolidación electrónica de operaciones	186
1.4.	Programa de capacitación	188
2.	CARACTERÍSTICAS DE LA ORGANIZACIÓN Y SU ENTORNO	191
2.1.	Adaptación de la empresa a su entorno (perspectiva del LA/FT)	192
2.2.	Diagnóstico de la prevención y control del LA/FT en la empresa	193
2.2.1.	Diagnóstico de fortalezas y debilidades	193
2.2.2.	Amenazas del entorno por riesgo de LA/FT	198
2.2.3.	Oportunidades del entorno para enfrentar el riesgo de LA/FT	199
2.2.4.	Fortalezas internas de la empresa para la prevención y control del LA/FT	200
2.2.5.	Debilidades internas de la empresa para la prevención y control del LA/FT	200
2.3.	Vulnerabilidad de la empresa al riesgo de LA/FT	201
3.	POLÍTICAS PARA LA PREVENCIÓN Y CONTROL DEL LA/FT	204
3.1.	Políticas generales para la gestión del SARLA/FT	205
3.2.	Políticas específicas para impulsar la cultura de prevención y control del riesgo LA/FT en la empresa	209

3.3.	Políticas específicas para cada etapa del SARLA/FT.....	211
3.3.1.	Para la identificación de eventos de riesgo de LA/FT....	211
3.3.2.	Para la medición de eventos de riesgo de LA/FT.....	212
3.3.3.	Para el control de eventos de riesgo de LA/FT.....	213
3.3.4.	Para el monitoreo de eventos de riesgo de LA/FT	214
3.4.	Políticas específicas para los mecanismos e instrumentos de la etapa de control del SARLA/FT.....	215
3.4.1.	Para el conocimiento del usuario	215
3.4.2.	Para el conocimiento del cliente.....	216
3.4.3.	Para el conocimiento de clientes especiales	224
3.5.	Políticas específicas para la capacitación	225
3.6.	Políticas específicas de productos y servicios.....	227
3.7.	Consideraciones básicas para la implementación de las políticas de prevención y control del LA/FT.....	228
3.7.1.	Diseño y aplicación de una metodología para la identificación de operaciones inusuales y diseño de controles que mitiguen el riesgo de LA/FT.....	228
3.7.2.	Diseño de mecanismos e instrumentos para implementar el SIPLA/FT o el SARLA/FT	228
3.7.3.	Definición de mecanismos, procedimientos, instancias responsables de los órganos de funciones de control interno para el riesgo de LA/FT	229
3.7.4.	Diseño de tipos de reportes que debe generar el sistema...	230
3.7.5.	Diseño de políticas, procesos y procedimientos para la documentación y registros del sistema	230
4.	PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE POLÍTICAS DEL SARLA/FT	230
4.1.	Para identificar (buscar, denominar, describir) operaciones inusuales	231
4.2.	Para detectar operaciones sospechosas	231
4.3.	Para impulsar la cultura organizacional de prevención y control del riesgo de LA/FT	234
4.4.	Para los mecanismos de control	235
4.4.1.	Para el conocimiento del usuario	236
4.4.2.	Para el conocimiento del cliente	237
4.4.3.	Para el conocimiento de proveedores	239
4.4.4.	Para el conocimiento de empleados	240
4.4.5.	Para el conocimiento de los accionistas	240

4.4.6. Para el conocimiento de la junta directiva	240
4.4.7. Para el conocimiento del mercado	241
4.4.8. Excepciones	242
4.5. Para los instrumentos establecidos para la prevención y control del LA/FT	244
4.6. Para dar cumplimiento a las obligaciones relacionadas con las listas internacionales	246
4.6.1. Listas internacionales vinculantes para Colombia	246
4.6.2. Otras listas de control de riesgos LA/FT	247
4.7. Para garantizar la reserva de la información reportada conforme lo establece el Estatuto Orgánico del Sistema Financiero	253
4.8. Para prevenir y resolver los posibles conflictos de interés e imposición de sanciones	253
4.9. Para asegurar el cumplimiento de los reglamentos internos y demás disposiciones relacionadas con el SARLA/FT	256
5. EMPRESAS OBLIGADAS A DISEÑAR E IMPLEMENTAR EL SARLA/FT O EL SIPLA/FT	256
5.1. Empresas del sector real y del sector financiero	261
5.2. Características de las empresas obligadas a diseñar e implementar el SIPLA/FT y el SARLA/FT	262
5.2.1. Concepto de servucción	263
5.2.2. Concepto de producción	268
6. NECESIDADES DE PREVENCIÓN Y CONTROL DEL LA/FT	268
6.1. Necesidades de prevención de las empresas	269
6.2. Necesidades de prevención del Estado	269
6.3. Necesidades de <i>stakeholders</i> o partes interesadas	269
7. SISTEMA EMPRESARIAL DE PRODUCCIÓN: MACROPROCESOS Y PROCESOS DEL SISTEMA	270
7.1. Enfoque sistémico de la organización y factores que la exponen al riesgo de LA/FT	271

CAPÍTULO 3 **Propuesta metodológica**

1. OPERACIONES SOSPECHOSAS Y OPERACIONES INUSUALES	275
1.1. Identificación de operaciones inusuales	276
1.2. Detección de operaciones sospechosas	278

1.3. Ejemplos de identificación y detección de OI y OS por OM	279
1.4. Responsables en el proceso de identificación de OI y detección de OS	280
2. OPERACIÓN SOSPECHOSA Y SU ASOCIACIÓN CON UN EVENTO DE RIESGO DE LA/FT	281
3. REPORTE DE OPERACIONES SOSPECHOSAS (ROS)	282
4. GESTIÓN DEL SIPLA/FT Y DEL SARLA/FT MEDIANTE RIESGOS EN PROCESOS	284
4.1. Gerencia o gestión de riesgos por procesos.....	285
4.2. Caracterización del proceso de gestión del SIPLA/FT y del SARLA/FT	285
4.3. Lógica del proceso SARLA/FT	288
4.4. Breve presentación de metodologías y procesos de las etapas de administración del SARLA/FT	289
5. METODOLOGÍA DE LA ESPINA DE PESCAZO Y DEFINICIÓN DE EVENTOS DE RIESGO DE LA/FT	291
5.1. Aplicación general de la metodología de la espina de pescado.....	293
5.2. Aplicación de la metodología de la espina de pescado en un evento de riesgo de LA/FT	296
6. METODOLOGÍA PARA LA IDENTIFICACIÓN DE EVENTOS DE RIESGO DE LA/FT	302
6.1. Factores de riesgo en empresas del sector real.....	303
6.2. Señales de alerta.....	304
6.3. Grupos de señales de alerta	306
6.4. Identificación de eventos de riesgo de LA/FT	310
6.4.1. Detección del conjunto inicial de eventos de riesgo de LA/FT.....	311
6.4.2. Detección de componentes de eventos de riesgo de LA/FT	315
6.4.3. Descripción de eventos de riesgo de LA/FT mediante la aplicación del diagrama causa-efecto ("espina de pescado").....	315
6.4.4. Materialización de eventos de riesgo de LA/FT (riesgos asociados al LA/FT).....	317
6.4.5. Descripción de eventos de riesgo de LA/FT que se podrían utilizar en la empresa.....	317

7. METODOLOGÍA PARA MEDICIÓN O EVALUACIÓN DE EVENTOS DE RIESGO DE LA/FT	321
7.1. Medición del riesgo inherente	322
7.2. Medición del riesgo residual	322
7.3. Medición o evaluación de un evento de riesgo de LA/FT	323
7.3.1. Medición de la probabilidad de ocurrencia de un evento de riesgo de LA/FT	324
7.3.2. Escalas de medición de impacto para cada uno de los riesgos asociados	326
7.4. Severidad de un evento de riesgo de LA/FT	328
7.5. Disposición gráfica del mapa de un evento de riesgo de LA/FT	333
7.5.1. Medición de probabilidad e impacto del riesgo inherente	333
7.5.2. Medición de probabilidad, impacto y severidad de un evento de riesgo de LA/FT del riesgo residual.....	338
8. METODOLOGÍA DE CONTROL DE EVENTOS DE RIESGO DE LA/FT	342
8.1. Metodología de los “cinco por qué”	343
8.2. Identificación de controles existentes.....	345
8.3. Validación y evaluación de controles actuales (para el riesgo inherente)	346
8.3.1. Relación costo-beneficio de controles de eventos de riesgo de LA/FT	347
8.3.2. Decisiones con respecto a los controles de eventos de riesgo de LA/FT	348
8.4. Medición de la efectividad de los controles	350
8.4.1. Análisis de efectividad de controles	351
8.3.2. Consolidación de mapas de riesgo (residual e inherente)	357
9. MONITOREO DE EVENTOS DE RIESGO DE LA/FT	358
9.1. Monitorear, medir y revisar un evento de riesgo de LA/FT	361
9.2. Metodología de monitoreo de un evento de riesgo de LA/FT	361
9.2.1. Indicador de gestión (eficacia) del SIPLA/FT o del SARLA/FT: la propensión marginal de la empresa al riesgo de LA/FT	361
9.2.2. Variables de la propensión al riesgo de LA/FT	363
9.2.3. Definición de propensión marginal al riesgo de LA/FT (PMRLA/FT).....	364

9.2.4.	Cálculo del indicador de la propensión marginal al riesgo de LA/FT	365
9.2.5.	Medidas del indicador de la PMRLA/FT	366
9.2.6.	Técnicas estadísticas para medir el indicador de la PMRLA/FT	366
9.2.7.	Interpretación del indicador de la PMRLA/FT	366
9.2.8.	Ejemplo de propensión marginal al riesgo de LA/FT.....	367
9.2.9.	Ejemplo de propensión marginal de una empresa al RLA/FT por operaciones inusuales (PMRLA/FT-OI) ..	368
9.2.10.	Ejemplos de propensión marginal de una empresa al riesgo de LA/FT por operaciones inusuales y por operaciones sospechosas	369
10.	IMPLEMENTACIÓN DEL SARLA/FT (EL CICLO PHVA)	370
10.1.	Fase Planear (establecer el SARLA/FT)	373
10.2.	Fase Hacer (implementar y operar el SARLA/FT)	375
10.3.	Fase Verificar (monitorear, medir y revisar el SARLA/FT) ..	376
10.4.	Fase Actuar (mantener y mejorar continuamente el SARLA/FT o el SIPLA/FT)	377
11.	SENCILLO APlicATIVO PARA GESTIONAR EL SIPLA/FT O EL SARLA/FT	378
12.	DOCUMENTACIÓN	383
12.1.	Criterios y procesos de manejo	383
12.2.	Guarda	383
12.3.	Conservación.....	384

ANEXOS

1.	Calificación de la severidad de un evento de riesgo de LA/FT	387
2.	Mapa de eventos de riesgo de LA/FT inherentes.....	389
3.	Ejemplo de medición del impacto para el riesgo residual	392
4.	Mapa de eventos de riesgo de LA/FT residual	394
5.	Ejemplo de causas y controles para cinco eventos de riesgo de LA/FT	397
6.	Indicadores de efectividad de los controles	400
7.	Señales de alerta que se pueden percibir en la operación comercial o financiera de una empresa del sector real	404
	BIBLIOGRAFÍA	417
	CONTENIDO DEL CD-ROM	425

ABREVIATURAS

BIS	<i>Bank for International Settlements</i>	OGBS	<i>Offshore Group of Banking Supervisors</i> (Grupo Extraterritorial de Supervisores Bancarios)
BGC	Buen gobierno corporativo	OI	Operaciones inusuales
BSBC	<i>Basel Committee on Banking Supervision</i> (Comité sobre Supervisión Bancaria de Basilea o Comité de Basilea)	OM	Operaciones múltiples
CDD	<i>Costumer due diligence</i>	ON	Operaciones normales
CEO	Cantidad de eventos ocurridos	ONU	Organización de las Naciones Unidas
CEP	Cantidad de eventos posibles	OS	Operaciones sospechosas
CICAD	Comisión Interamericana para el Control del Abuso de Drogas	OT	Operaciones totales
CIFIN	Centro de información financiera	P	Probabilidad
DOF	Declaración de origen e fondos	PEP	Persona expuesta públicamente
ERLA/FT	Evento de riesgo de lavado de activos y financiación del terrorismo	PMRLA/FT	Propensión marginal al riesgo de LA/FT
GAFI	Grupo de Acción Financiera (<i>Financial Action Task Force, FATF</i>)	ROS	Reporte de operaciones sospechosas
GAFIC	Grupo de Acción Financiera del Caribe	S	Severidad
GAFISUD	Grupo de Acción Financiera de Sudamérica	SARLA/FT	Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo
IAIS	<i>International Association of Insurance Supervisors</i> (Asociación Internacional de Supervisores de Seguros)	SARO	Sistema de administración del riesgo operativo
IOSCO	<i>International Organization of Securities Commissions</i> (Organización Internacional de Comisiones de Valores)	SFC	Superintendencia Financiera de Colombia
LA/FT	Lavado de activos y financiación del terrorismo (<i>anti-money laundering/combatting the financing of terrorism, AML/CFT</i>)	SIPLA/FT	Sistema Integral para la Prevención del Lavado de Activos y de la Financiación del Terrorismo
OEA	Organización de Estados Americanos	UE	Unidad estratégica
		UERLA/FT	Unidad estratégica en riesgos de lavado de activos y financiación del terrorismo
		UIAF	Unidad de Información y Análisis Financiero
		UNODC	<i>United Nations Office on Drugs and Crime</i> (Oficina de las Naciones Unidas contra la Droga y el Delito)

PRÓLOGO

*Por: Viviane Morales Hoyos
Fiscal General de la Nación*

A lo largo de las últimas dos décadas hemos presenciado un cambio importante de paradigma en el Derecho Penal. Algunos círculos académicos denominan este cambio: “*la expansión del Derecho Penal*”, y le atribuyen importantes manifestaciones como la creación de nuevos bienes jurídicos y de nuevos delitos, el aumento generalizado de las penas, la flexibilización de los criterios para la atribución de responsabilidad penal y la disminución de ciertas garantías procesales.

La expansión del Derecho Penal resulta en sí misma interesante, no sólo por sus manifestaciones sino también por sus causas. Es interesante reflexionar, por ejemplo, acerca de cómo la globalización económica, el desarrollo de los medios de comunicación y de transporte, el avanzado proceso de tecnificación de diversos ámbitos de la vida diaria y otras tantas características de nuestra sociedad actual pueden ayudar a explicar ese fenómeno. Sin embargo, detrás de todas las causas que se le atribuyen a la expansión del Derecho Penal existe un factor común, que resulta esencial para entender el cambio de paradigma que venimos presenciando: el aumento de nuestro conocimiento y, por consiguiente, de nuestra sensibilidad frente a los diversos riesgos a los que estamos expuestos.

En efecto, un sector de la sociología contemporánea ha calificado acertadamente nuestra sociedad actual, como una “sociedad del riesgo”. Una sociedad que gracias al mejoramiento de su capacidad para comprender los fenómenos, ha desarrollado la habilidad de identificar las causas de los sucesos, a predecir los eventos desafortunados y, hasta cierto punto, a prevenirlos. Esta preocupación por identificar y prevenir la rea-

lización de riesgos es evidente en prácticamente todas las áreas del conocimiento: por ejemplo, los economistas desarrollan modelos matemáticos cada vez más complejos para predecir el comportamiento de los mercados y reducir los riesgos financieros; los médicos investigan métodos de diagnóstico que permitan identificar las enfermedades antes de que el paciente las padezca; y los abogados han creado una vasta legislación en materia de Derecho de seguros que permite asegurar casi todos los riesgos imaginables.

Por supuesto, la política no podía ser ajena a esta realidad, y mucho menos la política criminal. Durante años se sostuvo que como el Estado tiene la obligación de proteger la vida, honra, bienes y creencias de los ciudadanos, la única finalidad legítima que puede tener el Derecho Penal en el marco de un Estado social y democrático de Derecho es la protección de los bienes jurídicos. Sin embargo, al amparo del principio de *lesividad*, el *ius puniendi* del Estado sólo se activaba cuando el bien jurídico ya había sido lesionado, porque se consideraba que sólo entonces la imposición de una pena resultaba legítima. Esta circunstancia sustentó durante años el cuestionamiento de que el Derecho Penal siempre llegaba tarde a cumplir su función, y que por lo tanto no la cumplía verdaderamente, en tanto que la imposición de la pena tenía un valor más simbólico que real a la hora de proteger los bienes jurídicos lesionados: la pena no devuelve la vida, la salud, la honra o la libertad arrebatadas con el delito.

La preocupación por la ineeficacia del Derecho Penal, sumada al exacerbado sentimiento de inseguridad desatado en la última década por el crecimiento de la amenaza terrorista en los países desarrollados (acostumbrados a ser sociedades pacíficas y seguras), impuso la necesidad de redefinir la política criminal: el Estado ya no puede esperar la lesión de los bienes jurídicos para recurrir al Derecho Penal, sino es necesario aplicar el conocimiento en materia de prevención de riesgos para producir un adelantamiento en la esfera de protección de los bienes jurídicos. De esta manera se produjo un vertiginoso avance en la política criminal moderna, que pasó de estar enfocada en la *represión* del delito a poner el acento en la *prevención*.

Una manifestación evidente de esto es el aumento significativo de tipos penales de peligro, e incluso la aparición de tipos penales de peligro

abstracto. Sin embargo hay otras manifestaciones menos evidentes en el ámbito del Derecho Penal, porque son el producto de una política criminal expandida que recurre a otras ramas del Derecho, en una especie de combinación de todas las formas válidas de lucha contra el delito. Me refiero a la creación de regímenes administrativos o mercantiles especiales, para la prevención de ciertas manifestaciones específicas de criminalidad. Y precisamente, el mejor ejemplo de esta expansión de la política criminal es el tema del que se ocupa la presente obra: el régimen administrativo de prevención del lavado de activos en los mercados financiero, bursátil, asegurador y cambiario.

En efecto, a la hora de enfrentar un fenómeno criminal tan complejo como el lavado de activos, la política criminal tradicional se habría limitado a fortalecer los mecanismos de represión del delito aumentando las penas, dotando de mayores facultades judiciales a los órganos de investigación, contrayendo ciertas garantías procesales, incrementando el número de investigadores, fiscales y jueces etc. Sin embargo, la eficacia de estas medidas habría sido limitada y su capacidad de rendimiento escasa. En lugar de esto, la comunidad internacional aunó esfuerzos por desarrollar unos estándares internacionales en materia de política criminal contra este delito, que cambiaran el enfoque tradicional. Fue así que apreció la recomendación de crear normas, que obligaran a los particulares a tomar medidas para prevenir el lavado de activos.

El cambio de paradigma en la lucha contra el lavado de activos fue una estrategia brillante y sumamente útil de la comunidad internacional: en lugar de imponer al Estado la enorme y pesada carga de fortalecer él sólo la persecución del delito, la responsabilidad de prevenir su comisión se dispersó entre diversos sectores de la sociedad, con lo cual se logró un efecto de cooperación y coordinación entre el Estado y la sociedad civil para hacer frente a un fenómeno altamente lesivo y desestabilizador. Gracias a este nuevo enfoque, el Estado ya no estaría sólo en su lucha contra el lavado de activos, ni contra todas las formas de criminalidad organizada asociadas a este delito. Ahora toda la sociedad, y particularmente los sectores más utilizados para su comisión, tendrían una buena parte de la responsabilidad. Todo esto en el marco de un régimen que intenta, y en la mayoría de los casos logra satisfactoriamente, combinar la heterorregulación estatal y la autorregulación de los particulares.

Pero por supuesto, este nuevo enfoque sólo fue posible gracias a la comprensión del lavado de activos, no como sólo delito sino como fenómeno criminal. En la medida que se entendieron mejor las causas, modalidades y consecuencias propias del lavado de activos, las autoridades agudizaron su comprensión del fenómeno y pudieron identificar los sectores más afectados por este delito. Además, enfocar el lavado de activos como fenómeno criminal y no sólo como delito permitió darle un tratamiento distinto, a partir de los diferentes riesgos a los que están expuestas las personas más utilizadas para su comisión: riesgos legales, operacionales, reputacionales, de contagio, etc.

La conciencia acerca de las consecuencias del lavado de activos permitió sensibilizar a los particulares acerca de los riesgos a los que se ven expuestos cuando son utilizados para la comisión de este delito, y ello estimuló la adopción de programas de cumplimiento (autorregulación) para prevenirlo. Hoy podemos decir que existe una creciente cultura de la prevención del lavado de activos, la cual no sólo va en aumento sino que se desarrolla y perfecciona permanentemente: de los programas inicialmente concebidos como sistemas estáticos de prevención, se ha dado un giro hacia los sistemas dinámicos de gestión (administración) de los riesgos inherentes al lavado de activos.

El trabajo elaborado por Francisco Sintura, Wilson Alejandro Martínez y Francisco Quintana tiene el mérito de abordar el estudio del lavado de activos desde la perspectiva en que actualmente se trabaja. Su libro no se ocupa del lavado de activos como delito, ni intenta ser otro estudio dogmático más acerca de ese tema. El enfoque de su libro es el de la política criminal de la prevención, lo que da a su obra un alcance internacional y la hace un trabajo notoriamente destacable en su género. Además de ser una obra cuidadosa y sistemáticamente organizada, lo que de entrada lo convierte en un libro de estudio útil para todos los que incursionan por primera vez en este tema, también es un trabajo valiente por ocuparse precisamente de uno de los aspectos más complejos, técnicos y menos estudiados de la prevención del lavado de activos: la metodología para la identificación y medición de los riesgos inherentes a ese delito.

Debo decir que me complace mucho poder prologar esta obra, y llamar la atención del lector respecto de su originalidad, importancia y ri-

gor académico. Tengo la seguridad de que este libro constituye un valioso aporte para el estudio, diseño y mejoramiento de las políticas públicas de prevención del lavado de activos, tanto en Colombia como en todos los demás países en que se distribuirá. Por esta razón no sólo recomiendo su lectura, sino además su profundo estudio y discusión académica, segura como estoy que se trata de un referente importante para cualquier persona que desee o deba conocer a profundidad este tema.

Bogotá D.C., febrero 28 de 2011

PRÓLOGO

Por: Eduardo A. Fabián Caparrós^()*

Sin duda, la mayor parte de los ciudadanos identifica el *lavado de activos* con la idea de delito y, más concretamente, con el tratamiento penal de las finanzas relacionadas con el crimen organizado y la corrupción.

La amenaza penal es popular. En general, impacta favorablemente entre la mayoría de sociedad porque todo el mundo piensa que hay que ser duro con los infractores y que la cárcel “es cosa de otros”. Sin embargo, todos sabemos que el Estado se encuentra sometido a límites constitucionales que le impiden desplegar su potestad punitiva a discreción. El Derecho Penal debe ser *ultima ratio* y a él sólo se debe acudir cuando sea verdaderamente imprescindible; cuando otros medios de control menos agresivos se revelen ineficaces. Y ello no deber ser así sólo por el –insoslayable– respeto a las garantías fundamentales, sino también por razones de eficacia, de orden práctico: como la economía, también el *ius puniendi* puede verse afectado por el virus de la inflación, de modo que un desmedido uso del castigo criminal devaluará su significado, permitiendo que los miembros de la comunidad no encuentren demasiadas razones para respetarla. Si, además, nos centramos en el terreno que aborda la presente obra, debemos partir de la idea de que la mejor manera de construir un buen Derecho Penal económico es, precisamente, haciendo economía del Derecho Penal.

(*) Profesor Titular de Derecho Penal. Director del Master “Corrupción y Estado de Derecho”, Universidad de Salamanca.

En el marco del control del lavado de activos, sabemos que la frontera que existe entre el Derecho Administrativo y el Derecho Penal no deriva del establecimiento de límites cuantitativos, sino de un reparto de misiones cualitativamente diferenciadas. El Derecho Penal debe castigar a quienes blanqueen fondos de origen delictivo, pero al Derecho Administrativo le está encomendada la tarea de hacer lo posible para que tales actos de blanqueo no lleguen a tener lugar; debe anticiparse al reciclaje de fondos de procedencia ilícita e, imponiendo obligaciones previas de control, cumplir con el consejo que Cesare Beccaria defendía hace ya dos siglos y medio: “es mejor evitar los delitos que castigarlos”.

Los blanqueadores disimulan la procedencia ilegal de los bienes distanciándolos progresivamente de su origen ilegal. A tal efecto, realizan sobre ellos las operaciones económicas que sean precisas para ofrecer la apariencia de que tales ganancias derivan de actividades lícitas o, al menos –interviene en su beneficio el principio de presunción de inocencia–, para que no revelen su procedencia inconfesable. Para ello se valen de los mercados y de los cauces que ofrece la normativa reguladora de la dinámica patrimonial. Ello significa que las operaciones con recursos de procedencia ilícita trascienden más allá de la opacidad fiscal para desarrollarse en el ámbito de la legalidad tributaria, involucrando a un amplio abanico de sujetos económicos que, consciente o inconscientemente, incorporan a su actividad ordinaria los rendimientos derivados de la comisión de actividades. El lavado se viste de compraventa, préstamo, arrendamiento, donación, transferencia, depósito, etc. En consecuencia, objetivo prioritario para las instituciones públicas consiste en vigilar la licitud de esas operaciones, para lo cual se ven en la necesidad de apelar a la ayuda de los profesionales que intervienen en ellas; de imponerles ciertas normas de cuidado y de colaboración cuya infracción queda respaldada por la imposición de sanciones gubernativas. Surge así la figura del sujeto obligado.

Bajo el impulso de diversas iniciativas internacionales, a lo largo de la última década hemos asistido a una auténtica explosión de la regulación tendente a prevenir el blanqueo y, en especial, de la ampliación del cuadro de sujetos obligados. Así lo viene haciendo el FATF-GAFI desde 1990, o la CICAD desde 1992 en la OEA, secundado por otros organismos regionales como GAFIC o GAFISUD, que actúan conforme a criterios similares en sus respectivos ámbitos territoriales; pero fueron los acontecimientos

producidos en Estados Unidos el 11 de septiembre de 2001 los que motivaron la referida ampliación, también focalizada ahora sobre la financiación del terrorismo.

Las primeras normas sobre prevención del blanqueo apenas pensaron en los intermediarios financieros y en otros pocos ámbitos, como el de las entidades de crédito, aseguradoras y otras corporaciones similares. Ya entonces fue notoria la resistencia de estos profesionales, invocando la suficiencia de la autorregulación en cada ramo, pero la progresiva aceptación de estas normas motivó la huida de los blanqueadores hacia otros sectores de actividad económica, desembocando a su vez en la ampliación por parte del Estado del cuadro de sujetos obligados que, muy poco a poco, han venido aceptando que la colaboración con las instancias del control del lavado de activos es imprescindible para el funcionamiento de sus negocios y, en general, para la salud del sistema.

Utilizando una terminología de corte anglosajón comúnmente extendida en Derecho comparado, a esos profesionales no sólo se les pide que ejerzan un mero papel de *gatekeepers*, vinculados al simple deber de abstenerse de intervenir en la ejecución de las operaciones sospechosas que se les soliciten, sino que han de ejercer como *whistleblowers*, denunciando las posibles conductas irregulares ante las autoridades. Tratándose de ciertos profesionales, ese deber activo de colaboración ha sido objeto de intensa controversia, especialmente cuando se ha valorado la especial posición de los abogados, tradicionalmente amparados por su derecho y deber de sigilo profesional. Delimitar lo exigible de lo intangible constituye uno de los principales retos que se nos ofrecen actualmente en este terreno.

Prologar una obra sobre prevención del lavado de activos constituye un reto singular para alguien –como es mi caso– que procede del ámbito criminal. Como ya indiqué anteriormente, las normas de prevención del blanqueo de capitales permiten que el Derecho Penal sea más pequeño, y ese es un efecto extraordinariamente favorable, coherente con los fines que debe perseguir un Estado social y democrático de Derecho. Sabido es que vivimos en una sociedad de riesgos, y que éstos son de la más diversa índole. El Derecho permite peligros, ponderándolos, y en este sentido el con-

trol que ofrece el Derecho Administrativo sobre la esfera del lavado establece pautas de lo que debe ser permitido y de lo que no. A la normativa preventiva del blanqueo de capitales se le encomienda la tarea de gestionar esos riesgos, sabiendo que no puede obsesionarse con su absoluta supresión, toda vez que la intervención masiva sobre el tráfico económico es incompatible con las libertades esenciales del mercado.

Por eso, los dispositivos administrativos de prevención también deben ser valoradas con mesura. Una hipertrofia administrativa ralentiza el funcionamiento de los operadores económicos, dificulta la gestión de la información y, en última instancia, puede llegar a perjudicar el propio desarrollo de las naciones. En consecuencia, ahora que parece aceptarse cada vez con menos reparos la necesidad de contar con la participación de todos esos colaboradores *ex lege*, llega el momento de interiorizar la necesidad de su concurso, concienciarlos de la importancia de su papel en la protección de la integridad de los mercados y, en suma, hacerlos parte activa en la lucha contra el lavado de activos. No se trata de una tarea sencilla; como todo proceso teñido de componentes culturales, no se puede esperar que las cosas cambien de la noche a la mañana. Pero no debemos renunciar a fomentar la capacidad analítica de los operadores, que deben renunciar a las ventajas del corto plazo en beneficio del crecimiento estable y continuado a medio y largo plazo. No se trata de una “simple” cuestión de ética en el marco de las políticas de buen gobierno corporativo, sino de actuar para no sucumbir ante el poder corruptor de las fortunas ilícitas y, en suma, del crimen organizado.

La lucha contra el blanqueo forma parte importante de la defensa de nuestro sistema económico. Las normas de prevención, adecuadamente formuladas, no constituyen una amenaza para el mercado, ni un atentado contra las garantías fundamentales de los individuos. En su justa medida, no constituyen –como algún parlamentario español defendió hace casi dos décadas, durante el trámite de la ya derogada Ley 19/1993– una suerte de “Gestapo financiera”. Más bien, constituyen una nueva cláusula de ese pacto social al que se refirieron los pensadores ilustrados, pero ahora en el contexto de la globalización: una vez más, debemos aceptar la limitación de una parte de nuestras libertades para disfrutar con tranquilidad de las que nos restan.

El trabajo que tengo el honor de prologar es una obra necesaria que se ha resuelto de un modo extraordinario. Describir un denso y enmarañado cuadro normativo como el que aquí se aborda, con una estructura tan coherente como la que se ofrece, constituye un regalo para el estudioso y, sobre todo, una valiosa hoja de ruta para los sujetos obligados e, incluso, para el legislador.

Conozco del rigor de los profesores Francisco Sintura, Wilson Martínez y Fernando Quintana. Desde hace años trabajan en la identificación y análisis de riesgos financieros, extremo que han realizado con la perspectiva que les permite su conocimiento de los temas jurídicos y económicos. Su experiencia y su buen hacer se ofrecen ahora al gran público enmarcando el problema del lavado de activos en su contexto histórico y funcional dentro del sistema jurídico en su conjunto, destacando permanentemente la necesidad de adecuación que todos los países tienen respecto de las iniciativas internacionales sobre la materia.

La lucha contra el blanqueo es compleja y requiere de una notable claridad de ideas acompañada de un importante esfuerzo de especialización. El trabajo que el lector tiene ahora en sus manos proyecta luz sobre un terreno que la precisa y ofrece *expertise* a todos aquellas personas e instituciones que precisan de una ayuda cualificada en este ámbito. Mi más sincera enhorabuena a los autores y mi felicitación a la editorial por haber hecho posible la materialización de este volumen.

Salamanca (España), febrero de 2011

INTRODUCCIÓN

La prevención del lavado de activos como una política de buen gobierno corporativo y de responsabilidad empresarial

Las políticas de “buen gobierno corporativo” (BGC) están orientadas hacia la transparencia, eficiencia y probidad en el desarrollo de los negocios. Constituyen un presupuesto para actuar competitiva y éticamente en los mercados cada vez más integrados. Sin embargo, la falta de transparencia empresarial y la ausencia de buenas prácticas mercantiles, generan obstáculos para el crecimiento y la competitividad de las compañías.

El estudio del concepto “buen gobierno corporativo” (BGC) es relativamente reciente y a principios de la década de los noventa se profundizó en él por los procesos de privatización en Europa Oriental. No obstante, con ocasión de los escándalos de compañías tales como *Enron*, *WorldCom* y *Parmalat*, el tema adquirió relevancia y llamó la atención de los analistas especializados.

En términos generales, el BGC está constituido por un conjunto de prácticas comerciales que se dan en las relaciones entre los administradores sociales y todos aquellos que invierten recursos en la empresa; igualmente, con las prácticas que se deben observar con clientes, proveedores, empleados y órganos de supervisión y control. De este modo, su buen ejercicio conduce a asegurar la transparencia de la administración social, el uso óptimo de los recursos y la probidad de la información financiera y contable.

Los asuntos que abarca el BGC tienen estrecha relación con la vigilancia en la preparación de los estados financieros, la independencia de los au-

idores, la revisión de las compensaciones para los altos ejecutivos, las formas como los individuos son nominados a las altas posiciones, el manejo de los recursos a disponibilidad de los directores y las políticas de distribución de dividendos, entre otras, todo ello en procura de un manejo honesto en la administración de las empresas. Precisamente, cuando las compañías públicas o privadas no adoptan políticas de BGC se suscitan fallas en su información financiera, abuso en los derechos de las minorías, falta de independencia en los órganos de auditoría y de control interno, contratación de personal no idóneo o acuerdos restrictivos de la competencia.

Hace menos de seis años Confecámaras, la agremiación que reúne a las Cámaras de Comercio de Colombia, diseñó un modelo de código de buen gobierno corporativo, como herramienta para las sociedades colombianas que les sirviera para adoptar estándares internacionalmente reconocidos sobre la forma como deben ser administradas. Tal modelo incorpora principios en materia de (i) derechos de los accionistas; (ii) funciones y responsabilidades de los órganos de dirección; (iii) transparencia e integridad de la información; (iv) grupos de interés o de influencia; (v) conflictos de interés; (vi) reglas relativas a las funciones y actividades del ejecutivo principal; y (vii) reglas sobre administración y resolución de controversias, que bien vale la pena adoptar como un instrumento de autorregulación empresarial.

A los anteriores principios se añaden otras recomendaciones que ordinariamente se formulan en materia de responsabilidad social empresarial, política ambiental, protección de la propiedad intelectual, políticas antisoborno y, finalmente, prevención y detección del lavado de activos y la financiación del terrorismo; en el entendido de que el riesgo de tales eventos que se presenten puede producir la posibilidad de pérdida o daño de una empresa, por su propensión 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 terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

No es desconocido que las empresas que adoptan hoy principios orientados a la aplicación de buenas prácticas comerciales procuran la construcción colectiva de postulados éticos, la promoción de pactos de trans-

parencia e instrumentos de autorregulación, como quiera que obrar de manera transparente garantiza la confiabilidad del consumidor y su competitividad.

Por consiguiente, la prevención del lavado de activos y la financiación del terrorismo se convierten en instrumentos de autorregulación para aquellas empresas que no están obligadas por la ley a contar con estándares de protección mínimos, de allí que en el actual estado de cosas resulte más conveniente que aquellas, aún no sometidas a regímenes obligatorios de protección contra el lavado, acojan por vía de la autorregulación medidas orientadas a ese propósito, teniendo en cuenta que la concreción del riesgo de lavado de activos genera desequilibrios entre los deberes y responsabilidades en cabeza de los órganos de Gobierno y produce efectos reputacionales, operativos, legales y de contagio.

La prevención del lavado de activos en las empresas públicas y privadas constituye una buena práctica mercantil y una política de buen gobierno corporativo, si entendemos que hoy en el mundo de los negocios es necesario saber: quién está al otro lado de la mesa, con quién se están realizando actos de comercio y de dónde obtiene sus recursos el otro contratante, lo que antes no era una preocupación relevante. Hoy los negocios están expuestos al riesgo de contagio con una actividad ilícita del crimen organizado y por ello la prevención es la herramienta más apropiada para evitarlo.

Justamente en las actividades del crimen organizado, una de las razones que inducen al delito es la expectativa de obtener en corto tiempo y con el menor esfuerzo posible, un beneficio de lucro significativo. Para alcanzar tales propósitos, la delincuencia debe adoptar mecanismos que no solo le permitan eludir las consecuencias desfavorables derivadas del ilícito, sino que además le garanticen su completa impunidad. Los delincuentes son conscientes que la principal labor de las autoridades es la de encontrar y recaudar la evidencia suficiente para identificar los autores del crimen, así como demostrar su responsabilidad penal. Ellos también son conscientes que algunos bienes obtenidos como producto del delito, dada su trascendencia, llaman la atención de las autoridades al punto que su tenencia o posesión, cuando no se puede justificar debidamente, se convierte en un importantísimo indicio de responsabilidad penal. Es así como los

delincuentes tratan de ocultar los bienes que han obtenido ilícitamente, dándoles una apariencia de legalidad.

Para el alcance de estos propósitos y en el proceso del lavado de activos, la delincuencia requiere reconducir recursos de origen ilícito al círculo económico legal. Para lograrlo se valen en la gran mayoría de los casos del concurso de las personas jurídicas que actúan como intermediarios legales en el mercado financiero, cambiario, bursátil, asegurador, inmobiliario, en el comercio exterior o, en fin, en toda actividad económica que maneje una buena parte de sus recursos en efectivo. Así que la actividad de lavado se desarrolla mediante una sucesión de actos con intervención de diversas personas naturales o jurídicas que cumplen determinada función. Por ello podemos definirlo como el proceso de ocultamiento de recursos o activos de origen ilícito y los subsiguientes actos de simulación respecto de tal origen, para darles apariencia de legitimidad.

Como el lavado de activos se realiza mediante un conjunto de actividades o procedimientos, tal como se anotó, la doctrina internacional sobre la materia ha ideado un método de comprensión y análisis, que consiste en la segmentación del proceso en fases. De los modelos propuestos, el que más ha hecho carrera por haber sido mayoritariamente aceptado entre la comunidad internacional es el del Grupo de Acción Financiera, GAFI (Financial Action Task Force, por sus siglas en inglés, FATF), que divide el proceso de lavado de activos en tres fases. Más allá de las posibles críticas que puedan hacerse al método de división en fases, creemos que en este caso particular, el modelo del GAFI se convierte en un importante recurso metodológico que contribuye no solo a un adecuado entendimiento del fenómeno criminal del lavado de activos, sino también a la apropiada elaboración de un Sistema Integral para la Prevención del Lavado de Activos y de la Financiación del Terrorismo (SIPLA/FT), o conforme con las nuevas recomendaciones del Comité de Basilea II, al Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo (SARLA/FT), siglas que en lo sucesivo adoptaremos.

Según los expertos del GAFI, la primera necesidad del delincuente es llevar el dinero obtenido, producto de un hecho ilícito, a un sitio distinto de aquel en el que se cometió el delito, preferiblemente fuera de la jurisdicción de las autoridades locales –por lo general a otro país–. Con ello se

dificulta la labor de las autoridades y se impide de inmediato, que los grandes volúmenes de dinero llamen la atención de los funcionarios encargados de perseguir el ilícito. A esta secuencia de actos tendientes a llevar el dinero obtenido ilícitamente a un lugar diferente a aquel en donde se cometió el delito se le ha denominado: *fase de colocación*.

Así mismo, cuando se acude al lavado de activos como mecanismo de encubrimiento, se debe a que se ha obtenido ilícitamente una gran cantidad de dinero. Debido al volumen y peso del efectivo a lavar resulta materialmente imposible hacerlo en una sola operación, lo que impone la necesidad de darle apariencia de legalidad de forma gradual y progresivamente en pequeñas cantidades de dinero. Por esta razón, mientras una parte del dinero es maquillado, el resto debe ser encubierto. Ello se hace introduciéndolo en la economía legal –por lo general, pero no exclusivamente, al mercado financiero, cambiario, bursátil, inmobiliario, de comercio exterior o el asegurador– para no levantar sospecha, poniéndolo luego a circular a tal velocidad que sea difícil de rastrearlo por parte de las autoridades. Estos actos constituyen lo que los especialistas del GAFI han llamado: *fase de ocultación*.

Finalmente, los delincuentes dan apariencia de legalidad al dinero, creando una actividad económica, un negocio o una operación comercial que justifique su tenencia, posesión o propiedad. Etapa llamada: *fase de integración*.

Como fácilmente se advierte, resulta muy complejo estructurar un sistema capaz de prevenir el lavado de activos en todas sus fases y en todas sus modalidades. Por ello, cada actividad económica susceptible de una operación de lavado está llamada a segmentar su mercado y diseñar alertas propias que evidencien, con una plataforma tecnológica apropiada, la aparición de operaciones inusuales, no habituales o sospechosas.

Es por ello que la exigencia legal en la mayoría de los países se debe contraer a la obligatoriedad de implementar un SIPLA/FT o un SARLA/FT eficaz, en atención al exacto conjunto de actividades económicas que integran el objeto social de la organización en la cual se va aplicar, y a los procedimientos operacionales específicos que aquella utiliza para el ejercicio de dichas actividades. Esto es, que cada empresa, de

conformidad con la naturaleza de las operaciones que realiza en desarrollo del giro ordinario de sus negocios, debe analizar el tipo de sistema que resulta más eficiente para reducir los riesgos de ser empleada en una operación de blanqueo de capitales.

A manera de ejemplo, si una empresa se dedica al negocio de los seguros debe adoptar un Sistema de Prevención del Riesgo de Lavado de Activos y Financiación del Terrorismo que considere las operaciones regulares de inversión, tales como la compra de derechos a beneficiarios de pólizas de seguros de vida (mercado secundario de pólizas de seguros de vida a enfermos terminales), o la compra de otros seguros que bajo ciertas condiciones ofrecen al inversionista la posibilidad de recuperar las sumas invertidas. En algunos casos, esas inversiones en pólizas de seguros deben cancelarse mediante el pago de sumas de dinero en el exterior, efecto para el cual, además de la inversión, debe llevarse a cabo una operación de compra y transferencia de divisas, las cuales abren la posibilidad de que también se utilicen estos productos para el lavado de activos en *fase de colonización*. En ese evento, lo que ocurre es que el delincuente paga la inversión mediante la transferencia o consignación de las divisas en la cuenta que la compañía aseguradora le indique en el exterior, para lo cual hace uso de los recursos obtenidos ilegalmente. Posteriormente, y apelando a las condiciones de la póliza que le permiten recuperar su dinero, procede a cancelar el negocio solicitando que el reintegro de los recursos se haga mediante el pago, consignación o transferencia, a una cuenta ubicada en un país diferente a aquel en el que se realizó originalmente la inversión. Por esta vía, el delincuente logra sacar del país de origen los recursos obtenidos ilegalmente, dificultando seriamente la labor de las autoridades que investigan el delito.

La legislación colombiana es especialmente prolífica en el control de varias actividades económicas frente a las que viene exigiendo que quienes se dedican de manera profesional a ellas, desarrollen programas efectivos de prevención. Así ocurre frente a: (i) las entidades bajo la vigilancia y control de la Superintendencia Financiera entre las que se cuentan los bancos, las corporaciones financieras, las compañías de financiamiento comercial, los almacenes generales de depósito, las sociedades fiduciarias, las compañías de *leasing*, las sociedades aseguradoras, las casas de cambio, las comisionistas de bolsa de valores, etc.; (ii) las personas que se

dedican a la actividad de comercio exterior; (iii) las que operan como casinos, loterías o ejercen negocios juegos de azar, y (iv) las notarías, entre otras. Sobre este tema nos extenderemos en los capítulos siguientes donde se dará a conocer una amplia legislación dispersa sobre la materia.

Así, si quienes estando obligados a adoptar estos mecanismos de prevención no lo hacen de manera consciente y ocultan el origen ilícito de los recursos, se verán expuestos a investigaciones penales por el delito de lavado de activos, y en otros casos por el de omisión de control, sin perjuicio de las sanciones administrativas, personales o institucionales que pueden ser impuestas por los órganos oficiales de supervisión.

La responsabilidad empresarial en la prevención

Desde ya advertimos que los regímenes normativos que obligan a algunas empresas a adoptar mecanismos de prevención del riesgo de lavado de activos, seguramente serán incluidos en todas las actividades económicas, inicialmente invitándolas a la autorregulación, y posteriormente bajo un régimen de obligación o de deber, en el entendido de que en el mundo de los negocios siempre es necesario conocer quién es la contraparte que se encuentra al otro lado de la mesa. Instrumentar entonces un sistema de prevención del riesgo de lavado de activos, así no exista la obligación legal de hacerlo, constituye una buena práctica mercantil, una conducta diligente y prudente y un mecanismo de autoprotección.

La responsabilidad del empresario por el producto o el servicio que ofrece, es tema actual de aguda controversia en el derecho económico, de cara a la responsabilidad que como garante tiene de conformidad con la estructura constitucional otorgada en la Carta de 1991. Precisamente, la Constitución económica colombiana se erige bajo tres pilares fundamentales: la garantía de la propiedad privada como una función social que implica obligaciones; la libertad económica y de iniciativa privada con responsabilidad, y la libre competencia económica. Ello es consecuencia del carácter intervencionista del Estado en materia económica en procura de la satisfacción del bien común y del derecho de elección que tienen los consumidores frente a la calidad de los bienes y servicios que se les ofrecen.

En desarrollo de este precepto, las autoridades nacionales han dispuesto al interior del régimen legal del comercio un “código de conducta” que obliga al empresario a obrar de buena fe, con absoluta corrección y lealtad y a guardar las precauciones que debe observar un hombre diligente, para evitar que sus empresas y la actividad económica que ejer- cen sean utilizadas por la delincuencia organizada. Pero además, frente a ciertas actividades económicas sujetas a inspección, vigilancia y control como las que tienen que ver con el manejo, aprovechamiento o inversión del ahorro privado, el comercio exterior, los juegos de azar, el cambio de divisas o la rotación de los inmuebles, el Estado ha dispuesto todo un régimen normativo de obligatoria observancia que tiene una finalidad eminentemente profiláctica; es decir, evitar que las herramientas y mecanismos dispuestos por el Estado para facilitar el intercambio económico sean utilizados por la delincuencia, para realizar operaciones de lavado de activos. Este conjunto normativo se encuentra dispuesto en decretos y circulares externas relativas a la prevención del lavado de activos emitidas por la Superintendencia Financiera, la Dirección de Impuestos Nacionales y el Instituto de Comercio Exterior. La Superintendencia de Notariado y Registro, la Superintendencia de Sociedades, ETESA, entre otras, han proferido una imbricada regulación al respecto. Por ello, simplemente para sintetizar y a manera de comentario, debemos decir que ellas imponen a las entidades a las que les es aplicable, la obligación de crear un sistema administrativo de profilaxis criminal que contenga los mecanismos de control allí especificados, y que se orienten a ejercer una verdadera prevención de actividades delictivas desde el seno de la organización.

De manera general, el régimen administrativo de prevención del lavado de activos y la financiación del terrorismo en materia financiera, cambiaria, bursátil y aseguradora será materia de estudio detallado en el capítulo siguiente. No obstante podemos señalar preliminarmente algunos elementos que se constituyen en buenas prácticas mercantiles, que resultan recomendables adoptar como políticas empresariales en aquellas compañías que no pertenecen a estos mercados o que no están actualmente sujetas a obligatoria regulación, en el entendido que constituyen buenas prácticas de autorregulación y autoprotección:

1. Instrumentos aplicables para obtener la información tendiente a conocer el cliente y el mercado, tales como formularios, certificaciones y

constancias exigidas a las personas con quienes se tienen relaciones comerciales, *software*, etc.

2. Parámetros para calificar la operación de un cliente como sospechosa.

3. Medidas que deben tomar en cuenta los empleados, administradores y directivos cuando se encuentren frente a una operación sospechosa de un cliente.

4. Asignación de la responsabilidad de cada uno de los empleados, administradores y directivos en relación con los procedimientos, instrumentos y mecanismos aplicados a la estructura orgánica de la empresa para la prevención de las actividades delictivas desde su seno.

5. Cláusulas contractuales de salvaguarda, en las que se manifieste bajo la gravedad del juramento que todos los efectos necesarios para ejecutar el contrato, y en particular el dinero con que se pagará el precio, tienen origen lícito.

6. La designación de un funcionario de prevención que dirija su actividad a verificar el cumplimiento de cada una de las disposiciones del manual de procedimientos, y en especial del SIPLA/FT, quien además de ejercer una función de vigilancia ha de tener la tarea de realizar estudios criminalísticos y criminológicos que permitan incrementar la seguridad de la empresa frente a los intentos de la delincuencia de utilizarla para ejecutar actividades ilícitas. Del mismo modo ha de rendir informes periódicos a los órganos directivos de la empresa, acerca de los logros y fallas en materia de prevención de actividades delictivas a través de la compañía; y tener un contacto permanente y directo con las autoridades nacionales que ayuden a conservar y garantizar la legalidad de las operaciones externas de la empresa.

7. La detección y reporte de operaciones sospechosas, efecto para lo cual es indispensable entender que a la entidad le conviene extender sus controles hasta restringir cualquier operación, de la cual se pueda siquiera llegar a pensar que el cliente, proveedor o distribuidor se está valiendo de la relación comercial para realizar actividades delictivas. Este aspec-

to es esencial para cualquier comerciante que pretenda mantener imponente su nombre comercial y su imagen corporativa, pues determinar cuándo una persona con quien se tienen relaciones comerciales está involucrada en actividades no muy legales le permite a la empresa alejarse y conservar una distancia prudente con la delincuencia, de modo que jamás pueda ser señalada como autora o partícipe de hechos punibles. Máxime si se considera que verse involucrada en investigaciones penales, aun cuando no se tenga ninguna responsabilidad, ocasiona la pérdida de importantes relaciones comerciales.

8. Derivado de la política nacional de prevención del lavado de activos, es conveniente no tener relación alguna con personas inmersas en investigaciones penales que tengan que ver con alguna de las modalidades de crimen organizado, es decir: narcotráfico, secuestro, extorsión, terrorismo, genocidios, concierto para delinquir, tráfico de insumos químicos, de armas, de menores, de material nuclear, de inmigrantes, trata de personas, lavado de activos, etc.

9. La inclusión de cláusulas en las que se obligue al contratante a adoptar medidas mínimas de prevención para evitar que el producto sea adquirido con recursos de origen ilícito.

10. Normas internas que contribuyan a liberar a los funcionarios de la empresa de cualquier responsabilidad civil o penal futura cuando reportan una operación como sospechosa.

11. La fijación de cláusulas que otorguen el derecho a verificar que el cliente dentro del proceso de comercialización esté aplicando efectivamente un SIPLA/FT que cuente con todos los elementos necesarios y suficientes para evitar que el producto sea adquirido con recursos de origen ilícito.

12. La inclusión de cláusulas que otorguen la facultad de terminar unilateralmente un contrato, cuando se determine que el contratante no aplica un SIPLA/FT que cuente con todos los elementos necesarios y suficientes para evitar el riesgo de lavado de activos.

13. La inclusión en los procesos de auditoría o control de la verificación del cumplimiento de las normas administrativas sobre preven-

ción de lavado de activos, y la adecuada aplicación del SIPLA/FT frente a los inversionistas del producto. Este debería quedar consignado como un punto específico, independiente y adicional en todas las auditorías o controles.

14. Elaborar un *Manual de prevención de lavado de activos*, en el cual se relacionen detalladamente las políticas, los procedimientos, los criterios y los mecanismos adoptados por la entidad para prevenir dicho delito.

15. Adoptar los mecanismos necesarios para que, con independencia de los procesos de conocimiento del cliente adoptados por el contratante, también confirme y actualice periódicamente la información consignada en el formulario de apertura del plan y en la declaración de origen de fondos.

16. Asignar a un funcionario de la entidad –o designar un funcionario especial para ese efecto– la labor de verificar el cumplimiento del *Manual de prevención* que se redacte, así como de promover la adopción de nuevas políticas, procedimientos, criterios y mecanismos para la prevención del lavado de activos.

17. Adelantar, dejando constancia de ello, un programa de capacitación en materia de prevención de lavado de activos, dirigido a la *totalidad* de los funcionarios de la compañía.

18. La emisión periódica de circulares, memorandos o notas internas, en las que se recuerde e insista a los funcionarios de la entidad la necesidad de prevenir el lavado de activos.

19. La inclusión dentro del proceso de contratación de personal, un breve estudio de seguridad que permita a la compañía confiar que sus nuevos empleados no utilizarán la organización para facilitar la comisión de hechos punibles.

20. Exigir que junto con la declaración de origen de fondos (DOF), el solicitante aporte documentación que razonablemente permita confirmar la información allí consignada.

21. La emisión periódica de comunicaciones a las personas encargadas de comercializar sus productos informándoles de nuevas modalidades de lavado de activos que afectan los productos, junto con las señales de alerta que permitan identificar y evitar esas conductas.

22. Incluir dentro del contrato una cláusula que permita el derecho a terminar unilateralmente el negocio, si surgen sospechas o dudas sobre la licitud del dinero o recursos con que se están cancelando las obligaciones por parte del tomador del plan.

23. En caso de cambio de inversionistas, diseñar procedimientos para asegurar que este nuevo tomador será sometido a los mecanismos de conocimiento del cliente existentes para cualquier inversionista que desee acceder al plan.

24. Exigir que en todo caso, el pago de las obligaciones se haga mediante cheque o transferencia bancaria, pero nunca en efectivo o mediante consignación de efectivo en las cuentas de la compañía. Ello como un control adicional, pues si los recursos salen directamente de una institución financiera, es ella quien debe tener los controles para la prevención del lavado de activos como una garantía adicional de la licitud de los mismos.

25. Exigir a las personas encargadas de comercializar el producto que cuando este sea tomado por una persona jurídica, el control del conocimiento del cliente incluya también una verificación de los accionistas y de los funcionarios de dirección, control y manejo de la misma.

PRIMERA PARTE

Marco jurídico de la prevención del lavado de activos y la financiación del terrorismo

La prevención del riesgo de lavado de activos en la actividad comercial es una política de buenas prácticas comerciales, imprescindible en el mundo globalizado y de indiscutible incorporación en el código de buena conducta de los empresarios y comerciantes.

El trabajo que se aborda no constituye una revisión de los aspectos jurídicos de la norma penal, sino de aquellos administrativos y de orden comercial que le dan sustento, en cuanto su debido cumplimiento evita el riesgo de exposición a una investigación criminal por conductas activas o de omisión, que pueden sancionarse en atención a la posición de garante que asumen los empresarios o comerciantes, por los cursos de acción o de peligro que se ocasionen cuando debiendo haber observado un régimen preventivo, no lo hacen de manera consciente o por omisión del deber objetivo de cuidado. Igualmente, contiene recomendaciones importantes para iniciar un proceso preventivo en las empresas no vigiladas por las autoridades de supervisión y control, que conduzca a edificar una cultura de precaución y de administración del riesgo de lavado de activos.

En el marco teórico asumimos como concepto fundamental, que el lavado de activos⁽¹⁾ o blanqueo de capitales, es el proceso delictivo de ocul-

(1) El delito de lavado de activos se encuentra tipificado en los artículos 323 y 324 del Código Penal Colombiano: “ART. 323—**Lavado de activos**. El que adquiera, resguarde, invierta, transporte, transforme, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, delitos contra el sistema financiero, la administración pública, o vinculados con el producto de los delitos objeto de un concierto para delinquir, relacionadas con el tráfico de

tamiento de activos o de recursos provenientes de actividades ilegales y los subsiguientes actos de simulación para darles apariencia de legalidad y ocultar su origen, tal como ya se había señalado *supra*.

Inicialmente se asoció el fenómeno del lavado de activos al tráfico ilícito de sustancias estupefacientes o sicotrópicas, por cuanto la Convención de Viena de 1988 contra el narcotráfico, obligaba a los países miembros a la tipificación autónoma de este delito en sus legislaciones internas⁽²⁾. Sin

(Cont. nota 1)

drogas tóxicas, estupefacientes o sustancias sicotrópicas, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre tales bienes, o realice cualquier otro acto para ocultar o encubrir su origen ilícito incurrirá, por esa sola conducta, en prisión de seis (6) a quince (15) años y multa de quinientos (500) a cincuenta mil (50.000) salarios mínimos legales mensuales vigentes.

La misma pena se aplicará cuando las conductas descritas en el inciso anterior se realicen sobre bienes cuya extinción de dominio haya sido declarada.

El lavado de activos será punible aun cuando las actividades de que provinieren los bienes, o los actos penados en los apartados anteriores, se hubiesen realizado, total o parcialmente, en el extranjero.

Las penas privativas de la libertad previstas en el presente artículo se aumentarán de una tercera parte a la mitad cuando para la realización de las conductas se efectuaren operaciones de cambio o de comercio exterior, o se introdujeren mercancías al territorio nacional.

El aumento de pena previsto en el inciso anterior, también se aplicará cuando se introdujeren mercancías de contrabando al territorio nacional.

ART. 324—Circunstancias específicas de agravación. Las penas privativas de la libertad previstas en el artículo anterior se aumentarán de una tercera parte a la mitad cuando la conducta sea desarrollada por quien pertenezca a una persona jurídica, una sociedad o una organización dedicada al lavado de activos y de la mitad a las tres cuartas partes cuando sean desarrolladas por los jefes, administradores o encargados de las referidas personas jurídicas, sociedades u organizaciones”.

(2) El artículo 3º de la Convención de Viena de 1988 dispone: “**Artículo 3º—Delitos y sanciones.** 1. Cada una de las partes adoptará las medidas que sean necesarias para tipificar como delitos penales en su derecho interno, cuando se cometan intencionalmente: [...]

b) i. la conversión o la transferencia de bienes a sabiendas de que tales bienes proceden de alguno o algunos de los delitos tipificados de conformidad con el inciso a) del presente párrafo, o de un acto de participación en tal delito o delitos, con objeto de ocultar o encubrir el origen ilícito de los bienes o de ayudar

(Cont. nota 2)

embargo, es una actividad propia de la delincuencia organizada, que extiende sus alcances a otras modalidades como el tráfico de insumos químicos, de órganos humanos, de inmigrantes, de materiales nucleares, a la trata de personas, el contrabando, la corrupción, el secuestro, el terrorismo, la extorsión, etc.

El lavado de activos que en la legislación penal colombiana se ubica dentro de aquellos delitos que tutelan el orden económico y social como bien jurídico materia de protección, sanciona la sola probabilidad de lesión o de daño, en cuanto el Legislador entiende que es necesario intervenir tipificando una conducta que supone un riesgo, sin necesidad de esperar a que este se concrete, en la medida que la sociedad actual en la que vivimos tiene al “lavado de activos” como una conducta además asociada a varias formas de criminalidad organizada.

a cualquier persona que participe en la comisión de tal delito o delitos a eludir las consecuencias jurídicas de sus acciones;

- ii. la ocultación o el encubrimiento de la naturaleza, el origen, la ubicación, el destino, el movimiento o la propiedad reales de bienes, o de derechos relativos a tales bienes, a sabiendas de que proceden de alguno o algunos de los delitos tipificados de conformidad con el inciso a) del presente párrafo o de un acto de participación en tal delito o delitos;
- c) a reserva de sus principios constitucionales y a los conceptos fundamentales de su ordenamiento jurídico:

- i. la adquisición, la posesión o la utilización de bienes, a sabiendas, en el momento de recibirllos, de que tales bienes proceden de alguno o algunos de los delitos tipificados de conformidad con el inciso a) del presente párrafo o de un acto de participación en tal delito o delitos;
- ii. la posesión de equipos o materiales o sustancias enumeradas en el Cuadro I y el Cuadro II, a sabiendas de que se utilizan o se habrán de utilizar en el cultivo, la producción o la fabricación ilícitos de estupefacientes o sustancias sicotrópicas o para tales fines;
- iii. instigar o inducir públicamente a otros, por cualquier medio, a cometer alguno de los delitos tipificados de conformidad con el presente artículo o a utilizar ilícitamente estupefacientes o sustancias sicotrópicas;
- iv. la participación en la comisión de algunos de los delitos tipificados de conformidad con lo dispuesto en el presente artículo, la asociación y la confabulación para cometerlos, la tentativa de cometerlos, y la asistencia, la incitación, la facilitación o el asesoramiento en relación con su comisión”.

No es necesario por tanto acreditar una vulneración efectiva del orden económico y social considerado como el conjunto de instrumentos de que está dotado el Estado para regular su intervención conforme con los lineamientos de la Constitución económica, sino la sola puesta en peligro; y ello ocurre, porque desde sus orígenes, la teoría del delito se edificó desde la perspectiva de los delitos de lesión y el “lavado de activos”, es de aquellos llamados *de peligro*, frente a los que no hay un resultado lesivo sensorialmente perceptible, sino una amenaza concreta o, cuando menos hipotética, de vulneración al bien jurídico tutelado por la norma penal. Su tipificación como delito de peligro es pues resultado de la actual situación de “objetiva inseguridad”, que obliga al Legislador a intervenir antes de que una lesión al interés jurídico se concrete.

La ley presume de derecho que la realización de cualquiera de las conductas descritas por el artículo 325 del Código Penal colombiano, genera un riesgo, un peligro “hipotético”, ya que al definirse la conducta en cada uno de los verbos rectores que la integran, es necesario además que esta resulte idónea para ocultar o encubrir el origen ilícito de los recursos.

Este contexto introductorio nos sirve para profundizar en el marco normativo, no penal, que resulta ser el foco de nuestra atención.

Una de las dificultades más sobresaliente en la lucha contra el lavado de activos es la detección del hecho punible. Por su naturaleza, este delito es de aquellos que algún sector de la doctrina califica como de *daño cumulativo*, y que se caracteriza porque su desvalor como conducta sólo se comprende a merced de “una valoración acerca de cuál sería la trascendencia global de un género de conductas, si es que éste se estima lícito. En otras palabras, la pregunta clave es: ‘¿Qué pasaría si todos los intervenientes en este sector de actividad realizaran la conducta X cuando existe, además, una seria probabilidad de que muchos de ellos lo hagan, de ser estimada lícita?’”⁽³⁾. A esta cualidad particular del delito de lavado de activos puede atribuirse la dificultad para su detección, pues de un

(3) Silva Sánchez, Jesús-María. *La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales*. Madrid, Ed. Civitas, 1999, p. 104.

lado sus consecuencias se hacen prácticamente imperceptibles para la comunidad, lo que reduce las probabilidades de que las autoridades tengan noticia sobre su ocurrencia mediante una denuncia, y de otro lado, la detección de la conducta constitutiva del delito sólo puede lograrse cuando se cuenta con toda la información necesaria para poder llevar a cabo una valoración completa de contexto, a la que tampoco tienen permanente acceso las autoridades.

Respecto a las dificultades relacionadas con la detección del lavado de activos importa destacar que el proceso de tecnificación, que ha acompañado las nuevas formas de delincuencia propias de las sociedades postindustriales, ha impuesto a las autoridades el reto de desarrollar nuevas técnicas en materia de investigación criminal para combatirlas. En el proceso de dicho desarrollo llegó un momento en el que los organismos de policía judicial descubrieron, que “sería sumamente útil seguir la pista tanto de las utilidades provenientes de actividades ilegales, como de la actividad misma”⁽⁴⁾. Técnica cuya eficacia quedó suficientemente demostrada “cuando los cargos por extorsión no pudieron sostenerse en el proceso contra Al Capone, [y] el fiscal tuvo que recurrir al cargo de evasión de impuestos”⁽⁵⁾. Sin embargo, la efectividad de la persecución del delito mediante el rastreo de las utilidades depende “de la disponibilidad de archivos e información financiera”⁽⁶⁾, motivo por el cual la banca cumple un papel fundamental en la ejecución de la política criminal del Estado.

Las legislaciones *antilavado* en el mundo se han inspirado en la idea de que para combatir este delito hay que detectarlo, y que esta detección sólo es posible si los intermediarios del mercado financiero –que es el ambiente idóneo para la comisión de este tipo de conductas– informan a las autoridades sobre cualquier operación sospechosa. Al fin de cuentas, “la

(4) Gay, Phillips, “Acciones gremiales en la lucha contra el lavado de activos en los Estados Unidos de América”, En: *Memorias del III Congreso de Administración del Riesgo* organizado por la Asobancaria en Rionegro entre el 14 y 15 de noviembre de 1996, p. 53.

(5) Gay, p. 54.

(6) Ibíd.

que más conoce las sospechas o la realidad económica de las operaciones es la propia entidad”⁽⁷⁾. Por esta razón, el Estado francés creó el 9 de mayo de 1990 un servicio administrativo denominado “Tratamiento de la Información y Acción contra los Circuitos Financieros Clandestinos” (Tracfin, por sus siglas en francés), que se constituiría como el organismo precursor de la inteligencia financiera especializada en materia de lavado de activos. Anticipando lo que en los siguientes cinco (5) años sería el modelo general de prevención de lavado de activos en el mercado financiero, la ley francesa antilavado del 12 de julio de 1990 impuso a las entidades bancarias la obligación de no solo levantar el secreto bancario, sino de informar al Tracfin sobre toda transacción que consideraran sospechosa, ofreciendo los datos relativos a la cuantía de la operación y la identidad de los sujetos que en ella interviniieran⁽⁸⁾.

De la importancia que tiene la banca en la persecución del lavado de activos se percató la comunidad latinoamericana desde 1990, cuando la Organización de Estados Americanos, OEA, por intermedio de la Comisión Interamericana para el Control y Abuso de Drogas, CICAD⁽⁹⁾, se “dio cuenta de la magnitud del negocio del tráfico de drogas y decidió tomar medidas, recomendando que los países del hemisferio aprobaran legislaciones que interfirieran con esas transacciones de comercio”⁽¹⁰⁾. A esos efectos, las recomendaciones de la CICAD se enderezaron a proponer la adopción de legislaciones que dispusieran de tres elementos básicos: “El primero, es la sugerencia de la criminalización y penas para el lavado de activos, incluyendo el decomiso de las ganancias del delito; el segundo, medidas para que las instituciones financieras prevengan la ocurrencia del

(7) García, Jean-Paul, “Objetivos administrativos y operativos de Tracfin”, En: *Memorias del III Congreso de Administración del Riesgo* organizado por la Asobancaria en Rionegro entre el 14 y 15 de noviembre de 1996, p. 71.

(8) En este sentido, cfr., García, p. 73.

(9) Sobre la CICAD, cfr. Sullivan, Michael, “Acciones y recomendaciones para la prevención del lavado de activos”, En: *Memorias del III Congreso de Administración del Riesgo* organizado por la Asobancaria en Rionegro entre el 14 y 15 de noviembre de 1996, p. 63), quien comenta que este organismo “Se creó como resultado de una conferencia especializada de la OEA en 1986, que analizaba el problema del tráfico de drogas y delitos conexos en el hemisferio”.

(10) Sullivan, p. 64.

lavado de dinero en sus instituciones; y, el tercero, medidas para fortalecer la cooperación internacional”⁽¹¹⁾.

En esta materia, el Gobierno de Estados Unidos de América fue pionero mediante la aprobación del Acta de Reserva Bancaria durante la administración de Richard Nixon, la cual concedía a las autoridades de policía “libre acceso a cierta información clave, considerada como ‘altamente útil para efectos de investigaciones, y para asuntos penales, impositivos y regulatorios’”⁽¹²⁾. Con fundamento en esta Acta, “el Congreso autorizó al Departamento del Tesoro para que dictara las reglas que establecieron el marco en el cual operan en la actualidad los bancos americanos y otras entidades no financieras. La esencia de dichas regulaciones se encuentra en el Código Americano de Regulaciones Federales, Título 31, Parte 103 A”⁽¹³⁾.

Desde 1996 y con fundamento en esta legislación se hizo obligatorio para los bancos estadounidenses, la presentación de Informes de Actividades Sospechosas (*Suspicious Activity Reports*, por sus siglas en inglés, SAR), cuyo contenido está definido por dos tipos de consideraciones imprescindibles: la primera consiste en establecer si la operación tiene un propósito comercial razonable, y la segunda si el banco está o no en condiciones de determinar si existe una explicación legítima para la operación. En el evento en que una operación realizada por un banco parezca no tener una explicación, y se establezca así mismo que la entidad no cuenta con los medios necesarios para investigarla más a fondo, se hace obligatorio para ella la presentación de un informe de actividades sospechosas de conformidad con lo establecido en el Código Americano de Regulaciones Federales emitido por el Departamento del Tesoro⁽¹⁴⁾.

A la luz de la propia Acta de Reserva Bancaria, en concordancia con el Código Americano de Regulaciones Federales emitido por el Departamento del Tesoro, “el banco no puede discutir el informe con ninguna persona, y por ningún motivo podrá notificar al cliente, empleado o a cualquie-

(11) Sullivan, p. 64.

(12) Gay, p. 54.

(13) Ibíd.

(14) En este sentido, cfr., Gay, p. 54.

ra sobre quien recaiga el informe. Eso constituye la base para garantizar al banco protección contra una posible demanda civil de un cliente (quien no estará enterado de la existencia del informe)⁽¹⁵⁾. Además, como ocurre en Colombia, en Estados Unidos de América el informe de actividades sospechosas no se dirige a los organismos encargados de adelantar las investigaciones penales (Fiscalía, FBI o la policía estatal), sino que debe presentarse a un organismo técnico especializado creado con el propósito principal de brindar apoyo a la lucha contra el delito mediante el desarrollo de actividades de inteligencia financiera, como lo es la *Financial Crimes Enforcement Network, FinCEN*, con sede en Washington D.C. Esta circunstancia, al igual que ocurre en nuestro país, permite diferenciar el informe de actividades sospechosas de una denuncia penal, con la consecuencia colateral de que no es posible atribuir a la entidad financiera por virtud del informe, la misma responsabilidad que cabría predicar de un particular que formula una denuncia penal contra otro⁽¹⁶⁾.

(15) Gay, p. 60.

(16) La comunidad internacional ha entendido que el mejor aliado del Estado en la lucha contra la delincuencia organizada es la banca, puesto que su posición en la sociedad le permite el conocimiento de información a la que normalmente las autoridades no están en condiciones de acceder, o no tienen la capacidad de procesar. Para que el Estado se pueda apoyar en las instituciones financieras, llegando incluso a imponerles cargas que no corresponden necesariamente al giro ordinario de sus negocios tal como lo es el reportar operaciones sospechosas, político-criminalmente, debe forjar relaciones de mutua confianza para que pueda existir un flujo dinámico de información. Como consecuencia fundamental de esta relación de confianza, surge la necesidad de exoneración de responsabilidad para las entidades financieras por los reportes de operaciones sospechosas que presenten, lo cual motiva a la institución a colaborar activamente con el Estado. Las autoridades judiciales deben ser conscientes de que en la lucha efectiva contra la delincuencia organizada, se requiere imponer a las instituciones financieras la no liviana carga de anteponer la prevención del delito a la obtención de sus legítimas metas comerciales. Y ello es así incluso en materia de reporte de operaciones sospechosas, pues cuando una entidad informa de una operación, en el fondo lo que está haciendo es dar elementos para que la autoridad de persecución penal inicie una investigación que puede generar perjuicios para uno de sus clientes. Si se toma en cuenta que el éxito económico de una entidad financiera depende en todo de sus clientes, y que por consiguiente es a ellos a quienes se debe, si quiere mantener un nivel de competitividad en el mercado, entonces se comprende que exigir a una entidad financiera que reporte operaciones de sus clientes en realidad supone pedir una acción contraria a la lógica
(Cont. nota 16)

Este esquema de exoneración de responsabilidad para la entidad reportante también existe en la legislación francesa, donde incluso se le impone la obligación de continuar sosteniendo la relación comercial con el cliente para evitar que advierta la circunstancia y entorpezca la investigación⁽¹⁷⁾. En efecto, en la legislación francesa “la declaración de sospecha sí exime de la responsabilidad, pero no significa que el banco se desentienda de la relación que se mantiene con la persona que ha hecho la declaración de sospecha. Por ley, el banco tiene que seguir el funcionamiento de la cuenta, si de ello se trata, o las consecuencias de las operaciones; si se trata de sacar dinero de la cuenta, el banco debe interesarse por el destino de estos fondos; si es efectivo, no se puede hacer el seguimiento, pero si es transferencia sí”⁽¹⁸⁾. Más aún, en la legislación francesa la exoneración de responsabilidad opera aun cuando la declaración de sospecha no es institucional sino que es presentada por el funcionario competente dentro de la entidad financiera. Tan nítida es la diferencia entre una denuncia penal y la declaración de sospecha en la legislación francesa, que desde “el 29 de enero de 1993, en el marco de una ley muy general de prevención y represión de la corrupción y transparencia de la vida política en Francia, se introdujo un artículo que modifica e implementa la ley inicial de 1990, en el cual se dice que la declaración de sospecha de una entidad obligada puede incluso ser verbal y que esta entidad puede pedir a Tracfin que no se man-

económica. Todo ello reforzado además por el hecho de que el reporte de operaciones sospechosas no genera tantos beneficios como costos a las instituciones financieras, siendo el Estado y la sociedad en general el único beneficiario de sus efectos. Es por ello que la buena voluntad de la banca en la lucha contra la delincuencia debe ser cultivada y recompensada por el Estado, quien para ello debe fomentar el sentimiento de confianza de los intermediarios hacia las autoridades, ofreciéndoles como mínimo la tranquilidad de saber que no serán perjudicados por el hecho de colaborar en la lucha contra el delito, mediante el reporte de operaciones que puedan parecer sospechosas.

(17) En Francia las autoridades han entendido que “la ley crea obligaciones referentes a entidades obligadas, no obligaciones referentes a Tracfin; después crea garantías, pero se ha deducido que entre Tracfin y los bancos o las entidades obligadas se debe mantener una relación fluida y de total confianza. Tracfin siempre responde favorablemente cuando un banco le presenta su plan de control interno; no es que haya una obligación de visado, sino que se hace así en la relación de confianza. Esto no supone que Tracfin tenga una responsabilidad en la aplicación de los planes, pero sí un compromiso de confianza con el banco” (García, p. 75).

(18) García, p. 75.

de acuse de recibo”⁽¹⁹⁾.

Por otra parte debe agregarse, que en la actualidad es dominante la tesis de que el lavado de activos no constituye solamente un delito que atenta contra el orden económico y social, sino que ya es considerado un problema que atañe a la seguridad nacional. Esta consideración llevó a las autoridades de diferentes países a diseñar e implementar una estrategia integral contra el blanqueo de capitales, que incluyó no sólo la penalización de la conducta, sino también la promulgación de una legislación que obliga a las entidades financieras a adoptar un sistema de controles especiales para la prevención del lavado de activos y la financiación del terrorismo, incluidos el levantamiento del secreto bancario, así como regulaciones en materia de comiso de bienes y cooperación judicial internacional.

En el caso de Estados Unidos de América, desde la promulgación del Acta de Reserva Bancaria se impuso a las entidades financieras una serie de obligaciones tendientes a la adopción de controles para impedir el acceso al sistema financiero de “ciertos elementos indeseables, específicamente aquellos individuos y organizaciones involucradas en actividades ilegales”. Por su puesto, la finalidad de dichas medidas es evitar que la delincuencia pueda aprovecharse de la infraestructura creada por el Estado y por los agentes del mercado para facilitar el intercambio económico lícito, en beneficio de sus propósitos lesivos para la sociedad⁽²⁰⁾. Esto significa que en la legislación estadounidense, como ocurre también en la mayoría de las legislaciones de Europa y América, las obligaciones de las entidades financieras en materia de prevención de lavado de activos y fi-

(19) García, p. 75.

(20) En relación con esto debe precisarse que la obligación de informar actividades sospechosas, no se relaciona de manera directa con el propósito de evitar que las entidades financieras sean utilizadas para canalizar recursos de origen ilícito, sino con la finalidad de suministrar a las autoridades más y mejor información acerca de los movimientos de los recursos provenientes de actividades ilícitas, en orden a facilitar la investigación criminal de las mismas. Dicho en otras palabras, el informe de actividades sospechosas, a diferencia de otros controles, como por ejemplo, los mecanismos de conocimiento del cliente o la adopción de manuales de procedimientos, no es una institución creada para proteger a los intermediarios financieros, sino para proporcionar a las autoridades la información necesaria para la detección y represión penal del delito.

nanciación del terrorismo no se contraen únicamente al reporte de operaciones sospechosas, sino que abarcan la implementación de un sistema de controles que cierre las puertas del sistema económico regular a los capitales de origen ilícito.

En el caso colombiano, la constitucionalidad del régimen que impone a las entidades financieras la obligación de adoptar estos costosos sistemas de prevención se basa, en que existen valores superiores cuya protección y realización constituye un deber de todos los ciudadanos. Sobre este particular ha sostenido la Corte Constitucional lo siguiente:

“Uno de los pilares fundamentales está constituido por el trabajo. La Constitución reconoce y ampara la propiedad obtenida con base en el mérito y el esfuerzo que el trabajo implica, y se lo desestimula en alto grado si se admitiera, que sin apelar a él, de modo fácil, por fuera de escrúpulos y restricciones, puede obtenerse y acrecentarse el patrimonio familiar.

Lo propio tiene que afirmarse de la libertad de empresa, de la actividad económica y de la iniciativa privada, aseguradas dentro de nuestro sistema dentro de los límites del bien común y bajo el supuesto de las obligaciones y los compromisos que implica su función social. La industria, el comercio, la producción agrícola y ganadera, la intermediación financiera, la gestión empresarial en sus diversas modalidades, razonable y lícitamente ejercidos, son factores de desarrollo que la Constitución protege, y fuente legítima de progreso y bienestar para quien se ocupa de ellos. En cambio, el montaje de empresas delictivas, la ejecución de actos con objeto ilícito, el saqueo del tesoro público, el negocio basado en la corrupción, la ganancia obtenida en abierta oposición a los valores jurídicos y éticos que la comunidad profesa son extraños al orden constitucional, atentan contra él y conspiran gravemente contra la pacífica convivencia y contra el bien común y privado, por lo cual no pueden acogerse a sus garantías ni contar con su protección”⁽²¹⁾.

(21) Corte Constitucional, Sentencia C-374 de agosto 13 de 1997.

Así pues, una adecuada interpretación de las normas que imponen la obligación de prevenir el lavado de activos y la financiación del terrorismo no puede omitir la referencia a la función político-criminal que cumplen, consistente en asegurar la detección de los dineros ilícitos que ingresan al circuito económico, para realizar valores como el trabajo, la libertad, la igualdad y la propiedad obtenida con base al mérito, sobre los que se construye el paradigma de sociedad que queremos llegar a ser.

CAPÍTULO 1

Retrospectiva en el derecho colombiano⁽¹⁾

Hablar de “lavado de activos” es hablar de un fenómeno delictivo cuyos orígenes conocidos se remontan al “Chicago de los años veinte”⁽²⁾. Sin embargo, la creación de instrumentos jurídicos específicamente diseñados para combatir esta modalidad delictiva resultan notablemente más recientes, cuando sólo hasta la década de los ochenta comienza a observarse un importante movimiento internacional orientado hacia la tipificación del lavado de activos como un delito autónomo, y hacia el incremento de los medios existentes para la persecución de estas conductas.

En nuestro país, la asunción de compromisos internacionales por parte del Estado en materia de lucha contra el narcotráfico fue la causa más importante –aunque no la primera–, que determinó la adopción de herramientas jurídicas específicamente orientadas a la prevención del lavado de activos. En efecto, “con ocasión de la aprobación por el órgano legislativo nacional, de la Ley 67 de 1993, por la cual se aprueba la Convención de las Naciones Unidas Contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas, suscrita en Viena el 20 de diciembre de 1988, Colombia adquirió el compromiso de tipificar en su legislación interna, una se-

-
- (1) Una relación histórica de las normas aplicables en Colombia en materia de prevención del lavado de activos desde el año de 1991 hasta la fecha, puede consultarse en el Concepto 2008040595-001 del 24 de junio de 2008, emitido por la Superintendencia Financiera.
 - (2) L'Express, “Así opera el lavado mundial de dineros sucios”, En: *Revista Summa*, ed. 86, p. 56. Donde también se explica que: “en aquella época, un ‘financista’ compraba una cadena de lavanderías automáticas, donde no se paga sino en efectivo. Cada noche, no tenía más que agregar dinero sucio a las ganancias del día. Antes de declarar al fisco, el dinero era blanqueado de esa forma”.

rie de conductas relacionadas con el narcotráfico en sus diferentes etapas, una de las cuales es la del blanqueo de los capitales ilegales”⁽³⁾. Aunque la atención de las obligaciones adquiridas con la comunidad internacional tardó casi cuatro años, la introducción del lavado de activos en el catálogo de conductas punibles ha constituido uno de los más importantes progresos del Estado colombiano en la lucha contra la delincuencia organizada. Por lo que es importante destacar, que hasta antes de la expedición de la Ley 365 de 1997 –norma en la que por vez primera se tipificó autónomamente la conducta–, los comportamientos que hoy se encuentran descritos en el tipo penal de lavado de activos sólo podían ser prevenidos “por la vía del enriquecimiento ilícito (Decreto de Estado de Sitio 1985 de agosto 24 de 1989, convertido en legislación permanente por el D. 2266 de 1991), el testaferrato (art. 6º del D. 1856 de agosto 18 de 1989, convertido en legislación permanente por el D. 2266 de 1991) o los delitos de favorecimiento y receptación (arts. 176 y 177 del Código Penal)”⁽⁴⁾.

La descripción que en aquel entonces se le dio al lavado de activos no fue únicamente producto de la discusión sostenida en el desarrollo de los debates parlamentarios, sino que el texto de la norma estuvo profundamente influenciado por el *Reglamento Modelo sobre Delitos de Lavado Relacionados con el Tráfico Ilícito de Drogas y Delitos Conexos*, aprobado en el curso de la octava sesión plenaria del 23 de mayo de 1992 de la Asamblea General de la Organización de Estados Americanos, OEA, y que fuera elaborado por expertos de trece países de América, a instancias de la Comisión Interamericana para el Control del Abuso de Drogas, CICAD, de la OEA.

En lo que hace al tema estrictamente financiero, “los esfuerzos realizados por Colombia para penalizar las operaciones de lavado de dinero a través de instituciones financieras datan de junio de 1987”⁽⁵⁾, y se remontan concretamente al memorando del 15 de junio de 1987 remitido al se-

(3) Sintura, Francisco, *Concesión de beneficios por colaboración eficaz con la justicia. El lavado de activos. Normas penales y estados de excepción*, Bogotá, Ed. Dike, 1995, p. 100.

(4) Sintura, p. 99. El Código Penal que aquí se cita, corresponde al Decreto-Ley 100 de 1980.

(5) Sintura, p. 103.

ñor Presidente de la República por parte de Jorge Humberto Botero, entonces secretario jurídico de la Presidencia de la República, en el que se consideró que la creación de mecanismos para evitar que las instituciones financieras fueran utilizadas para encubrir el origen de recursos ilícitos, “no debía tener un alcance simplemente nacional, sino que resultaba necesario que participara en los estudios a nivel internacional que venían proponiendo por una normatividad uniforme”⁽⁶⁾.

Pese a lo anterior, debe reconocerse que los primeros intentos concretos por evitar que la banca nacional fuera utilizada para el encubrimiento de recursos de origen ilícito provinieron directamente de las instituciones financieras, en un momento en el que no existía norma jurídica alguna que tan siquiera hiciera imperativo para el Estado colombiano la adopción de herramientas jurídicas específicas en la lucha contra el lavado de activos. Es así que el día 21 de octubre de 1992, casi un año antes de que la Convención de Viena de 1988 fuera incorporada a nuestro ordenamiento jurídico, la Junta Directiva de la Asociación Bancaria de Colombia aprobó el *Acuerdo Sobre el Papel del Sistema Financiero en la Detección, Prevención y Represión del Movimiento de Capitales Ilícitos*, con el cual el sistema financiero colombiano pretendía ponerse a la altura del “reto formidable”⁽⁷⁾ al que tendría que dar respuesta de allí en adelante⁽⁸⁾. En lo atinente al deber de reportar operaciones sospechosas, este Acuerdo ya contiene los primeros vestigios de lo que luego sería esta obligación, toda vez que en él se establece el compromiso de colaborar “con las autoridades judiciales y de policía nacionales responsables de la investigación y represión de delitos mediante el suministro de información por estos requerida, así como de la realización de operaciones sospechosas, con base en parámetros previamente establecidos”⁽⁹⁾.

(6) Sintura, p. 103.

(7) Ospina Velasco, Jaime, “Análisis crítico y perspectivo de la detección, prevención y control del lavado de activos en Colombia”, En: *Memorias del III Congreso de Administración del Riesgo* organizado por la Asobancaria en Rionegro entre el 14 y 15 de noviembre de 1996, p. 119. Expresión utilizada por Ospina siendo contralor general del Banco del Estado.

(8) Al respecto, cfr., Ospina, p. 119.

(9) Hernández Quintero, Hernando, *El lavado de activos*, 2^a ed., Bogotá, Ed. Gustavo Ibáñez, 1997, p. 43.

Como se observa, los sistemas de prevención de lavado de activos tienen su origen en los mecanismos de autorregulación que se remontan al acuerdo de octubre de 1992, por virtud del cual las instituciones agremiadas en la Asociación Bancaria asumieron un propio código de buena conducta en materia de prevención y detección de operaciones que tuvieran la potencialidad de utilizar al sistema financiero para actividades de blanqueo.

Exactamente un mes después de esta iniciativa privada, el 20 de noviembre de 1992, el Gobierno Nacional procedió a emitir el Decreto 1872, el cual contiene una regulación orientada hacia ese mismo sentido⁽¹⁰⁾. Par-

(10) En Concepto N° 2003044819-1 del 15 de septiembre de 2003, la Superintendencia Bancaria (hoy Superintendencia Financiera) explicó lo siguiente: “Al respecto cabe señalar que desde 1992 se impuso a las entidades que conforman el sector financiero, la obligación de implementar medidas tendientes a evitar el lavado de activos. En efecto, con el Decreto 1872 de ese año se les obligó a las instituciones a adoptar medidas de control orientadas a evitar que en la realización de operaciones puedan ser utilizadas para el ocultamiento, manejo, inversión o aprovechamiento de dineros u otros bienes provenientes de actividades delictivas”.

Es así como dentro de los mecanismos de control se estableció la obligación de reportar de forma inmediata y suficiente las operaciones sospechosas a determinadas autoridades, esto es, enviar cualquier información relevante sobre el manejo de los fondos cuyas características no guarden relación con la actividad económica de sus clientes o sobre transacciones que por sus peculiaridades puedan conducir razonablemente a sospechar que los mismos están utilizando a la entidad para realizar operaciones provenientes de hechos ilícitos (...).

Como quedó atrás anotado en lo que corresponde a las normas de control de lavado de activos en el sistema financiero importa destacar que sólo a partir de 1992, con la expedición del decreto anotado, se obliga a los intermediarios financieros a adoptar las medidas de control necesarias para prevenir el lavado de dinero. Dicho decreto fue incorporado en su totalidad en los artículos 102 a 107 del Estatuto Orgánico del Sistema Financiero (D. 663 de 1993), EOSF, en su capítulo XVI, Parte Tercera.

Al Decreto 1872 de 1992 le siguieron las Circulares Externas 075 de 1992, 015, 019 y 052 de 1993, a través de las cuales la Superintendencia Bancaria impartió instrucciones a sus vigiladas con el propósito de asegurar la cabal observancia de aquél, teniendo en cuenta los mecanismos de control que legalmente se debían adoptar.

Posteriormente, se expidió la Circular Externa 061 de 1996 mediante la cual se hace obligatorio para las entidades vigiladas la adopción de un Sistema Integral para la Prevención de Lavado de Activos, Sipla. Este instructivo esclarece la manera como debían cumplirse las obligaciones establecidas por el estatuto, consagrando

ticularmente en materia de reporte de operaciones sospechosas, este decreto en el artículo 2º literal d) consagraba la obligación para las entidades financieras de “Reportar de forma inmediata y suficiente a la Fiscalía General de la Nación, o a los cuerpos especiales de policía judicial que esta designe, cualquier información relevante sobre el manejo de fondos cuya cuantía y características no guarden relación con la actividad económica de sus clientes, o sobre transacciones de sus usuarios que por su número,

(Cont. nota 10)

la definición de cliente, y señala cómo debe desarrollarse el conocimiento del mismo. De igual manera se fijan los parámetros de mercado, entendiendo éste como el ámbito en el cual se desenvuelven los usuarios de las entidades, y se señala la necesidad de contar con una plataforma tecnológica adecuada para poder implementar estos mecanismos al igual que con un conjunto de señales de alerta que permitan detectar la ocurrencia de operaciones por fuera de los rangos de normalidad en que se mueven los clientes.

Exige además la designación de un oficial de cumplimiento, persona encargada de velar porque al interior de la entidad se dé cumplimiento a todas esas disposiciones, y el adoptar un código de conducta y un manual de procedimientos. Igualmente, se establecen los rangos a partir de los cuales se realizará el control y reporte de transacciones en efectivo.

En cuanto al conocimiento del cliente, la Circular Externa 072 de 1996 establece los requisitos para su vinculación a través de cuentas corrientes, cuentas de ahorro y CDT's; las 081 y 084 de 1996 lo hacen respecto de negocios fiduciarios; la 005 de 1998 establece esos requisitos respecto de las compañías aseguradoras y sociedades de capitalización; y, la 006 de 1998, por último, los establece respecto de los fondos de pensiones voluntarias, de los afiliados independientes a los fondos de cesantía, y para la realización de aportes voluntarios a los fondos de pensiones obligatorias.

A su turno, la 018 de 1997 establece los plazos para actualizar la información de los clientes vinculados a través de cuentas corrientes, cuentas de ahorro, depósitos a término y negocios fiduciarios; y la 039 de 1997 prevé que cuando las entidades realicen operaciones de compra y venta de inversiones deben identificar al comprador y su actividad económica. Ahora bien, dichos instructivos fueron incorporadas en el Capítulo Noveno del Título Primero de la Circular Básica Jurídica (Cir. Externa 007 de 1996), expedida por esta agencia gubernamental.

En la actualidad, a través de la Circular Externa 046 de octubre del 2002, la cual fue incorporada en el Capítulo Décimo Primero de la Básica en mención (modifica la Circular Externa 061 de 1996) se impartieron nuevas instrucciones a las vigiladas sobre las reglas relativas a la prevención y control de lavado de activos, en la que se señalaron parámetros sobre la forma de conocer al cliente, la detección de operaciones inusuales y el reporte de operaciones y de transacciones en efectivo, entre otros (se adjunta copia). Así mismo, este instructivo fue modificada por la Circular Externa 025 del 10 de junio de 2003.

por las cantidades transadas o por las características particulares, las mismas, puedan conducir razonablemente a sospechar que los mismos están usando a la entidad para transferir, manejar, aprovechar o invertir dinero o recursos provenientes de actividades delictivas”⁽¹¹⁾. Así que, para diciembre de ese año, sobrevino la reglamentación del Decreto 1872, la cual se llevó a cabo mediante la Circular Externa número 75 emitida por la Superintendencia Bancaria.

La reglamentación que de la obligación de reportar operaciones sospechosas hizo la Circular Externa 75 fue minuciosa, al punto que muchas de las limitaciones y alcances que hoy existen encuentran en esta normatividad su primer antecedente. En efecto, esa circular modelaba la obligación de reportar operaciones sospechosas atribuyéndole las siguientes características: (i) el término para reportar sería de cinco (5) días hábiles bancarios siguientes a la fecha en la que la entidad tuvo conocimiento de la operación; (ii) la obligación de reportar debería cumplirse, sin perjuicio de la obligación de suministrar nuevamente la misma información, o la que estuviera a su disposición, cuando así lo solicitara la Fiscalía General de la Nación por intermedio de sus directores regionales o seccionales (art. 7º D. 1870); (iii) el reporte de operaciones sospechosas no exoneraría a las entidades de su deber de presentar los informes periódicos sobre transacciones en efectivo, de que trataba el artículo 6º del Decreto 1872, y (iv) las entidades deberían adoptar un sistema de control de transacciones en efectivo que les permitiera identificar operaciones múltiples, y reportarlas a la Fiscalía General de la Nación o a los cuerpos de policía judicial.

El año 1993, fue sin duda más importante que vivió Colombia en la lucha contra la delincuencia organizada, especialmente contra el lavado de activos a través del sistema financiero. En primer lugar, en ese año tuvo lugar la aprobación de la *Convención de las Naciones Unidas Contra el Tráfico Ilícito de Estupefacientes y Sustancias Sictotrópicas*⁽¹²⁾. Pero además, también las normas relativas a la prevención de actividades delictivas contenidas en el Decreto 1872 fueron incluidas en el Capítulo XVI del De-

(11) Hernández, p. 46.

(12) Declarado exequible por la Corte Constitucional mediante Fallo C-176 del 12 de abril de 1994.

creto 663 de 1993, Estatuto Orgánico del Mercado Financiero, el cual contiene en sus artículos 102 a 107 las disposiciones fundamentales sobre las cuales se elabora e interpreta en la actualidad todo el régimen general de prevención de lavado de activos en el mercado financiero y en otros mercados a los que se ha hecho extensible esa regulación.

En lo específicamente atinente al deber de reportar operaciones sospechosas, el literal d) del numeral 2 del artículo 102 del Decreto 663 reproducía el mandato contenido en el literal d) del artículo 2º del Decreto 1872, por lo que las disposiciones contenidas en la Circular Externa 75 de 1992 continuaron vigentes. Por su parte, en lo que hace a la obligación de hacer reportes periódicos de operaciones en efectivo –ya no sospechosas–, su reglamentación fue excesivamente dispendiosa desde el punto de vista operativo para la Superintendencia Bancaria, y de ello dan cuenta las tres intervenciones que mediante las circulares 15, 19 y 52 tuvo que realizar la entidad, para alcanzar una regulación razonablemente satisfactoria. La adecuada recopilación y procesamiento de la voluminosa información remitida por las entidades financieras significó para la Superintendencia un reto de enormes proporciones, y para ello debió intentar diversas regulaciones frente a aspectos como: diseño de formularios para remisión de información, categorías o clases de operaciones, formas de envío de la información, plazos para recibir la información, presentación de la información relativa a operaciones en divisas, etc. Mas sin embargo, y haciendo abstracción de las dificultades anotadas, puede decirse que 1993 es el año en que la práctica de reportar operaciones inicia su funcionamiento, en el marco regulativo emitido por la Superintendencia Bancaria⁽¹³⁾.

Pese al avance que suponía esta regulación, ella no era suficiente para atender la necesidad de profilaxis criminal de la sociedad colombiana, pues esta normatividad se encuentra particularmente entroncada en la legislación financiera, lo que significaba que el Estado carecía de una legislación que abarcara otros ámbitos de la realidad nacional distintos del sector financiero. Así mismo, la realidad nacional exigía una legislación que fuera específicamente penal, para obtener las herramientas orientadas a combatir las nuevas formas de delincuencia organizada desarrolladas en

(13) Al respecto, cfr., Ospina, p. 119.

contexto del narcotráfico, la corrupción y el conflicto armado al que se enfrentaba la sociedad.

En parte para solventar esta falencia y poder cumplir los compromisos internacionales adquiridos con la aprobación de la Convención de Viena, durante el Gobierno de César Gaviria se realizó al menos un intento por parte de Andrés Gómez Díaz, Ministro de Justicia, enderezado a impulsar una ley destinada a ofrecer nuevos mecanismos penales para combatir estas formas de delincuencia. Lamentablemente, este proyecto adolecía de evidentes errores no sólo de técnica legislativa sino también de contenido, por lo que no tuvo acogida en el Congreso y naufragó⁽¹⁴⁾. La senda que definitivamente conduciría a la promulgación de una legislación como la demandada se inició, cuando el entonces “ministro de Justicia del nuevo gobierno del presidente Samper, Néstor Humberto Martínez, presentó en la segunda semana del mes de octubre de 1994, un proyecto de ley ‘por la cual se dictan normas tendientes a preservar la moralidad en la administración pública y se fijan disposiciones con el fin de erradicar la corrupción administrativa’, cuyo Capítulo IV sobre el régimen penal, en los artículos 43 y 44 consagraban aspectos relacionados con el lavado de activos”⁽¹⁵⁾. Este proyecto, que en términos generales acogía las recomendaciones que en materia de prevención del lavado de activos se ofrecieron desde la Fiscalía General de la Nación a la Asociación Bancaria de Colombia⁽¹⁶⁾, vino finalmente a convertirse en la Ley 190 de 1995, también conocida como “Estatuto Anticorrupción”. Sin embargo, debe aclararse que la Ley 190 no logró dar al delito de lavado de activos la fisonomía requerida, pues la tipificación de esta conducta no se llevó a cabo de manera autónoma, sino mediante la reforma del artículo 177 del Código Penal entonces vigente (D.L. 100/1980), relativo al delito de *receptación*.

No obstante haberse omitido la recomendación de crear un tipo penal autónomo para el lavado de activos, la Ley 190 de 1995 significó de to-

(14) Hernández, p. 63.

(15) Sintura, p. 104.

(16) El contenido de estas recomendaciones se encuentra recogido en el texto de la conferencia ofrecida por Francisco José Sintura Varela el 29 de julio de 1994, siendo Vicefiscal General de la Nación, a la Asociación Bancaria de Colombia.

das formas un gran paso en la lucha contra este tipo de delincuencia, particularmente porque elevó a la jerarquía de Ley de la República una serie de disposiciones que obligaban a las entidades financieras a asumir un compromiso irrenunciable en la lucha contra la criminalidad, lo que hasta entonces había sido exiguamente desarrollado por la normatividad administrativa.

Uno de los mayores méritos de la Ley 190 en materia de prevención del lavado de activos fue haber intentado organizar de la mejor manera, la gestión de la información necesaria para la detección del delito. Si bien es cierto que esta ley no produjo modificaciones sustanciales en cuanto al contenido de la obligación consagrada en el literal d) del numeral 2 del artículo 102 del Decreto 663 de 1992, ni tampoco al desarrollo que dicha obligación había tenido en la Circular Externa 75 de 1992, esta norma sí propició una organización administrativa más adecuada para el manejo de los reportes de operaciones sospechosas. Antes de la Ley 190, las transacciones en efectivo debían reportarse a la Superintendencia Bancaria y las operaciones sospechosas a la Fiscalía General de la Nación o a los cuerpos de policía judicial que ésta designara⁽¹⁷⁾. Debido a esta situación, en la práctica se había producido un fenóme-

(17) En el Concepto 2003044819-1 del 15 de septiembre de 2003, la Superintendencia Bancaria (hoy Superintendencia Financiera) explicó que: “Tratándose del reporte de operaciones sospechosas, importa destacar que teniendo en cuenta que de conformidad con lo señalado en el Decreto 1872 de 1992 las operaciones sospechosas debían remitirse a la Fiscalía General de la Nación, no existía un procedimiento específico sobre la forma como debía enviarse dicha información ni la Superintendencia Bancaria de Colombia diseñó tal procedimiento”.

No obstante lo anterior, debe precisarse que mediante Carta Circular 36 de 1995, aunque se titula “Transacciones en efectivo”, se instruyó a las entidades vigiladas sobre el reporte que debían enviar a la Fiscalía General de la Nación en cumplimiento de los previsto en el numeral 2 del artículo 102 del EOSF, en concordancia con lo reglado en el numeral 1 de la Circular Externa 075 de 1992, en el sentido de que el mismo debía remitirse a la Dirección del Cuerpo Técnico de Investigación de dicha autoridad.

Así mismo, no existía un formato especial para que las entidades enviaran el reporte de operaciones sospechosas, sólo hasta la expedición de la Circular Externa 061 de 1996 se dispuso lo siguiente: “Por otra parte es importante señalar que pese a las facultades concedidas por la Ley 190, como se verá, los reportes de operaciones sospechosas se seguirán remitiendo a la Fiscalía General de la Nación hasta el año 1999, cuando se crea la UIAF”.

no perverso de ineeficiencia en la persecución del delito, toda vez que los organismos encargados de la investigación penal se encontraron literalmente inundados de reportes y sin la capacidad operativa de indagarlos todos⁽¹⁸⁾. Para conjurar esta circunstancia, el parágrafo primero del artículo 40 de la Ley 190 manifestó que “el Gobierno Nacional por conducto del Ministerio de Hacienda y Crédito Público, podrá disponer que la información recaudada por las personas a las que se refiere este artículo y el artículo 43 de la presente ley, sea remitida a la autoridad que el reglamento determine, con el propósito de centralizar y sistematizar la información, en orden a establecer mecanismos de control comprensivos de las distintas operaciones realizadas”.

Pero además y anticipándose al papel que las Superintendencias cumplirían en el marco de las normas que el Gobierno emitiría en uso de la facultad que se le otorgaba, el legislador consagró en el parágrafo 2º de ese mismo artículo 40 que “dentro de los dos meses siguientes a la vigencia de esta ley, la Superintendencia Bancaria y de Valores asignarán a una de sus dependencias la función de control de las operaciones de que tratan los artículos 102 a 107 del Estatuto Orgánico del Sistema Financiero (D. 663/1993), sin perjuicio de que el Gobierno Nacional cree Unidades Especializadas dentro de ellas, para tal efecto”.

(18) En materia de reporte de operaciones sospechosas, el artículo 40 de la Ley 190: “Establece la obligatoriedad del informe de operación sospechosa que hoy, con un desarrollo posterior, se identifica en dos niveles diferentes: primero, inusual; y, después, sospechosa” (Ospina, p. 121). Así mismo desde su consagración en esta ley, la obligación de reportar las operaciones tuvo una naturaleza y alcance perfectamente definido, por virtud de la regulación que de la misma se hizo en los artículos 39 a 44. Desde entonces ha estado claro que el reporte de operaciones sospechosas en ningún caso constituye denuncia (cfr., la exposición de motivos de la L. 190/1995), al punto que el artículo 42 prescribe que, a diferencia de la responsabilidad que puede generar (*delito de falsa denuncia*), “cuando se suministre la información de que trata el artículo 40 de la presente ley, no habrá lugar a ningún tipo de responsabilidad para la persona jurídica informante, ni para los directivos o empleados de la entidad, en concordancia con el artículo 102 del Decreto Ley 663 de 1993”. Adicionalmente, tal como puede extraerse del tenor literal del artículo 42 de esta Ley 190, ya desde esta regulación se adoptó la postura de que los reportes debían ser institucionales, por lo que desde entonces es claro que la autoría del reporte pertenece a la institución financiera como persona jurídica, y no al funcionario o funcionarios que lo elaboran.

Atendiendo los propósitos de la Ley 190, el Gobierno Nacional hizo uso de las facultades que se le otorgaban y procedió a emitir el Decreto 1552 de ese año, por virtud del cual se creó una unidad especial en la Superintendencia Bancaria para el manejo de esos temas. Esta decisión fue sin duda importante, “porque hasta 1995, tres años después de la expedición del Decreto 1872, la Superintendencia Bancaria no había entendido que ese era un problema de manejo especial”⁽¹⁹⁾, y el nuevo esquema creó las condiciones necesarias para permitir “un flujo de información menos rígido y muy productivo, con el cual la Superintendencia ha entrado en una nueva etapa del manejo del problema”⁽²⁰⁾.

En medio de este escenario, los esfuerzos privados e independientes del sector financiero continuaron, y desde el *Comité de Administración de Riesgo* creado en 1994 por la Asociación Bancaria de Colombia, el cual estaba integrado por funcionarios de alto nivel jerárquico del área de contraloría de los diferentes bancos, se impulsaron importantes iniciativas. Una de ellas culminó con la adopción del convenio sobre suministro de información para fines investigativos, suscrito entre la Asobancaria y la Fiscalía General de la Nación el día 6 de septiembre de 1995. En el marco de ese convenio, la Asociación Bancaria no solo proveería a la Fiscalía General “la información disponible en su base de datos (CIFIN)”⁽²¹⁾, sino que además adoptaría “un sistema de información para el reporte de transacciones en efectivo superiores a determinada cuantía, que permita centralizar y sistematizar la información”⁽²²⁾.

En el ámbito particular de los reportes, “este convenio generó la primera mecánica de los reportes a la Fiscalía en forma ignominada [sic] con el ánimo de salvaguardar la naturaleza de la información y su origen, y también preservar la integridad de los funcionarios”⁽²³⁾. Ya en este momento se reconoce abiertamente que la reserva de la identidad de los funcio-

(19) Ospina, p. 121.

(20) Ibíd.

(21) Hernández, p. 44.

(22) Ibíd.

(23) Ospina, p. 122.

narios encargados del control de operaciones, asegurada mediante el carácter institucional de los reportes, tiene una doble justificación: en primer lugar, evitar el ejercicio de presiones sobre ellos por parte de la delincuencia organizada, y en segundo lugar, brindar la seguridad de que el reporte de operaciones no tendría consecuencias personales sobre el funcionario, con lo cual se pretendía promover esta práctica.

Gracias a este nuevo impulso que la Ley 190 imprimió a la política de lucha contra la delincuencia organizada y concretamente contra el lavado de activos, en lo sucesivo se dieron avances puntuales en relación con la regulación específica de algunos mecanismos de control. Tal fue el caso de las Circulares Externas 71, 72 y 74 emitidas por la Superintendencia Bancaria, las cuales regularon la manera en que debía cumplirse la obligación de conocimiento del cliente por parte de las instituciones financieras, y de las Circulares Externas 75 y 80 también de la Superbancaria, destinadas a regular la prevención de lavado de activos en el mercado fiduciario y en el mercado de bonos respectivamente.

No pasó mucho tiempo –menos de un año– antes de que se advirtiera la existencia de una dificultad derivada de la excesiva proliferación de normas, y se desarrollara una conciencia colectiva acerca de la necesidad de recopilar toda esa legislación en un solo cuerpo. Con este propósito, la Superintendencia Bancaria se dio a la tarea de crear una norma razonablemente sistemática que compilara y ampliara la regulación ya emitida por ella desde 1992, consecuencia de lo cual fue el Capítulo XI de la Circular Básica Jurídica 7 de 1996. Esta circular fue la primera norma que compiló la regulación existente en materia de prevención de lavado de activos, y a la sazón se encargó de reglamentar todo lo relativo a los mecanismos de conocimiento del cliente, conocimiento del mercado, control y reporte de operaciones y capacitación, así como también los instrumentos de control obligatoriamente adoptables por las instituciones financieras, tales como los códigos de conducta, manuales de procedimientos, oficial de cumplimiento, sistemas de manejo de información, etc.

La regulación contenida en la Circular Básica Jurídica 7 se convirtió en el principal punto de referencia para la definición y delimitación de los Sistemas Integrados para la Prevención del Lavado de Activos, cuya adopción se hizo obligatoria para todos los intermediarios de los mercados fi-

nanciero, cambiario, asegurador y bursátil⁽²⁴⁾. Regulación que vino a mantenerse casi intacta hasta el año 2003, siendo apenas complementada en temas puntuales por las Circulares Externas 61 de 1996 y 12 de 1999 emitidas por la Superintendencia Bancaria, y por las Cartas Circulares 6 y 135 de 1998 emitidas de manera conjunta por las superintendencias Bancaria y de Industria y Comercio.

Para 1997 era mucho lo que se había avanzado en materia de preventión de lavado de activos y en su regulación administrativa, a pesar de las múltiples lagunas, anunciable ya visos de exhaustividad. Sin embargo, no se habían atendido en debida forma los compromisos internacionales adquiridos con la aprobación de la Convención de Viena de 1988, en tanto que la Ley 190 no había tipificado de manera autónoma el delito de lavado de activos, limitándose a criminalizarlo como una forma agravada de la receptación mediante la modificación del artículo 177 del Decreto-Ley 100 de 1980 (Código Penal entonces vigente). Para esta época era ya claro que la penalización del lavado de activos como una forma de receptación era en todo caso inconveniente, pues en primer lugar el artículo 177 del Cód-

(24) En relación con la obligación de reportar operaciones sospechosas, puede decirse que la Circular Básica Jurídica 7 fue prolífica, pues no se contrajo a contemplar la obligación, sino que de hecho se dio a la tarea de precisar algunos conceptos importantes para su cumplimiento. En este sentido, el artículo 2.3.1.4.1 definió como operaciones sospechosas: “A aquellas que, confrontadas las detectadas como inusuales con la información acerca de los clientes y del mercado, permite colegir fundadamente que resulta, conforme al buen criterio de la entidad, irregular o extraña, al punto que escapan de lo simplemente inusual para llevar a considerar que con ella se están consumando actividades delictivas” (una explicación de esta disposición puede encontrarse en Martínez Sánchez, Wilson Alejandro, p. 97). A la par de la definición de *operaciones sospechosas*, la norma mantuvo la obligación de reportar estas a la Fiscalía General de la Nación o a los cuerpos de policía judicial designados por estos, pues para la fecha de la emisión de dicha circular, el Gobierno Nacional aún no había creado la unidad administrativa especial a que se refería la Ley 190 de 1995 en el parágrafo 1º de su artículo 40. En términos generales, el reporte de operaciones sospechosas siguió estando caracterizado por su carácter institucional (no debía ser firmado por funcionario alguno), por la exoneración de responsabilidad para la entidad informante y por su diferenciación con la denuncia penal en cuanto a las responsabilidades derivadas de su presentación, tal como venía establecido desde la Circular Externa número 75 del año 1992 y la Ley 190, cambiando apenas en algunos aspectos formales como por ejemplo los plazos para presentación de reportes y los formularios previstos para ello.

go Penal vigente sancionaba el ocultamiento del origen ilícito de recursos limitándolo a aquellos casos distintos de los concursos de delitos, lo cual “impedía la aplicación del concurso entre el delito del cual proviene el producto ilícito (extorsión, narcotráfico, secuestro, etc.), con el tipo de lavado de activos (receptación en este evento), resultando entonces muy benigna la sanción”⁽²⁵⁾. Y en segundo lugar, porque la no distinción entre el lavado de activos y la recepción impedía al Estado dar una respuesta punitiva diferente a cada uno de estos fenómenos criminales, lo que había degenerado en la excesiva punibilidad del delito de recepción común, por virtud del aumento de los marcos sancionatorios que la Ley 190 había consagrado en su afán de prevenir el lavado de activos.

La réplica del Gobierno a esta situación tuvo lugar mediante el proyecto de ley presentado por el Ministro de Justicia de la época, Carlos Medellín Becerra, por medio del cual se creaba un marco jurídico-penal “para acabar con el narcotráfico y el crimen organizado”⁽²⁶⁾. Este proyecto de ley, que a la postre se convertiría en la Ley 365 de 1997, introdujo en el Código Penal vigente cuatro nuevos artículos a saber: el 247A, en el cual se tipificaba por fin, de manera autónoma, el delito de *lavado de activos*; el 247B, en el cual se creaba el delito de *omisión de control*; el 247C, en el cual se preveían unas circunstancias específicas de agravación para los dos artículos anteriores y el 247D, en el cual se imponían una penas accesorias comunes a los dos delitos anteriores. Desde entonces la lucha contra el lavado de activos era frontal, pues ahora era una forma delictiva autónoma y los mecanismos penales para su prevención y represión se habían robustecido, salvo por la subsistencia de problemas operativos en el procesamiento de los reportes de operaciones sospechosas.

En efecto, la perversidad del congestionamiento que padecía el Cuerpo Técnico de Investigaciones (CTI) como consecuencia del significativo volumen de reportes de operaciones sospechosas continuaba, y para 1997, dos años después de que la Ley 190 le diera al Gobierno las facultades para conjurar ese hecho, la situación seguía siendo la misma. La solución solo vendría hasta 1999 cuando la Ley 526 crea la *Unidad de Información y Análisis Financiero*.

(25) Hernández, p. 81.

(26) Ibíd.

mación y Análisis Financiero (UIAF), que se concibió como una unidad administrativa especial adscrita al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y régimen especial en materia de administración de personal. Esta unidad, creada para operar a la manera de una central de inteligencia financiera, sería en adelante la receptora de los reportes de operaciones sospechosas, así como la encargada de analizar y sistematizar dichos reportes en orden a determinar si existe mérito para que la Fiscalía General de la Nación se aboque a una investigación penal. Los procedimientos adoptados por la UIAF se inspiraron en su mayoría por las experiencias adquiridas por el *Grupo de Acción Financiera Internacional* (su sigla en español, GAFI) y el *Grupo Egmont*, los cuales buscaron garantizar que antes de que el Estado incurriera en el desgaste que supone el desarrollo de una investigación penal, los reportes fueran técnicamente estudiados por parte de personal especializado en el mercado financiero, quienes no sólo filtrarían hacia la Fiscalía las operaciones verdaderamente merecedoras de su intervención, sino que además podrían servir como asesores especializados para ofrecer a los órganos jurisdiccionales mejores elementos de juicio en materia de lavado de activos. En este sentido, la gestión que cumple la UIAF como receptora de los reportes y como filtro de casos hacia la Fiscalía es una labor verdaderamente seria, dotada de fundamento técnico y absolutamente especializada. Esto asegura que en el evento que una operación reportada como sospechosa termine en manos de la Fiscalía es porque existen razones suficientes, para pensar que aquella realmente puede ser constitutiva de lavado de activos.

Normativamente, lo dicho tuvo reflejo en la modificación que la Ley 526 de 1999 introdujo al literal d) del numeral 2 del artículo 102 del Decreto 663 de 1993, en el sentido que los reportes de operaciones sospechosas ya no se dirigirían a la Fiscalía General de la Nación, ni a los organismos con funciones de policía judicial designados por ella, sino a la UIAF como organismo técnico y especialmente dotado con capacidad para analizar, sistematizar y procesar esa información. De igual manera y para el adecuado cumplimiento de sus funciones, la Ley 526 dispuso que la UIAF podría ser dotada de manera transitoria de funciones de policía judicial, lo que tendría una doble consecuencia: de un lado, que las evidencias recolectadas por esta unidad durante el curso de aquellas investigaciones en las que fuera dotada de aquellas facultades tendrían pleno valor como prue-

bas dentro de los procesos penales; y de otra parte, que los funcionarios de la unidad encargados de las investigaciones podrían actuar revestidos de una autoridad especial, que les facilitaría la consecución de un mayor volumen de elementos de prueba.

Finalmente, el último gran paso dado en la lucha contra el lavado de activos en el mercado financiero consistió en una reestructuración y complementación de la regulación contenida en el Capítulo XI de la Circular Básica Jurídica 7 de 1996, efecto para el cual se emitió la Circular Externa 25 de 2003 por parte la Superintendencia Bancaria, la que recientemente fue modificada en algunos aspectos puntuales por parte de la Circular Externa 34 de 2004. La principal virtud de esta normatividad fue ofrecer una comprensión más sistemática de los mecanismos de prevención obligatoriamente adoptables por parte de las entidades financieras, sin introducir modificaciones sustanciales en materia conceptual.

CAPÍTULO 2

Estándares internacionales en materia de prevención

La difícil situación interna que padece nuestro país como consecuencia del conflicto armado y el narcotráfico exige, que la legislación en materia de prevención del lavado de activos y la financiación del terrorismo (LA/FT en castellano, o *anti-money laundering/combatting the financing of terrorism* –AML/CFT por sus siglas en inglés– sea la mejor. Por esta razón, las autoridades ocupadas de ejecutar la política criminal del Estado, así como los diferentes organismos y agremiaciones privadas encargados de la autorregulación del mercado financiero, cambiario, bursátil y asegurador han hecho ingentes esfuerzos para que la legislación nacional satisfaga los estándares internacionales en esta materia. Como consecuencia de ello, el régimen actual de prevención del lavado de activos y la financiación del terrorismo en Colombia incorpora las recomendaciones impartidas por las más importantes organizaciones internacionales ocupadas de la materia.

Varios son los organismos internacionales que han emitido recomendaciones y algunos de los más importantes son los siguientes: *Basel Committee on Banking Supervision* (BCBS) o Comité de Supervisión Bancaria de Basilea, *Bank for International Settlements* (BIS), Programa de Asistencia Legal para Latinoamérica y el Caribe adscrito a la Oficina Contra la Droga y el Delito de la Organización de Naciones Unidas (UNODC)⁽¹⁾, *Financial Action Task Force* (FATF) o Grupo de Acción Financiera Internacional (GAFI), *Offshore Group of Banking Supervisors* (OGBS)⁽²⁾,

-
- (1) La página web oficial en castellano de esta oficina es <<http://www.integranet.un.org/spanish/Depts/dpi/boletin/drogas/info.shtml>>.
 - (2) También conocido en nuestro idioma como el Grupo Extraterritorial de Supervisores Bancarios.

International Association of Insurance Supervisors (IAIS), e *International Organization of Securities Commissions* (IOSCO). Estos organismos han elaborado diversos documentos, algunas veces de manera separada y otras conjuntamente, en los cuales establecen los estándares mínimos que deben satisfacer los sistemas adoptados por las entidades financieras, cambiarias, bursátiles y aseguradoras, para la adecuada administración del riesgo relativo al lavado de activos y la financiación del terrorismo.

1. PRINCIPIOS GENERALES DE PREVENCIÓN DEL COMITÉ DE BASILEA

Uno de los documentos más antiguos en esta materia es el que contiene las recomendaciones emitidas en el mes de diciembre de 1988 por el Comité de Supervisión Bancaria de Basilea o Comité de Basilea (*Basel Committee on Banking Supervision*, BCBS por sus siglas en inglés), titulado “Declaración de principios sobre prevención del uso criminal del sistema bancario para fines de lavado de activos” (*Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering*)⁽³⁾. Este documento fija los estándares mínimos internacionales en materia de prevención del lavado de activos, a partir de cuatro principios a saber:

1.1. Identificación del cliente

Para asegurar que la entidad no sea utilizada para canalizar recursos de origen ilícito, las entidades financieras deben establecer con seguridad la verdadera identidad de las personas que solicitan sus servicios. Especialmente identificar adecuadamente al propietario de los recursos que se canalizan a través de la entidad, los titulares de las cuentas y los usuarios de sus servicios. Este conocimiento del cliente debe ser una política institucional clara, por lo cual debe abstenerse de realizar transacciones con personas a quienes no pueda identificar plenamente.

(3) Disponible en Web: <<http://www.bis.org/publ/bcbsc137.pdf?noframes=1>> (consultado el 7 de octubre de 2009).

1.2. Aseguramiento y control del cumplimiento de la ley

Los directivos y administradores de las entidades financieras deben asegurarse de que los negocios están siendo desarrollados conforme a altos estándares éticos, y con riguroso apego a la normatividad aplicable. Aunque en muchos casos es difícil establecer si una de las transacciones realizadas con un cliente es parte de una actividad delictiva, las entidades deben abstenerse de realizar aquellas transacciones sospechosas de lavado de activos.

1.3. Cooperación con las autoridades judiciales

Las entidades financieras deben colaborar a las autoridades nacionales, suministrando la mayor cantidad de información que sea posible de acuerdo con la regulación en materia de confidencialidad y secreto bancario. Además deben tomar precauciones para evitar que la información suministrada a las autoridades respecto de los clientes sea alterada, incompleta o extraviada. Cuando las entidades tengan la presunción razonable de que los dineros depositados o utilizados en una transacción pueden provenir de actividades ilegales deben tomar medidas apropiadas de acuerdo con la ley, tales como negar la prestación del servicio al cliente o la cancelación o congelamiento de las cuentas.

1.4. Adopción formal de políticas para la prevención del lavado de activos

Las entidades deben adoptar de manera explícita y formal políticas consecuentes con los principios antes mencionados. Así mismo deben asegurarse de que todos los funcionarios estén informados y preocupados por la aplicación efectiva de dichas políticas. A tal efecto, los funcionarios deben ser capacitados en los temas relacionados con los principios mencionados, y la entidad debe adoptar procedimientos específicos para el conocimiento del cliente y la conservación de registros internos de las transacciones. Finalmente, la entidad debe disponer la realización de auditorías para establecer y evaluar el cumplimiento de los principios mencionados y las políticas adoptadas.

2. RECOMENDACIONES DEL GRUPO DE TRABAJO DE ACCIÓN FINANCIERA, GAFI

El GAFI es un cuerpo intergubernamental creado en 1989, cuyo propósito principal es promover y desarrollar políticas nacionales e internacionales orientadas a combatir el lavado de activos y la financiación del terrorismo⁽⁴⁾. El GAFI es en ese sentido un cuerpo creador de las políticas necesarias para generar normas o regulaciones adecuadas en esa materia. A tal propósito, este organismo publicó en el año 1990 un documento contentivo de cuarenta (40) recomendaciones para la prevención del lavado de activos. Este documento fue revisado por primera vez en 1996 para dar cuenta de las nuevas modalidades de lavado de activos y anticipar el surgimiento de nuevas tendencias, y desde entonces ha tenido actualizaciones puntuales. La más importante de estas tuvo lugar octubre de 2001, oportunidad en la cual se incluyeron ocho recomendaciones adicionales directamente orientadas a prevenir la financiación del terrorismo. La última revisión culminó el 20 de junio de 2003, con la publicación de la versión del documento de las cuarenta recomendaciones originales y de las ocho adicionales⁽⁵⁾. Este ha sido suscrito a la fecha por 130 países, y actualmente es la publicación internacional más importante en la materia. Finalmente, el GAFI también ha emitido varias notas interpretativas diseñadas para aclarar las recomendaciones, y ofrecer una guía general para su comprensión⁽⁶⁾.

Las recomendaciones impartidas por el GAFI constituyen las medidas mínimas de prevención que deberían exigirse por parte de los diferentes países, mediante su inclusión en la regulación prevista en las respectivas legislaciones nacionales sobre la materia. Ellas definen el estándar mínimo internacional de regulación jurídica penal, administrativa y financiera en materia de lavado de activos y financiación del terrorismo, y de paso

(4) La página web oficial de este organismo es <<http://www.fatf-gafi.org>> (consultado el 15 de octubre de 2009).

(5) Documento disponible en Web: <<http://www.fatf-gafi.org/dataoecd/38/53/34030987.pdf>> (consultado el 15 de octubre de 2009).

(6) Las notas interpretativas están disponibles en la página web: <http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236920_33988956_1_1_1,00.html#General_information> (consultado el 15 de octubre de 2009).

ofrecen un patrón normativo que se debería implementar por parte de las entidades financieras y por otros profesionales expuestos a riesgos similares, facilitando la cooperación internacional frente al lavado de activos y la financiación del terrorismo.

Sumado a lo anterior, el GAFI hace seguimiento y evaluación permanente de la aplicación de sus recomendaciones por parte de los diferentes países. A tal efecto lleva a cabo evaluaciones con apoyo de sus grupos regionales (en el caso de Suramérica es el Gafisud), o de organismos internacionales como el Fondo Monetario Internacional o el Banco Mundial, los cuales le permiten diagnosticar el estado del implementación de las cuarenta recomendaciones.

Ahora bien, en lo que hace al contenido de dichas recomendaciones, una exposición completa no es posible aquí. Por tal razón se recomienda consultar directamente el documento publicado por ese organismo, a efectos de poder conocer en detalle su contenido y alcance. No obstante, algunas de las principales recomendaciones podrían sintetizarse de la siguiente manera:

—La primera y más importante es la de tipificar el lavado de activos como delito autónomo, en los términos indicados en la Convención de Viena contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas proclamada en 1988, y la Convención de Palermo contra Delincuencia Organizada Transnacional organizada por Naciones Unidas en el año 2000. Se recomienda a los países que dicha tipificación incluya la mayor cantidad de delitos subyacentes posible, y como mínimo los delitos considerados de mayor gravedad en cada legislación. También se recomienda que el tipo penal de lavado de activos comprenda aquellas conductas realizadas por fuera del territorio nacional, y que sean consideradas como delito subyacente por la respectiva legislación nacional.

—Se recomienda a los países incluir en su legislación interna un régimen de responsabilidad para las personas jurídicas. Lo ideal es que prevean un régimen de responsabilidad penal directa. Sin embargo, cuando los principios rectores de la legislación nacional no permitan esta forma de responsabilidad, el régimen debería prever alguna consecuencia civil o administrativa.

— Los países deberían incluir en sus legislaciones instituciones o mecanismos jurídicos que permitan el decomiso de los activos lavados, los bienes producto del lavado de activos o de algún delito subyacente, los recursos utilizados para realizar el lavado de activos o algún delito subyacente, o bienes por un valor equivalente. El objetivo es que las autoridades dispongan de mecanismos eficaces para privar a los delincuentes de los activos obtenidos de manera ilícita, y de los utilizados para la comisión del delito de lavado de activos o cualquier otra conducta punible. Se recomienda que los países prevean en su legislación interna que este tipo de medidas pueden hacerse efectivas, sin necesidad de que medie una condena penal.

— El GAFI recomienda que las normas sobre secreto y confidencialidad bancaria no sean un obstáculo para la eficacia de las investigaciones por el delito de lavado de activos.

— Las entidades financieras deben adoptar medidas oportunas y suficientes para obtener un conocimiento adecuado de sus clientes. Esto significa que no debería permitirse la apertura de cuentas anónimas, cifradas o bajo nombres ficticios. Estas medidas para el conocimiento del cliente deben adoptarse desde el comienzo de la relación comercial, y aplicarse periódicamente para mantener actualizada y verificada la información disponible. En el caso de los clientes que por su actividad económica, perfil comercial, domicilio, etc., representen una mayor exposición al riesgo de lavado de activos, las medidas de conocimiento deben ser más rigurosas.

— Especial atención deben prestar las entidades a aquellas operaciones que por su complejidad, por su cuantía o por cualquiera otra circunstancia resulten inusuales. La entidad debe evaluar los antecedentes de estas operaciones, asentar las conclusiones por escrito y dejar la información correspondiente a disposición de los auditores y las autoridades.

— Las entidades financieras deben adoptar sistemas para el monitoreo permanente de sus operaciones. Estos sistemas deben permitir identificar plenamente al ordenante y al beneficiario, determinar hasta dónde sea posible el origen y destino de los fondos, y evaluar la normalidad de la operación. Igualmente, los sistemas de monitoreo deben permitirle a las entidades identificar las operaciones sospechosas, para reportarlas a las autoridades competentes (Reporte de Operaciones Sospechosas, ROS).

—Los Estados deberían crear un organismo o agencia gubernamental de inteligencia financiera. Así mismo deberían incluir en sus legislaciones o reglamentos, la obligación de reportar las operaciones sospechosas a dichas unidades de inteligencia financiera, quienes deberían estar encargadas específicamente de analizar esa información. Este organismo debe tener acceso a toda la información financiera necesaria para investigar oportuna y eficazmente operaciones de lavado de activos.

—Las legislaciones nacionales deberían proveer alguna forma de protección a los directivos, administradores o funcionarios encargados de realizar los reportes de operaciones sospechosas. Al mismo tiempo debería prohibirse expresamente divulgar al cliente o a cualquiera otra persona, el hecho de haber sido reportada una de sus operaciones.

—Se recomienda a los países exigir normativamente a las entidades el diseño y aplicación de sistemas de prevención del lavado de activos y la financiación de terrorismo. Estos sistemas deben incluir políticas, procedimientos y controles internos. También deben incluir protocolos para la selección y capacitación permanente del personal. Así mismo deben incluir procedimientos para la auditoría y evaluación permanente del sistema.

—Las entidades financieras deben adoptar las medidas necesarias para asegurar que sus bancos corresponsales en el extranjero son confiables. Esto implica que, entre otras cosas, debe estudiarse el perfil comercial del banco corresponsal, determinar su reputación, establecer si ha sido objeto de sanciones relacionadas con el lavado de activos o delitos conexos, y asegurarse que posea un sistema de prevención adecuado.

—Las entidades deben adoptar políticas y procedimientos para hacer frente a los riesgos de lavado de activos derivado de la implementación de nuevas tecnologías. Concretamente debe implementar medidas para mitigar el riesgo de lavado en aquellas operaciones que no requieren presencia física del cliente, como por ejemplo, las transferencias electrónicas.

—Las entidades deberían conservar por un periodo mínimo de cinco (5) años la documentación que soporta la información relacionada con las operaciones nacionales e internacionales. Además, esta documentación debe ser conservada y organizada de tal forma que se garantice la facilidad de acceso cuando sea requerida por las autoridades.

— Se recomienda a los países extender las obligaciones de conocimiento del cliente, reporte de operaciones sospechosas y conservación de información a otras profesiones o actividades distintas de la financiera, cuando quiera que ellas estén expuestas también al riesgo de lavado de activos.

— Los Estados deberían asegurar que las entidades financieras estén sometidas a una supervisión constante por parte de algún organismo gubernamental. Este organismo velará porque las entidades cumplan los estándares mínimos de diligencia en materia de prevención de lavado de activos, y tendrán la facultad de imponer sanciones a aquellas que no lo hagan.

— Se recomienda que las legislaciones nacionales extiendan la supervisión a los casinos, y que exijan de éstos la implementación de mecanismos que satisfagan los estándares mínimos previstos en las recomendaciones del GAFI.

— Las entidades financieras y no financieras especialmente expuestas al riesgo de lavado de activos (casinos, casas de cambio, cambistas profesionales, etc.) deberían funcionar bajo licencia o autorización del Estado. Dicha licencia se otorgará cuando el organismo de supervisión estatal competente haya verificado el cumplimiento de la regulación en materia de prevención del lavado de activos y financiación del terrorismo, y será revocada en el caso de que esas entidades no apliquen adecuadamente los controles mínimos exigidos por la respectiva legislación.

— Las autoridades no autorizarán el funcionamiento de las entidades que incumplan con los estándares mínimos de prevención del lavado de activos y la financiación del terrorismo, y revocarán la autorización a aquellas que habiéndola obtenido no implementen este tipo de sistemas de prevención.

— Los países deben adoptar medidas para controlar el tránsito de dinero o de instrumentos negociables al portador a través de sus fronteras. Así mismo implementar un sistema de información al cual se reporten las operaciones en divisas superiores a determinada cuantía, por parte de las instituciones financieras y los intermediarios del mercado cambiario.

— Las entidades deben prestar especial atención a las operaciones realizadas desde o hacia países que no hayan acogido o que no apliquen por completo las recomendaciones del GAFI en materia de prevención del lavado de activos y la financiación del terrorismo.

— La investigación del lavado de activos y la financiación del terrorismo debe ser competencia de autoridades revestidas de amplias facultades para garantizar el cumplimiento de la ley. Estas autoridades deben aplicar técnicas de investigación eficaces, como por ejemplo las entregas vigiladas o las operaciones encubiertas. Los países deberían alentar la creación de grupos permanentes especializados en la investigación del lavado de activos y la financiación del terrorismo. Los grupos creados prestarán su colaboración a las autoridades de otros países, como parte de los mecanismos de cooperación internacional en esta materia.

— Los gobiernos deben estimular la armonía y cooperación entre las diferentes agencias u organismos involucrados en la lucha contra el lavado de activos y la financiación del terrorismo. Además deben asegurar que estas agencias u organismos cuenten con los recursos necesarios y suficientes para el adecuado cumplimiento de su labor.

— Se recomienda incluir en las legislaciones nacionales mecanismos o instituciones para impedir que las personas jurídicas puedan ser utilizadas para lavar activos o financiar el terrorismo. Específicamente debe impedirse, que las sociedades que emitan acciones al portador puedan ser utilizadas para esos propósitos.

— Los países deben adoptar mecanismos para garantizar la cooperación internacional en materia de prevención del lavado de activos y financiación del terrorismo, aplicando sin restricciones la Convención de Viena contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas de 1988, la Convención para la Supresión del Financiamiento del Terrorismo de 1999, la Convención de Palermo contra la Delincuencia Organizada Transnacional del año 2000, la Convención del Consejo de Europa sobre Blanqueo de Capitales, Investigación, Incautación y Decomiso de los Productos del Delito, y la Convención Interamericana contra el Terrorismo del año 2002.

— Los países deben prestarse asistencia judicial mutua en forma amplia, eficiente y eficaz. Esto implica prestar la asistencia legal aun en caso

en que no haya doble incriminación, y acceder a las solicitudes de identificación, embargo, congelamiento, incautación y decomiso de los activos lavados, de los recursos que son producto del lavado de activos o del delito subyacente, y de los bienes utilizados para la comisión del lavado de activos o del delito subyacente. Así mismo los Estados aplicarán ampliamente mecanismos de cooperación judicial internacional como la extradición, en esta materia.

3. RECOMENDACIONES DE LA ONU

3.1. Convención de Viena de 1988

Mediante Resolución 39/141 del 14 de diciembre de 1984, la Asamblea General de la Organización de Naciones Unidas solicitó al Consejo Económico y Social de ese mismo organismo, que en el marco de la 31º sesión de la Comisión de Estupefacientes⁽⁷⁾ que tendría lugar el día 14 de febrero de 1985 se tuviera en cuenta como tema prioritario, la preparación de una convención contra el tráfico ilícito de drogas. Con motivo de esta solicitud, el Secretario General preparó el texto inicial de la Convención contra el Tráfico de Drogas y Substancias Estupefacientes, el cual surtió durante algo más de tres años un proceso de revisión que incluyó la discusión por parte de los diferentes gobiernos, de diferentes organismos y comisiones al interior de la ONU, y de varios grupos de expertos internacionales conformados específicamente para ello. Después de este largo proceso, la ONU convocó para que entre el 25 de noviembre y el 20 de diciembre de 1988 se llevara a cabo en Viena la Conferencia para la Adopción de la Convención contra el Tráfico de Drogas y Substancias Estupefacientes, en la cual se adoptó el texto final de la misma⁽⁸⁾.

(7) La comisión de estupefacientes es una comisión orgánica permanente del Consejo Económico y Social de la Organización de Naciones Unidas. Cfr., en la página web oficial de la ONU: <<http://www.un.org/spanish/Depts/dpi/boletin/drogas/fiscalizacion.shtml>> (Consultado el día 21 de octubre de 2009).

(8) La versión en inglés del texto completo de la Convención puede consultarse en la página web: <http://www.unodc.org/pdf/convention_1988_en.pdf> (Consultado el día 21 de octubre de 2009).

La Convención que fue adoptada el 19 de diciembre de 1988 tiene el propósito fundamental de señalar las medidas que deben tomar los Estados parte, para prevenir el tráfico ilícito de drogas y otras substancias estupefacientes. No obstante, en ella se reconoce la existencia de una estrecha relación entre el tráfico ilícito de drogas y otras conductas delictivas, frente a las cuales deben tomarse también medidas de prevención. En lo que se refiere al tema de este trabajo, la Convención reconoce la existencia de una relación entre el tráfico ilícito de drogas y el lavado de activos, así como que esta relación afecta la estabilidad, la seguridad y la soberanía de los Estados. Textualmente se admite que los Estados parte son “conscientes de que el tráfico ilícito genera considerables rendimientos financieros y grandes fortunas que permiten a las organizaciones delictivas transnacionales penetrar, contaminar y corromper las estructuras de gobierno, el comercio legítimo y las empresas financieras, y la sociedad en todos sus niveles”⁽⁹⁾. Por esta razón, la Convención también declara expresamente tener el propósito de que los Estados implementen mecanismos que permitan privar a las organizaciones criminales de los beneficios económicos del delito, de modo que desaparezcan todos los incentivos para el tráfico ilícito de estupefacientes.

Teniendo en cuenta lo anterior, el literal b) del numeral 1 del artículo 3º de la Convención insta a los Estados partes a adoptar en su legislación interna, normas que penalicen la realización de cualquiera de las siguientes conductas:

- “b) i) La conversión o la transferencia de bienes a sabiendas de que ellos proceden de alguno o algunos de los delitos tipificados o de conformidad con el literal a) del presente párrafo, o de un acto de participación en tal delito o delitos, con objeto de ocultar o encubrir el origen ilícito de los bienes o de ayudar a cualquier persona que participe en la comisión de tal delito o delitos a eludir las consecuencias jurídicas de sus acciones, y
- ii) La ocultación o el encubrimiento de la naturaleza, el origen, la ubicación, el destino, el movimiento o la propiedad reales de bienes,

(9) Preámbulo de la Convención.

o de derechos relativos a tales bienes, a sabiendas de que proceden de alguno o algunos de los delitos tipificados de conformidad con el literal a) del presente párrafo o de un acto de participación en tal delito o delitos”⁽¹⁰⁾.

Complementariamente, la Convención entiende que el delito de lavado de activos es cometido mayoritariamente por grupos criminales organizados que actúan internacionalmente, y por esta razón dispone que los Estados parte deben asegurar que los jueces o tribunales competentes estén facultados para agravar las penas y demás consecuencias del delito en circunstancias de particular gravedad, tales como:

- “a) La participación en el delito de un grupo delictivo organizado del que el delincuente forme parte, y
- “b) La participación del delincuente en otras actividades delictivas internacionales organizadas”⁽¹¹⁾.

Para hacer eficaces estas medidas, la Convención insta a las partes a adoptar en su legislación interna normas para el decomiso de los bienes

(10) El texto en inglés es el siguiente: “b) i) The conversion or transfer of property, knowing that such property is derived from any offence or offences established in accordance with subparagraph a) of this paragraph, or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions; ii) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences established in accordance with subparagraph a) of this paragraph or from an act of participation in such an offence or offences”.

(11) El texto en inglés es el siguiente: “The Parties shall ensure that their courts and other competent authorities having jurisdiction can take into account factual circumstances which make the commission of the offences established in accordance with paragraph 1 of this article particularly serious, such as:

- a) The involvement in the offence of an organized criminal group to which the offender belongs;
- b) The involvement of the offender in other international organized criminal activities”.

producto del tráfico ilícito de estupefacientes, o de bienes por valor equivalente. Por medio de esta disposición se pretende que los Estados parte adopten normas que les permitan perseguir no sólo los recursos provenientes del narcotráfico, sino también los bienes que son utilizados para encubrir el origen o la ubicación de tales recursos. De esa manera, los diferentes Estados deben ponerse en condición de decomisar legalmente tanto los bienes obtenidos mediante narcotráfico, como los utilizados con el propósito de lavar dichos activos.

En lo que al tema de este trabajo respecta importante resulta mencionar que en los términos del numeral 2 del artículo 5º, los Estados deben asegurar que las autoridades estén en condiciones de identificar, detectar y embargar preventivamente los bienes susceptibles de decomiso⁽¹²⁾. Debido a esta disposición, la adopción de la Convención exige la emisión de un régimen legal que les permita a las autoridades acceder a la información financiera necesaria para la identificación, detección y embargo de bienes provenientes de narcotráfico, o de bienes adquiridos con dichos recursos. En consecuencia, aunque la Convención no contiene una disposición expresamente referida a la obligación de adoptar una legislación para la prevención del lavado de activos en el mercado financiero, cambiario, bursátil o asegurador, la obligación de garantizar que las autoridades estén en condiciones de identificar los bienes de origen ilícito supone claramente, que los Estados parte deben adoptar normas que permitan la cooperación entre las autoridades públicas y los intermediarios de los sectores financiero, cambiario, bursátil y asegurador. Prueba de lo anterior es que el numeral 4 del artículo 5º *Ibidem* señala claramente:

“A fin de dar aplicación a las medidas mencionadas en el presente artículo, cada una de las partes facultará a sus tribunales u otras autoridades competentes a ordenar a las entidades bancarias, financieras o comerciales poner a disposición sus registros para ser incautados. Las partes no podrán negarse a aplicar las disposiciones del presente pá-

(12) El texto en inglés de la norma es el siguiente: “Each Party shall also adopt such measures as may be necessary to enable its competent authorities to identify, trace, and freeze or seize proceeds, property, instrumentalities or any other things referred to in paragraph 1 of this article, for the purpose of eventual confiscation”.

rrafo amparándose en el secreto bancario”⁽¹³⁾.

Además del decomiso, la Convención también establece que los Estados parte deben adoptar en su legislación interna disposiciones que hagan posible la extradición, no sólo frente al delito de tráfico ilícito de estupefacientes, sino también respecto del delito de lavado de activos. Como consecuencia de lo anterior, en los términos de la Convención, la extradición por el delito de lavado de activos debe ser adoptada por los Estados como mecanismo de cooperación internacional en la lucha contra el tráfico ilícito de estupefacientes, de modo que pueda perseguirse a los lavadores de activos donde quiera que se encuentren después de haber cometido este delito en territorio de otro Estado.

Finalmente, un aspecto muy importante de la Convención es la reglamentación de la asistencia judicial recíproca en materia de tráfico de estupefacientes y lavado de activos. Para los fines de este trabajo es importante mencionar, que el literal f) del numeral 2 del artículo 7º establece que la asistencia judicial debe abarcar: “Entregar originales o copias auténticas de documentos y expedientes relacionados con el caso, inclusive documentación o registros bancarios, financieros, corporativos y comerciales”⁽¹⁴⁾. Igualmente importante resulta señalar, que el numeral 5 del artículo 7º dispone que: “Las partes no invocarán el secreto bancario para negarse a prestar asistencia judicial recíproca con arreglo a este artículo”⁽¹⁵⁾. Como consecuencia de lo dispuesto en la Convención, y así ella no lo disponga expresamente, los Estados parte deben adoptar necesariamente un régimen de cooperación entre las autoridades públicas y los intermediarios de los sectores financiero, cambiario, bursátil y asegurador. De otro modo, los

(13) El texto en inglés de la norma es el siguiente: “In order to carry out the measures referred to in this article, each Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. A Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy”.

(14) El texto en inglés de la norma es el siguiente: “Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes: f) Providing originals or certified copies of relevant documents and records, including bank, financial, corporate or business records”.

(15) El texto en inglés de la norma es el siguiente: “A Party shall not decline to render mutual legal assistance under this article on the ground of bank secrecy”.

Estados no contaría con los mecanismos necesarios para prestar la asistencia judicial recíproca que demanda la Convención.

3.2. Convención de Palermo

La Asamblea General de la Organización de Naciones Unidas aprobó mediante la Resolución 55/25 del 15 de noviembre de 2000, el texto de la Convención contra la Delincuencia Organizada Transnacional llevada a cabo ese mismo año en la ciudad de Palermo (Italia)⁽¹⁶⁾. En los artículos 6º y 7º de la Convención se establecen una serie de medidas que deben ser adoptadas por los Estados parte para prevenir el lavado de activos. La primera tiene que ver con la adopción de una legislación interna, en la que se tipifique como delito autónomo la realización de cualquiera de las siguientes conductas:

- “a) i) La conversión o la transferencia de bienes, a sabiendas de que esos bienes son producto del delito, con el propósito de ocultar o disimular el origen ilícito de los bienes o ayudar a cualquier persona involucrada en la comisión del delito determinante a eludir las consecuencias jurídicas de sus actos;
- “ii) La ocultación o disimulación de la verdadera naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes o del legítimo derecho a éstos, a sabiendas de que dichos bienes son producto del delito;
- “b) Con sujeción a los conceptos básicos de su ordenamiento jurídico:
 - “i) La adquisición, posesión o utilización de bienes, a sabiendas, en el momento de su recepción, de que son producto del delito;

(16) El texto de esta convención puede consultarse en la página web <<http://www.un.org/disarmament/convarms/ArmsTradeTreaty/docs/Background%20documents/Firearms%20Protocol%20-%20S.pdf>> (consultado el día 16 de octubre de 2009).

“ii) La participación en la comisión de cualesquiera de los delitos tipificados con arreglo al presente artículo, así como la asociación y la confabulación para cometerlos, el intento de cometerlos, y la ayuda, la incitación, la facilitación y el asesoramiento en aras de su comisión”.

El artículo 6º prescribe que de cara a la expedición de esa legislación, los Estados parte deben procurar que las normas que tipifiquen el lavado de activos abarquen la mayor cantidad de delitos subyacentes posibles. Esto quiere decir que el delito debería tipificarse de tal manera, que los activos materia de lavado puedan provenir de cualquiera de los delitos previstos en la legislación interna. Como mínimo, la Convención exige que los Estados parte incluyan como delitos subyacentes del lavado de activos los delitos de participación en grupo delictivo organizado (art. 5º), los delitos de corrupción (art. 8º), los delitos de obstrucción a la justicia (art. 23), y aquellos que en los términos del literal b) del artículo 2º son entendidos como “delitos graves”: “Por delito grave se entenderá la conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave”⁽¹⁷⁾.

Así mismo, la Convención dispone que los Estados parte deben tipificar el delito de lavado de activos, de tal manera que este se entienda consumado aun cuando el delito subyacente se hubiera cometido en otro Estado. No obstante, la recomendación es que el delito sea sancionado únicamente cuando el subyacente también sea considerado en la legislación interna del país correspondiente.

En lo que hace a las medidas para la prevención del lavado de activos, el artículo 7º también consagra una serie de recomendaciones que deben ser implementadas por los Estados parte en su legislación interna. La primera de ellas consiste en emitir un régimen amplio de reglamentación y supervisión para los bancos y las instituciones financieras no bancarias. Este régimen debe abarcar también a todos los demás sectores susceptibles de ser utilizados para el lavado de activos, y ha de consagrarse expresamente como mínimo el deber de conocimiento del cliente, el deber de efectuar

(17) Literal b) del artículo 2º de la Convención.

y conservar registros de información, y el deber de reportar operaciones sospechosas. Así mismo, ese régimen debe asegurar que las autoridades gubernamentales y judiciales encargadas de combatir el lavado de activos sean capaces de cooperar e intercambiar información con otros organismos u agencias internacionales. A tal propósito, los Estados parte deben considerar la posibilidad de crear un organismo de inteligencia financiera “que sirva de centro nacional de recopilación, análisis y difusión de información sobre posibles actividades de blanqueo de dinero”⁽¹⁸⁾.

Sumado a lo anterior, los Estados parte deben implementar mecanismos para detectar y vigilar el movimiento transfronterizo de dinero en efectivo, o de títulos negociables al portador. Para ello podrán crear normas imponiendo a los particulares y a las entidades comerciales la obligación de declarar o notificar ante las autoridades, el envío o recepción de transferencias transfronterizas de recursos en efectivo o de títulos negociables al portador.

Un aspecto importante de la Convención es que su artículo 10 prevé la obligación de crear mecanismos, para imputar responsabilidad a las personas jurídicas involucradas en cualquiera de los delitos mencionados allí, y entre los que se encuentra el lavado de activos. Sin embargo, esta no define qué clase de responsabilidad debe imputarse a las personas jurídicas, dejando a discreción de los Estados parte la definición de este aspecto, en función de los principios que orientan su legislación interna. De allí que se prevea la posibilidad de atribuir responsabilidad penal, civil o administrativa a las personas jurídicas, dependiendo de la elección de cada Estado. En cualquier caso, lo que sí se aclara es que la responsabilidad de las personas jurídicas debe ser directa, y con independencia de la responsabilidad penal imputable a las personas naturales que la dirigen o administran.

Por otra parte es importante mencionar, que la Convención extiende a los delitos transnacionales definidos en ella, la mayoría de las recomendaciones que el GAFI había emitido para prevenir el lavado de activos y la financiación del terrorismo. Así por ejemplo, texto contiene una reglamentación general sobre la adopción de mecanismos para el decomiso de

(18) Literal b) numeral 1 artículo 7º de la Convención.

los recursos provenientes de cualquiera de los delitos allí definidos, o de los bienes utilizados para su comisión⁽¹⁹⁾. En ella se prevé que los Estados parte deben implementar las medidas que sean necesarias para obtener la identificación de esos bienes, y lograr el embargo preventivo o la incautación con miras a su eventual decomiso. Además, estas medidas deben permitir que en el evento en que esos bienes se hayan transformado en otros, estos últimos u otros de igual valor puedan ser igualmente decomisados. Todo lo anterior, sin perjuicio de los derechos adquiridos por los terceros de buena fe.

Para que estas medidas sean realmente efectivas, los Estados parte deben promover la adopción de normas que faculten a los tribunales a ordenar la incautación de los documentos bancarios, financieros o comerciales que contengan información útil para identificar los bienes e incautarlos. Así mismo, estas medidas deben ser implementadas de tal forma, que permitan una cooperación internacional eficiente en materia de decomiso de bienes. Frente a esto último, la Convención contiene una regulación específica acerca de la disposición sobre los bienes decomisados, en la cual se señala que las legislaciones internas deben prever que los bienes decomisados sean devueltos o puestos a disposición del Estado solicitante, para que éste pueda indemnizar a las víctimas o restituirlos a sus legítimos propietarios.

Además del decomiso, la Convención contiene una reglamentación para que los Estados parte hagan uso de la extradición como mecanismo de cooperación judicial internacional en la lucha contra la delincuencia transnacional. Entre los muchos aspectos que son materia de regulación, el artículo 16 indica que la extradición debe proceder respecto de los delitos definidos allí, cuando la persona responsable se encuentre en el territorio de alguno de los Estados parte luego de haber cometido el delito en otro. Esta extradición ha de proceder siempre bajo la condición, de que la conducta por la cual se solicita sea considerada como delito en el Estado en el cual se encuentra la persona requerida. Adicionalmente, la Convención insta a los Estados partes a que sin perjuicio de los principios y reglas contenidas en el derecho interno hagan lo necesario, para adoptar procedi-

(19) Artículos 12, 13 y 14 de la Convención.

mientos ágiles para la extradición por delitos transnacionales. Igualmente, insta a los Estados a celebrar entre sí acuerdos bilaterales o multilaterales para hacer eficiente el mecanismo de la extradición.

Otro aspecto sumamente relevante es que la Convención recomienda la utilización de técnicas apropiadas de investigación (entrega vigilada, vigilancia electrónica, operaciones encubiertas, etc.) para los delitos transnacionales, y recomienda enfáticamente la asistencia judicial recíproca entre los Estados en esta materia. También exige a los Estados parte prestar la más amplia asistencia judicial en las investigaciones, procesos y actuaciones judiciales relacionadas con los delitos definidos en ella, sin menoscabo del derecho interno y sin perjuicio de las investigaciones y procesos penales que adelantan las autoridades a quienes se solicita colaboración.

De acuerdo con el numeral 3 del artículo 18, los Estados parte pueden solicitar asistencia judicial para los siguientes propósitos:

- “a) Recibir testimonios o tomar declaración a personas;
- “b) Presentar documentos judiciales;
- “c) Efectuar inspecciones e incautaciones y embargos preventivos;
- “d) Examinar objetos y lugares;
- “e) Facilitar información, elementos de prueba y evaluaciones de peritos;
- “f) Entregar originales o copias certificadas de los documentos y expedientes pertinentes, incluida la documentación pública, bancaria y financiera, así como la documentación social o comercial de sociedades mercantiles;
- “g) Identificar o localizar el producto del delito, los bienes, los instrumentos u otros elementos con fines probatorios;
- “h) Facilitar la comparecencia voluntaria de personas en el Estado parte requirente, y

“i) Cualquier otro tipo de asistencia autorizada por el derecho interno del Estado parte requerido”⁽²⁰⁾.

En relación con el tema que ocupa este trabajo llama especialmente la atención, que el numeral 8 del artículo 18 prescribe expresamente que “los Estados parte no invocarán el secreto bancario para denegar la asistencia judicial recíproca con arreglo al presente artículo”. De esta manera, la asistencia judicial en materia de lavado de activos impone como estándar mínimo internacional, el levantamiento del secreto bancario frente a las investigaciones adelantadas por las autoridades de cualquiera de los Estados parte en la Convención. Disposición que, por lo demás, resulta acorde con las recomendaciones efectuadas tanto por el GAFI como por el Comité de Basilea respecto de este mismo tema.

Finalmente, el artículo 31 dispone que los Estados parte procurarán formular y evaluar políticas y propuestas para la prevención de la delincuencia transnacional. En materia de lavado de activos, las medidas sugeridas deben impedir que las organizaciones criminales puedan participar en los mercados lícitos con los recursos provenientes de actividades delictivas. Para ello debe estimularse la cooperación entre las autoridades públicas encargadas de combatir esas formas de criminalidad. También es necesaria la creación de normas para salvaguardar la integridad de las entidades públicas y privadas expuestas al riesgo de lavado de activos, y la expedición de códigos de conducta para aquellos profesionales claves en materia de prevención (abogados, contadores, revisores fiscales, notarios públicos, etc.). Además, los Estados parte deben impedir la utilización de las personas jurídicas para la comisión del delito de lavado de activos, mediante la implementación de medidas tales como: la creación de un registro de las personas involucradas en la constitución, gestión y financiación de personas jurídicas; la posibilidad de inhabilitar las personas judiciales involucradas en actividades delictivas; la creación de un registro de personas inhabilitadas para actuar como directores, representantes o administradores de personas jurídicas; o el intercambio de información sobre personas jurídicas con otros Estados.

(20) Numeral 3 artículo 18 de la Convención.

4. RECOMENDACIONES DEL COMITÉ DE BASILEA PARA EL CONOCIMIENTO DEL CLIENTE

En octubre de 2001, el Comité de Basilea publicó el documento titulado “Debida diligencia con la clientela de los bancos”⁽²¹⁾, el cual contiene un conjunto de recomendaciones para el adecuado conocimiento del cliente por parte de las entidades financieras⁽²²⁾. Estas recomendaciones fueron producto de un estudio adelantado por el Grupo de Trabajo sobre Banca Transterritorial (equipo integrado por miembros del Comité de Basilea y del Grupo Extraterritorial de Supervisores Bancarios), acerca de los procedimientos utilizados por diversas entidades financieras para el conocimiento del cliente (*know your customer, KYC* por sus siglas en inglés). Las recomendaciones formuladas tuvieron principalmente en cuenta los resultados de una encuesta interna de banca transterritorial realizada por el Comité de Basilea en el año de 1999, la cual determinó que los mecanismos adoptados por las entidades financieras eran insuficientes.

Como punto de partida, en este documento se explica que sin los mecanismos adecuados para el conocimiento del cliente, las entidades po-

-
- (21) Documento disponible en la página web <<http://www.bis.org/publ/bcbs85s.pdf>> (consultado el 7 de octubre de 2009).
- (22) En este documento se explica que “El Comité de Basilea ha emitido orientaciones sobre KYC en tres documentos diferentes, los cuales reflejan la evolución del pensamiento de supervisión con el tiempo. Estos documentos son: ‘La Prevención del Uso Delictivo del Sistema Bancario con el Propósito de Lavado de Dinero’, emitido en 1988, en el que se estipula los principios éticos básicos y se insta a los bancos a instalar procedimientos eficaces para identificar a sus clientes, rechazar transacciones sospechosas y cooperar con los organismos encargados de hacer cumplir la legislación. Los ‘Principios Básicos para la Supervisión Bancaria Eficiente’ de 1997 sostienen, dentro de una discusión más general sobre controles internos, que los bancos deben contar con políticas, prácticas y procedimientos adecuados, incluyendo reglas estrictas de ‘conozca a su cliente’. Más concretamente, los supervisores deben alentar la adopción de las recomendaciones pertinentes del FATF. Estas recomendaciones se refieren a la identificación de clientes y al mantenimiento de registros, mayor diligencia por parte de las instituciones financieras para detectar transacciones sospechosas e informar sobre ellas, y medidas para tratar con países cuyas reglas contra el lavado de dinero son insuficientes. La ‘Metodología de los Principios Básicos’ de 1999 explica con más detalle los Principios Básicos, e incluye una lista de criterios esenciales y complementarios” (BCBS, *Debida diligencia con la clientela de los bancos*, p. 11).

drían asumir riesgos reputacionales, operativos, legales y de concentración que podrían conllevar costos financieros importantes⁽²³⁾. Por esta razón, el propósito de ese trabajo es ofrecer recomendaciones para el conocimiento del cliente desde una perspectiva general, y no sólo vinculada a la preventión del lavado de activos. En este sentido, las recomendaciones ofrecidas no sustituyen sino que complementan las realizadas por otros organismos como el GAFI en esa misma materia.

Uno de los pilares de este documento es la idea de que la efectividad de los mecanismos para conocimiento del cliente exige más actividades que la simple identificación al momento de apertura de una cuenta o de la adquisición de un producto o servicio financiero. Por este motivo se recomienda a las entidades adoptar un sistema para el conocimiento del cliente, que cuente al menos con los siguientes elementos esenciales.

4.1. Política clara y expresa para la aceptación de clientes

En primer lugar, el Comité de Basilea recomienda a las entidades fijar una descripción de los tipos de clientes que podrían representar un riesgo mayor al promedio. A tal efecto sugiere “tomar en cuenta factores tales como los antecedentes del cliente, su país de origen, si ocupa un puesto relevante en el sector público o privado, las cuentas vinculadas, actividad de negocios u otros indicadores de riesgo”⁽²⁴⁾. A partir de la definición de los perfiles de riesgo de los clientes, las entidades deben diseñar políticas gra-

(23) Textualmente se afirma allí: “La inadecuación o falta de normas KYC puede someter a los bancos a riesgos serios con sus clientes y contrapartes, especialmente riesgos de reputación, operativos, legales y de concentración. Cabe destacar que todos estos riesgos están relacionados entre sí. Sin embargo, cualquiera de ellos puede resultar en un costo financiero considerable para los bancos (por ejemplo, a raíz de la retirada de fondos por parte de los depositantes, el cese de servicios interbancarios, las demandas interpuestas contra del banco, los gastos de investigación, el embargo y la congelación de haberes, y los préstamos incobrables), así como en la necesidad de consagrar una cantidad considerable de tiempo y energía de gestión para resolver los problemas que surgen” (BCBS, *Debida diligencia con la clientela de los bancos*, p. 10). En este documento se ofrece además una definición de las diferentes categorías de riesgo mencionadas.

(24) Ibíd., p. 12.

duales de aceptación, de manera que cuanto mayor sea el perfil de riesgo del cliente mayor deberá ser el control y la diligencia para su vinculación a la entidad. Todo lo anterior sin permitir que las políticas de aceptación restrinjan el acceso de los ciudadanos al sistema financiero, especialmente a los sectores menos favorecidos de la sociedad.

4.2. Mecanismos para un adecuado y oportuno conocimiento del cliente

En segundo lugar, el Comité de Basilea establece en este documento algunos criterios generales para la identificación del cliente, y otros específicos aplicables en ciertas circunstancias especiales que son analizadas allí⁽²⁵⁾. En lo referente a los criterios generales, el Comité recomienda a las entidades adoptar procedimientos sistemáticos y documentados para conocer a sus clientes antes de aceptar su vinculación a la entidad. Estos deben aplicarse en principio al comienzo de la relación comercial, pero la entidad también debe ponerlos en práctica en cualquier momento en que perciba que la información y/o la documentación que tiene sobre un cliente son insuficientes. Estos procedimientos deben ser ejecutados por funcionarios que no se beneficien con la vinculación del cliente, por ejemplo, mediante el reconocimiento de comisiones o el cumplimiento de metas laborales. Esto implica que la decisión sobre la vinculación del cliente debe depender de un funcionario imparcial que pueda llevar a cabo todas las actividades necesarias para su adecuada identificación, tales como la recolección y verificación de la información personal y comercial aportada, el estudio de la documentación suministrada y una entrevista personal. Además, para el conocimiento del cliente no es suficiente la obtención y verificación de la información personal y comercial suministrada, y por esa razón las entidades deben emitir una regulación en la que se defina qué tipo

(25) En este apartado también se lleva a cabo la siguiente definición de cliente: “A efectos del presente documento, un cliente incluye: la persona o entidad que mantiene una cuenta con el banco o aquella para la que se mantiene la cuenta (es decir, el usufructuario); los beneficiarios de transacciones efectuadas por intermediarios profesionales, y toda persona o entidad ligada a una transacción financiera y que pudiera representar un riesgo considerable de reputación o de otro tipo al banco” (cfr. ibid., p. 12).

de información relativa a las operaciones de los clientes será registrada, analizada y conservada. Para terminar, el Comité recomienda de modo enfático a las entidades no realizar negocios con personas que insistan en el anonimato, que se rehúsen a suministrar la información necesaria para su identificación a satisfacción de la entidad, o que hayan suministrado información o documentación falsa o inexacta. Esto significa que no se recomienda funcionar bajo el modelo de cuentas cifradas (numeradas) que permitan ocultar la identidad del cliente.

4.3. Seguimiento continuo de las cuentas de alto riesgo

El Comité de Basilea recomienda a las entidades conocer las actividades habituales y razonables de sus clientes, al punto de poder identificar aquellas transacciones que se salen del patrón de normalidad. La identificación de estas transacciones inusuales es útil para seleccionar aquellas operaciones que deben ser evaluadas con detenimiento, y reconocer aquellas sospechosas de ser constitutivas de un delito. Esta identificación requiere que las entidades cuenten con sistemas que les permitan reconocer patrones de actividad anómalos en sus clientes, por ejemplo mediante la fijación de límites o rangos de normalidad para las diferentes operaciones, y la clasificación de los clientes en categorías de acuerdo con ellos. La adopción de este tipo de sistemas es importante, porque suministran el conocimiento que necesitan las entidades para identificar y reportar las operaciones sospechosas a las autoridades, en los casos en que tengan la obligación de hacerlo.

Por otra parte, el Comité recomienda que las entidades adopten sistemas adecuados para identificar las cuentas de alto riesgo, y que ejerzan sobre éstas una vigilancia más intensa y rigurosa. A tal propósito, las entidades deben definir criterios para identificar este tipo de cuentas, tales como el país de origen, la procedencia de los fondos, el tipo de transacciones, etc. Los sistemas adoptados para identificar y vigilar este tipo de cuentas deben asegurar que la entidad esté en condiciones de obtener información de terceros que la alerten sobre situaciones de riesgo, y de actualizar permanentemente el perfil de riesgo de sus clientes para detectar oportunamente cualquier cambio. En resumen, lo importante es que frente a este tipo de cuentas la entidad fije políticas y procedimientos claros que

aseguren una vigilancia permanente y adecuada de sus operaciones, y de las operaciones de las personas o cuentas asociadas a ellas.

4.4. Definición de la gestión de riesgos

Finalmente, el Comité de Basilea recomienda que las entidades adopten y apliquen un modelo de gestión eficaz para estos riesgos. En el documento se menciona por ejemplo la capacitación de funcionarios, la implementación de rutinas de vigilancia sobre el estado de los sistemas, controles y procedimientos adoptados, y la distribución de roles y funciones al interior de la entidad. Así mismo se recomienda a las entidades, que los canales y procedimientos para la notificación de las operaciones sospechosas estén claramente definidos por escrito, y al alcance de todos los funcionarios. Igualmente, el Comité llama la atención sobre la importancia que tiene la auditoría interna y externa en el modelo de gestión adoptado, subrayando que la verificación aleatoria y por muestreo permite identificar fallas en los sistemas implementados, y notificarlas al órgano de administración competente para que se adopten los correctivos necesarios. En este sentido, el documento recuerda que la auditoría permite asegurar que los sistemas implementados satisfagan los requisitos mínimos exigidos por la legislación interna en esta materia.

5. RECOMENDACIONES DEL FORO CONJUNTO ENTRE EL COMITÉ DE BASILEA, EL IAIS Y LA IOSCO

El Comité de Supervisión Bancaria de Basilea, la Asociación Internacional de Supervisores de Seguros (IAIS, por sus siglas en inglés) y la Organización Internacional de Comisiones de Valores (IOSCO, por sus siglas en inglés) emitieron conjuntamente en junio de 2003 un documento titulado “*Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism*”⁽²⁶⁾, el cual contiene una serie de reco-

(26) El documento disponible en la página web <<http://www.bis.org/publ/joint05.pdf?noframes=1>> (consultado el 14 de octubre de 2009).

mendaciones para la prevención del lavado de activos y la financiación del terrorismo en los diferentes sectores representados por cada una de estas organizaciones: bancario, asegurador y bursátil. Más allá de la especificidad de las recomendaciones para cada sector, este documento proporciona una mirada global a los estándares comunes a los tres sectores en materia de prevención del lavado de activos y financiación del terrorismo. Allí también se evalúan los vacíos y las inconsistencias de las propuestas y recomendaciones realizadas anteriormente, y se estudia para cada sector la relación entre las instituciones y sus clientes, enfocándose en los productos y servicios que son especialmente vulnerables al lavado de activos o a la financiación del terrorismo⁽²⁷⁾.

Una exposición de las recomendaciones ofrecidas por estos organismos para cada uno de los tres sectores no es posible aquí, y por ello se recomienda al lector remitirse directamente al documento. Ahora bien, en lo que respecta a los estándares comunes para dichos sectores, este documento sigue en lo fundamental Las cuarenta recomendaciones del GAFI, entre las cuales menciona expresamente las siguientes:

- Identificación y conocimiento del cliente.
- Monitoreo continuo de cuentas y transacciones.
- Registro, conservación y reporte de operaciones sospechosas.
- Controles y auditoría interna.
- Códigos de conducta.
- Cooperación entre supervisores y otras autoridades competentes.

No obstante lo anterior, el documento no sólo se limita a reiterar las recomendaciones del GAFI, sino que realiza además un importante apor-

(27) La última actualización de este documento es de enero de 2005, y está disponible en la página web <<http://www.bis.org/publ/joint11.pdf?noframes=1>> (consultado el 14 de octubre de 2009).

te en materia de prevención del lavado de activos y financiación del terrorismo, formulando algunas recomendaciones comunes a los tres sectores. La más importante de ellas tiene que ver con la adopción de mecanismos de prevención por parte de los grupos económicos (*holding company*) que realizan simultáneamente actividades financieras, aseguradoras y bursátiles a través de las diferentes instituciones que lo integran. El documento toma especialmente en consideración que en tales casos es ineficiente y costoso, que cada una de las entidades vinculadas realice de forma independiente todas las actividades de prevención de lavado de activos y financiación del terrorismo. Por esta razón se recomienda en esos casos implementar mecanismos y procesos de prevención que atraviesen de forma transversal el grupo económico, asegurando que el sistema ejerza una protección global.

Especial atención se presta en este documento al cumplimiento de la debida diligencia frente a los clientes (*Customer Due Diligence, CDD* por sus siglas en inglés), por parte de este tipo de holding. Allí se reconoce que el cumplimiento de la debida diligencia frente a los clientes por parte de las entidades pertenecientes a un grupo económico presenta problemas únicos que no tienen lugar en otro tipo de instituciones. Por ejemplo, el cliente de una de las entidades vinculadas a un sector del grupo normalmente puede llegar a querer realizar negocios con una de las entidades vinculadas a otro sector diferente, y no tiene sentido que las actividades de identificación y conocimiento del cliente se dupliquen por completo. Además debe tenerse en cuenta, que los problemas que surgen de la relación con el cliente no afectan exclusivamente a la entidad con la que se vincula contractualmente, sino que puede lesionar la reputación de todo el grupo económico. Debido a esta circunstancia, este foro conjunto recomienda que los grupos económicos adopten sistemas de identificación y conocimiento del cliente que les permita detectar cuándo una persona es simultáneamente cliente de dos o más instituciones vinculadas. Estos sistemas deben permitir monitorear la actividad de todos sus clientes, compartir esta información de forma eficiente, y alertar al grupo cuando una persona utilice sus servicios en cualquiera de los diferentes sectores.

Esto no significa que los requerimientos de debida diligencia frente a los clientes deban ser los mismos para las instituciones bancarias, aseguradoras y bursátiles vinculadas a un mismo grupo económico. La distin-

ta naturaleza de las actividades y operaciones de cada entidad justifica las diferencias en los requerimientos de debida diligencia frente a los clientes. Lo importante es optimizar los recursos y hacer eficiente el sistema, logrando que aquellos requerimientos comunes puedan ser cumplidos por una sola de las entidades vinculadas, y que la información obtenida pueda ser oportuna y adecuadamente compartida.

A tal efecto, todas las entidades vinculadas al grupo deben poder confiar en el cumplimiento de la debida diligencia frente a los clientes por parte de cualquiera de ellas. Esto significa que el grupo debe ser exigente en el cumplimiento de los estándares de debida diligencia por parte de las entidades vinculadas, de manera que las actividades de identificación y conocimiento de los clientes llevados a cabo por cualquiera de ellas puedan ser confiables para todas. Esto no quiere decir que el cliente recomendado o referido por una entidad del grupo deba ser necesariamente eximido de todos los controles establecidos, sino que debe ser sometido únicamente a los controles que no hubieran sido aplicados por la entidad que lo refiere o recomienda. Ello es especialmente razonable en aquellos casos en los que la información necesaria para cumplir con la diligencia debida frente a un cliente en un sector específico, resulta insuficiente para cumplir con esa diligencia debida en otro sector diferente. En esos casos, la entidad debería solicitar al cliente complementar la información que falta, dependiendo de la naturaleza de los productos o servicios solicitados por él. Igual procedimiento debe seguirse cuando un cliente solicita los servicios del grupo dentro del mismo sector, pero en un país diferente en el que los requerimientos legales de diligencia debida sean más estrictos.

6. CONVENIO DEL CONSEJO DE EUROPA SOBRE BLANQUEO DE CAPITALES

El comité de ministros de la Unión Europea aprobó y abrió a firmas en noviembre de 1990 el Convenio del Consejo de Europa sobre Blanqueo de Capitales, Investigación, Incautación y Decomiso de los Productos del Delito, el cual entró en vigor en septiembre de 1993. Este documento fue actualizado mediante la Convención del 16 de mayo de 2005 aprobada en Varsovia, mediante la cual se complementaron las medidas para prevenir

el lavado de activos con otras destinadas a combatir la financiación del terrorismo, en aplicación de lo previsto en la Convención de la ONU para la *Supresión del Financiamiento del Terrorismo* de 1999⁽²⁸⁾.

Siguiendo la línea de las recomendaciones del GAFI y de las diferentes convenciones de la ONU, la sección primera del capítulo tercero del Convenio del Consejo de Europa reitera la necesidad de que los Estados adopten en su legislación interna normativas que tipifiquen el lavado de activos y la financiación del terrorismo como delitos autónomos. Igualmente pide a las partes que adopten mecanismos que permitan: a) El decomiso de bienes de origen ilícito o de bienes utilizados para la comisión de delitos; b) El congelamiento, avalúo y confiscación de tales bienes; c) La atribución de responsabilidad a las personas jurídicas involucradas en esos delitos, y d) La implementación de técnicas apropiadas de investigación. Adicionalmente, el capítulo cuarto de este Convenio contiene disposiciones relacionadas con la obligación de adoptar medidas eficaces y eficientes para la cooperación internacional en materia de asistencia judicial recíproca, para el intercambio de evidencias y ayuda en la investigación, y en la confiscación de bienes.

En lo que al tema específico de este trabajo se refiere, la sección segunda del capítulo tercero del Convenio establece una serie de medidas importantes para el control del lavado de activos y la financiación del terrorismo en el sector financiero. El artículo 12 prescribe que los Estados deben adoptar legislaciones que permitan la creación de unidades de inteligencia financiera (*Financial Intelligence Unit*, FIU), asegurándose que éstas tengan acceso oportuno a la información financiera, administrativa y jurídica que requiera para el cumplimiento de sus funciones, incluyendo el análisis de los reportes de operaciones sospechosas.

Complementariamente, el artículo 13 dispone que los Estados deben adoptar un régimen interno completo para la supervisión y regulación bancaria en materia de prevención del lavado de activos y la financiación

(28) El texto completo del Convenio está disponible en la página web: <<http://conventions.coe.int/Treaty/EN/Treaties/Word/198.doc>> (consultado el 26 de octubre de 2009).

del terrorismo. Por disposición expresa del Convenio, el régimen interno adoptado debe tomar en cuenta los estándares internacionales existentes en esta materia, especialmente las recomendaciones impartidas por el GAFI, e incluir como mínimo lo siguiente:

1. Exigir a las personas naturales o jurídicas vinculadas a actividades especialmente expuestas al riesgo de lavado de activos, que establezcan y verifiquen la identidad de sus clientes, y en caso de ser necesario la de los beneficiarios finales de sus operaciones. A tal efecto es necesario imponer a estas personas la obligación de conducir sus negocios con la debida diligencia frente a sus clientes, tomando siempre en cuenta la necesidad de gestionar y reducir el riesgo al que se encuentran expuestas.
2. Exigir a las personas naturales o jurídicas vinculadas a actividades especialmente expuestas al riesgo de lavado de activos que reporten las operaciones sospechosas. Esta obligación de reporte debe estar sujeta a salvaguardas para la persona o entidad que reporta, a efectos de que las medidas sean eficaces.
3. Exigir a las personas naturales o jurídicas vinculadas a actividades especialmente expuestas al riesgo de lavado de activos, que conserven registros sobre la identidad y las operaciones de sus clientes, que capaciten adecuadamente sus empleados en materia de prevención de este tipo de actividades delictivas, y que adopten políticas y procedimientos ajustadas al tamaño y naturaleza de su negocio para la gestionar los riesgos a que se encuentran expuestos.
4. Prohibir a las personas naturales o jurídicas vinculadas a actividades especialmente expuestas al riesgo de lavado de activos, que informen a sus clientes el hecho de que alguna de sus operaciones haya sido reportada como sospechosa.
5. La medidas necesarias para asegurarse que las personas naturales o jurídicas vinculadas a actividades especialmente expuestas al riesgo de lavado de activos sean efectivamente monitoreadas y supervisadas por las autoridades, de modo que se garantice el cumplimiento de las normas sobre prevención adoptadas en la legislación interna.

6. Complementariamente, los Estados parte deben adoptar en su legislación interna normas para controlar el tránsito de dinero en efectivo y de instrumentos negociables al portador a través de sus fronteras.

Para asegurar que el régimen interno adoptado por los Estados sea realmente efectivo, el artículo 14 del Convenio exige que se adopten normas que aseguren que las unidades de inteligencia financiera, o cualquier otra autoridad competente, pueda suspender o negar la autorización para que una operación sospechosa de estar vinculada al lavado de activos pueda seguir adelante, hasta tanto la sospecha no sea confirmada o desvirtuada. Esta facultad para suspender o negar la autorización para realización de operaciones financieras debe restringirse, única y exclusivamente, a aquellos casos en los cuales aquella haya sido fundadamente reportada como sospechosa. Esto último en armonía con las previsiones adoptadas por cada Estado acerca de los términos, plazos y condiciones en que la suspensión o negación de la autorización puede proceder.

Finalmente, un tema muy importante regulado en el capítulo quinto del Convenio de la Unión Europea es la cooperación internacional entre unidades de inteligencia financiera. El artículo 46 regula no sólo las condiciones para la formulación de una solicitud de información, para la entrega de la información y para el manejo y utilización de la información trasmisida entre unidades de inteligencia financiera, sino también las medidas que deben adoptar internamente los Estados para asegurar desde su legislación local la eficacia de la cooperación internacional. Por ejemplo, el Convenio establece en ese capítulo que los Estados parte deben asegurarse de que su unidad de inteligencia financiera esté en capacidad de reunir, analizar y si es necesario investigar la información sobre cualquier hecho que pueda ser indicador de lavado de activos. Así mismo, las unidades de inteligencia financiera deben estar habilitadas para intercambiar espontáneamente o por solicitud, cualquier información que sea relevante para procesar, analizar y si es necesario investigar datos sobre transacciones financieras sospechosas de ser constitutivas de lavado de activos, o sobre las personas naturales o jurídicas relacionadas con esas transacciones. Además, para asegurar la efectividad de la cooperación internacional, el Convenio establece que cada Estado debe asegurar que el cumplimiento de las funciones atribuidas a la unidad de inteligencia financiera no se verá afectada por problemas internos, sin importar si el estatus de

esa unidad en el derecho local es el de una entidad administrativa, policial o jurisdiccional. Y por último, el artículo 47 del Convenio señala que los Estados deben adoptar en su legislación interna medidas, tendientes a asegurar que las unidades de inteligencia financiera tengan las facultades necesarias para prestar colaboración a otras unidades extranjeras en materia de control de operaciones sospechosas. Este tipo de normativa debe garantizar que cualquier unidad de inteligencia financiera pueda prestar colaboración a sus homólogas, tomando las medidas urgentes que sean necesarias para suspender o negar la autorización para la realización de operaciones sospechosas.

7. RECOMENDACIONES DEL GRUPO EGMONT⁽²⁹⁾

Representantes de las unidades de inteligencia financiera de 24 países y 8 organizaciones internacionales se reunieron el 9 de junio de 1995 en el Palacio Egmont Arenberg en Bruselas, y decidieron crear un grupo informal cuyo objetivo es facilitar la cooperación internacional en materia de prevención del lavado de activos y financiación del terrorismo⁽³⁰⁾. Actualmente el Grupo Egmont se reúne periódicamente tres veces al año para compartir experiencias, y tratar temas relacionados con cooperación en materia de intercambio de información y capacitación. Este Grupo es actualmente el principal *foro mundial de unidades de inteligencia financiera*; a él se encuentran vinculadas más de 101 unidades, y lleva a cabo diversas actividades para fomentar la cooperación internacional y el mejoramiento de las medidas existentes en los diferentes países para la prevención del lavado de activos.

En desarrollo de su objeto, el Grupo Egmont ha producido varios documentos en los cuales formula recomendaciones para la prevención del lavado de activos, y específicamente para facilitar y estimular la cooperación internacional mediante el intercambio de información entre unidades

(29) Grupo Egmont de Unidades de Inteligencia Financiera (Grupo Egmont).

(30) La página web oficial del Grupo Egmont es <<http://www.egmontgroup.org/>>. Allí puede encontrarse toda la información sobre su origen, estructura, funcionamiento, etc.

de inteligencia financiera. Entre los documentos más destacados producidos por este organismo encontramos los siguientes: “Best Practices for the Exchange of Information Between Financial Intelligence Units” (*Mejores prácticas para intercambio de información entre unidades de inteligencia financiera*, 2004); “Information Paper on Financial Intelligence Units and the Egmont Group” (*Documento informativo sobre las unidades de inteligencia Financiera y el Grupo Egmont*, septiembre de 2004); “Statement of Purpose of the Egmont Group of Financial Intelligence Units” (*Declaración de propósitos de las unidades de inteligencia financiera del Grupo Egmont*, junio de 2004), y “Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases” (*Principios para el intercambio de información entre unidades de inteligencia financiera en casos de lavado de activos y financiación del terrorismo*, junio de 2001)⁽³¹⁾.

En lo fundamental, todos los documentos producidos por el Grupo Egmont sugieren que las unidades de inteligencia financiera deben tener la posibilidad de compartir libremente información entre ellas, sobre la base del mutuo acuerdo y la reciprocidad, y mediante procedimientos que faciliten el entendimiento entre sí. Este intercambio debe tener como objetivo recoger toda la información disponible que pueda llegar a ser relevante, para el análisis o investigación de transacciones financieras o de personas involucradas en procesos sobre lavado de activos y financiación del terrorismo. Para cumplir dicho objetivo, todas las unidades de inteligencias vinculadas al Grupo deben trabajar para reforzar los mecanismos legales nacionales que les permiten acceder a información financiera relevante en materia de lavado de activos y financiación del terrorismo, luchando para que las normas internas sobre reserva de información no constituya un obstáculo para la cooperación internacional en esta materia. Así mismo, el Grupo estimulará a las unidades de inteligencia financiera a celebrar entre ellas acuerdos, y adoptar mecanismos que permitan resolver caso por caso los problemas específicos que surjan en materia de intercambio de información.

(31) La versión en inglés de estos documentos están disponibles en la página web oficial del Grupo Egmont: <<http://www.egmontgroup.org/library/egmont-documents>> (consultado el 10 de noviembre de 2009).

Adicionalmente, diversos documentos producidos por el Grupo Egmont indican que la cooperación internacional en materia de intercambio de información se sustenta en la confianza mutua entre unidades de inteligencia financiera. Como consecuencia de ello se ha definido como principio fundamental de cooperación internacional en materia de prevención del lavado de activos, que las solicitudes de intercambio de información entre unidades de inteligencia financiera deben revelar los datos mínimos que sean necesarios, en orden a determinar los propósitos para los cuales se utilizará la información solicitada, la razonabilidad de la solicitud y su procedibilidad conforme a la legislación nacional correspondiente. Esto demarca que la información intercambiada sólo puede ser utilizada para los propósitos definidos en la solicitud, y que la unidad de inteligencia financiera receptora no puede entregarla a una tercera parte ni utilizarla en procesos administrativos o judiciales sin el previo consentimiento de la unidad que la entregó. Más aún, las unidades de inteligencia financiera deben tomar medidas para asegurar que la información intercambiada sea conservada bajo reserva en condiciones óptimas de seguridad, lo cual implica adoptar sistemas de protección y provisiones de confidencialidad suficientes.

Igualmente, la relación de los requisitos mínimos que deben cumplir las solicitudes de intercambio de información y sus respuestas se encuentran en el documento titulado “Best Practices for the Exchange of Information Between Financial Intelligence Units” (*Mejores prácticas para intercambio de información entre unidades de inteligencia financiera*, 2004). Entre los aspectos más relevantes de este documento se prevé como regla general, que el intercambio de información no debe ser obstaculizado por razón de la naturaleza de la solicitud (administrativa, policial, judicial, etc.), y que las diferencias en la manera como se han definido (tipificado) los delitos en cada legislación no debe hacer inoperantes los mecanismos de cooperación internacional en esta materia. Así mismo se dispone, que los intercambios de información deben llevarse a cabo de la manera más informal y expedita posible, pero garantizando la protección de la privacidad y confidencialidad de los datos compartidos. En este documento se sugiere también que la comunicación entre las unidades de inteligencia financiera debe ser directa, en lo posible sin la presencia de intermediarios, y las solicitudes de intercambio de información sólo pueden ser negadas cuando ello se justifique por razones tales como: porque la entrega de la

información pueda afectar una investigación penal en curso, porque la solicitud resulte desproporcionada y pueda lesionar los intereses legítimos de una persona natural o jurídica, porque de alguna manera afecta los intereses del Estado, o porque no es conforme a los principios del derecho interno. En cualquier caso, la negación de una solicitud de intercambio de información debe ser suficientemente motivada y justificada.

8. RECOMENDACIONES DE LA CICAD

La Comisión Interamericana para el Control del Abuso de Drogas (CICAD) es una institución de la Organización de Estados Americanos establecida en 1986, para resolver el problema del consumo de drogas en el hemisferio. Esta Comisión está conformada por los representantes de los 34 países miembros, y se reúne dos veces al año para adoptar medidas tendientes a promover la cooperación y coordinación de los Estados alrededor de la lucha contra el abuso de drogas.

Una de las principales políticas adoptadas por la Comisión consiste en promover el mejoramiento de las leyes nacionales para el control del lavado de activos. A través de esta política se pretende privar a los productores y traficantes de droga del producto de sus delitos, como medida para desestimular la realización de este tipo de conductas. El objetivo de la Comisión es lograr que mediante una legislación más eficaz en materia de control de lavado de activos, la producción y el tráfico de drogas ilícitas sea una actividad cada vez menos lucrativa.

El control de lavado de activos como parte de una estrategia más amplia contra el abuso de drogas responde a una política ampliamente reconocida por la Organización de Estados Americanos en varias de las sesiones de esta Comisión.

Los jefes de Estado de los diferentes países miembros de la Organización han declarado en diversas cumbres, su propósito común de luchar contra el lavado de activos como medida para combatir el abuso de drogas, el terrorismo internacional y la delincuencia organizada transnacional. Así, en el marco de la II Cumbre de las Américas llevada a cabo en Santiago de Chile en 1996 los jefes de Estado de los países miembros declararon lo siguiente:

“Daremos nuevo impulso a la lucha contra la corrupción, el lavado de dinero, el terrorismo, el tráfico de armas y el problema de las drogas, incluyendo el uso indebido. Así mismo, trabajaremos conjuntamente para asegurar que los delincuentes no encuentren un refugio seguro en ninguna parte del Hemisferio. Estamos determinados a continuar por este camino”⁽³²⁾.

Manifestación que fue ratificada en la Declaración conjunta producida por los representantes de todos los Estados asistentes a la III Cumbre de las Américas realizada en Quebec en el año 2001, al afirmar que los diferentes gobiernos:

“Instrumentarán estrategias colectivas, incluyendo las que surgen de las Reuniones de Ministros de Justicia de las Américas, para fortalecer la capacidad institucional de los Estados en el intercambio de información y evidencias, concretando acuerdos internacionales relacionados con asistencia jurídica mutua que procedan; elaborarán y difundirán informes nacionales y fortalecerán la cooperación, buscando el apoyo técnico y financiero de las organizaciones multilaterales y bancos de desarrollo multilaterales, cuando corresponda, para combatir conjuntamente las nuevas formas de delincuencia transnacional, incluyendo el tráfico de personas, el lavado de dinero y de productos del delito y del delito cibernético;

“Revisarán políticas y leyes nacionales para mejorar la cooperación en áreas tales como la asistencia jurídica mutua, extradición y deportación a los países de origen, reconociendo las serias preocupaciones de los países que deportan a ciertos extranjeros por los crímenes cometidos en esos países y las serias preocupaciones de los países receptores por el efecto negativo de estas deportaciones en los niveles de criminalidad en los países de origen, y expresan el deseo de trabajar juntos, cuando corresponda, para abordar los efectos negativos en nuestras sociedades;

(32) El documento está disponible en la página web: <http://www.cicad.oas.org/ES/Basicdocuments/Cumbre2_DeclaracionFinal.asp> (Consultado el 10 de noviembre de 2009).

“Promoverán, cuando sea apropiado y de conformidad con su ordenamiento jurídico, la adopción de las técnicas de investigación comprendidas en la Convención de la ONU Contra la Delincuencia Organizada Transnacional, que constituyen herramientas muy importantes en la lucha contra la delincuencia organizada”⁽³³⁾.

Más recientemente, los jefes de Estado se pronunciaron en este mismo sentido en el marco de la V Cumbre de las Américas realizada en Puerto de España en 2009, donde manifestaron lo siguiente:

“76. Redoblaremos nuestros esfuerzos para evitar el acceso de los fondos/activos de origen ilícito a nuestros sistemas financieros mediante medidas nacionales y la cooperación internacional para identificar, rastrear, embargar, incautar o decomisar los fondos/activos y bienes que sean producto de la actividad delictiva, determinando su destino y/o repatriación, de conformidad con nuestra legislación nacional y el derecho internacional”⁽³⁴⁾.

Como parte de esta política de lucha contra el lavado de activos, la Comisión ha realizado importantes esfuerzos para producir documentos que contribuyan a fortalecer la legislación nacional de los Estados miembros de la organización. En efecto, la Comisión cuenta desde 1999 con una sección dedicada exclusivamente a la capacitación, apoyo técnico y asistencia en materia de lavado de activos a los Estados miembros. Esta sección cuenta con un grupo de expertos de diferentes países, el cual sirve actualmente como foro hemisférico para discutir los problemas existentes en materia de lavado de activos y financiación del terrorismo. El documento más importante que ha producido hasta ahora este grupo de expertos es el “Reglamento Modelo sobre delitos de lavado de activos relacionados con el tráfico ilícito de drogas, y otros delitos graves” (versión actualizada 2005)⁽³⁵⁾,

(33) El documento está disponible en la página web: <http://www.cicad.oas.org/ES_Basicdocuments/Quebec.asp> (Consultado el 10 de noviembre de 2009).

(34) El documento está disponible en la página web: <http://www.cicad.oas.org/ES_BasicDocuments/Summit5PortofSpain.asp> (Consultado el día 10 de noviembre de 2009).

(35) Este documento está disponible en la página web: <http://www.cicad.oas.org/Lavado_Activos/ESP/Reglamento_modelo_esp12_02/REGLAMENTO%20>

el cual sirve actualmente como guía para aquellos Estados que estén en proceso de establecimiento o reforma de la legislación en materia de control de lavado de activos y financiación del terrorismo.

En lo fundamental, el Reglamento Modelo propuesto por la CICAD sigue la misma línea de los demás instrumentos internacionales sobre la materia, tales como las recomendaciones del GAFI, las recomendaciones del Comité de Basilea o las diferentes convenciones de la ONU. En consecuencia, este Reglamento también insiste en la necesidad de tipificar el lavado de activos como delito autónomo, de adoptar medidas eficientes y eficaces para la incautación, decomiso o embargo de los bienes de origen ilícito, y de establecer acuerdos o convenios adecuados para la cooperación judicial internacional, entre otros.

En lo que respecta a la adopción de medidas para la prevención del lavado de activos en los sectores financiero, cambiario, bursátil y asegurador, los artículos 14 a 23 del Reglamento Modelo propuesto por la Comisión contienen una regulación específica sobre el tema. El artículo 14 comienza definiendo qué se entiende por “instituciones financieras” para efectos de ese Reglamento, y allí dispone textualmente lo siguiente:

“1. A los efectos de este Reglamento son consideradas instituciones financieras, entre otras, las siguientes:

“a) Banco comercial, compañía fiduciaria, asociación de ahorro y crédito, asociación de construcción y crédito, banco de ahorro, banco industrial, cooperativa de crédito, u otra institución o establecimiento de ahorro autorizado por la legislación bancaria interna, sean de propiedad pública, privada o mixta;

“b) Cualquier entidad que preste servicios financieros internacionales (*offshore*);

“c) Casa de corretaje o de intermediación en la negociación de valores o de inversiones o ventas a futuro;

(*Cont. nota 35*)

LAVADO%20-%20ESP%20negjun%2006.pdf> (Consultado el día 10 de noviembre de 2009).

- “d) Casa de intermediación en la venta de divisas o casa de cambio;
- “2. Así mismo, se asimilarán a las instituciones financieras las personas que realicen, entre otras, las siguientes actividades:
 - “a) Operaciones sistemáticas o sustanciales de canje de cheques;
 - “b) Operaciones sistemáticas o sustanciales de emisión, venta o rescate de cheques de viajero o giro postal o la emisión de tarjetas de crédito o débito y otros instrumentos similares;
 - “c) Transferencias sistemáticas o sustanciales de fondos o valores, incluyendo aquellas a través de redes o sistemas informales, y cualquier otra transacción que tenga ese resultado, y
 - “d) Cualquier otra actividad sujeta a supervisión por las respectivas autoridades competentes”.

A continuación, el artículo 15 del Reglamento señala que estas entidades deben ser sometidas a la vigilancia de una agencia gubernamental, quien deberá autorizar su funcionamiento previo la verificación del cumplimiento de las disposiciones aplicables en materia de control del lavado de activos y la financiación del terrorismo. En lo que atañe a los requisitos mínimos exigibles a las entidades financieras para la prevención del lavado de activos, el artículo 16 del reglamento dispone como primera obligación la de adoptar mecanismos para la adecuada identificación y conocimiento del cliente. De acuerdo con el Reglamento, las entidades deben adoptar sistemas de cuentas nominativas y abstenerse de abrir cuentas cifradas o bajo nombres ficticios. Así mismo, las instituciones financieras deben recoger y verificar toda la información concerniente a su cliente, asegurándose de obtener soportes documentales que comprueben la misma. La información de los clientes debe además ser conservada adecuadamente y actualizada periódicamente, especialmente cuando se trate de personas jurídicas o de personas extranjeras.

Adicionalmente, las entidades deben conservar registros que contengan la información necesaria para reconstruir cualquier transacción que pueda llegar a ser de interés para la entidad o para las autoridades, de modo que las investigaciones por lavado de activos y financiación del terrorismo

puedan contar fácilmente con la indagación financiera necesaria. A este respecto, el artículo 17 del Reglamento Modelo señala que las instituciones financieras deben tener la obligación de responder de forma rápida y completa los requerimientos de información provenientes de las autoridades, y deben tener proscrito informar a cualquier persona sobre dichos requerimientos. De hecho, el artículo 23 llega mucho más allá y dispone que las operaciones de cambio que impliquen el tránsito de divisas a través de fronteras deberán ser previamente notificadas y autorizadas por las autoridades nacionales correspondientes, al punto que no notificar o suministrar información falsa en la notificación debe ser tipificado como delito autónomo por parte de los Estados miembros. La información suministrada por las instituciones financieras deberá ser administrada bajo reserva y con absoluta confidencialidad por parte de las autoridades, sin perjuicio de la posibilidad de compartirla con las autoridades de otros países en el marco de acuerdos de cooperación internacional sobre la materia.

Como parte importante de la información que deben recolectar y conservar las instituciones financieras, el artículo 18 del Reglamento establece la obligación de adoptar formularios estándar para obtener los datos correspondientes a las transacciones en efectivo que superen determinado monto, ya sea que se realicen en moneda nacional o cualquier otra divisa. Estos formularios deben permitir a la entidad obtener todos los datos necesarios para conocer y analizar adecuadamente la operación, y deben ser conservados como mínimo por cinco años. En caso de que una persona realice múltiples operaciones en efectivo, estas serán consideradas como una sola cuando en conjunto superen determinado monto y tengan un mismo ordenante o beneficiario, haciéndose obligatorio entonces el diligenciamiento de un formulario especialmente diseñado para el efecto. Los formularios de las operaciones en efectivo o los registros de esas operaciones deben estar a disposición de las autoridades nacionales, para que ellas puedan acceder fácilmente a esos datos en el marco de investigaciones relacionadas con actividades de lavado de activos o financiación del terrorismo.

Los registros de información relacionada con transacciones en efectivo o con cualquiera otro tipo de operaciones tiene el propósito de facilitar la búsqueda de la misma por parte de las autoridades. El artículo 18 del Reglamento Modelo dispone que las instituciones deben analizar la información relativa a sus operaciones, para detectar cualquier situación anó-

mala. Debido a esta disposición, los registros de datos cumplen también el propósito de facilitar la tarea de análisis de las operaciones, en orden a identificar aquellas que son sospechosas de ser constitutivas de lavado de activos o financiación del terrorismo. En este sentido, el objetivo de la obligación de obtener y conservar registros es que las instituciones puedan identificar de forma eficaz y oportuna las operaciones sospechosas, y reportarlas a las autoridades para su investigación. Y para estimular este tipo de reportes, el Reglamento prevé que las instituciones no podrán informar a su cliente cuando una operación suya haya sido reportada, y que no habrá lugar a responsabilidad alguna para la institución cuando el reporte haya sido de buena fe.

Para asegurar el adecuado cumplimiento de todas las normas anteriores, el artículo 21 del Reglamento dispone que las instituciones financieras deben “adoptar, desarrollar y ejecutar programas, normas, procedimientos y controles internos para prevenir y detectar el lavado de activos o el financiamiento del terrorismo”. Estos programas deben garantizar como mínimo, que el personal al servicio de la entidad tenga integridad personal y esté libre de antecedentes por este tipo de delitos. Igualmente, deben implementar eventos de capacitación periódica sobre esta materia, e incluir en sus reglamentos de trabajo la obligación de asistir, aprobar las evaluaciones de esos programas, y aplicar los conocimientos obtenidos en sus labores cotidianas. Finalmente, la norma también dispone que los programas implementados por las instituciones deben contemplar la realización periódica de auditorías por parte de personal independiente, para evaluar su calidad, identificar las fallas e implementar las mejoras necesarias.

Como complemento a estas medidas de control para las instituciones financieras, el artículo 20 del Reglamento invita a los Estados miembros de la Organización a adoptar penas más severas para aquellos directores, administradores y empleados de instituciones financieras que sean autores o partícipes de los delitos de lavado de activo o financiación del terrorismo. Así mismo, el Reglamento asegura el cumplimiento de las normas sobre control de lavado de activos para instituciones financieras, recomendando a los Estados miembros tipificar el incumplimiento de esas obligaciones como delito autónomo.

En consecuencia se establece, que las instituciones financieras también deben responder penalmente como personas jurídicas, no sólo por el

delito de lavado de activos cuando alguno de sus directivos, administradores o empleados sea hallado responsable, sino también por un delito autónomo consistente en el incumplimiento de las órdenes de incautación, embargo o comiso de bienes de origen ilícito, o de las obligaciones de adoptar y ejecutar las medidas de control de lavado de activos mencionadas anteriormente. Así las cosas, el incumplimiento de obligaciones como el conocimiento adecuado del cliente, el registro de operaciones en efectivo o el reporte de operaciones sospechosas deberá generar responsabilidad penal para la persona natural (director, administrador o empleado) y para la persona jurídica (institución financiera), independientemente de la responsabilidad que surja o no por el delito de lavado de activos.

Finalmente, el artículo 22 del Reglamento abre la posibilidad de que los Estados miembros de la Organización extiendan el ámbito de aplicación de estas recomendaciones, a otro tipo de sectores tales como:

- “a) La venta o traspaso de bienes raíces, armas, metales preciosos, objetos de arte, objetos arqueológicos, joyas, automóviles, barcos, aviones u otros bienes colecciónables; y la prestación de servicios relacionados con los viajes o el entretenimiento;
- “b) Los juegos de azar y operaciones relacionadas a las mismas;
- “c) La prestación de toda clase de servicios profesionales incluyendo los notariales y contables;
- “d) Seguros, reaseguros y su corretaje;
- “e) Inversiones y fondos de inversión;
- “f) Las relacionadas con la comercialización internacional de bienes, servicios y transferencia de tecnología y la movilización de capitales;
- “g) El financiamiento de organizaciones no lucrativas o no gubernamentales, y
- “h) Cualquier actividad comercial que debido a la naturaleza de sus operaciones pudiera ser utilizada para fines relacionados con el lavado de activos y el financiamiento del terrorismo”.

CAPÍTULO 3

Normatividad colombiana vigente

El régimen vigente en Colombia en materia de prevención del lavado de activos se encuentra contenido en el Título I Capítulo XI de la Circular Básica Jurídica 7 de 1996, cuya última modificación integral tuvo lugar mediante la expedición de la Circular Externa 22 del 19 de abril de 2007⁽¹⁾ emitida por la nueva Superintendencia Financiera⁽²⁾. A través de esta última circular externa, la Superintendencia sustituyó el Sistema Integral para la Prevención del Lavado de Activos “SIPLA” que anteriormente estaban obligadas a adoptar las entidades sometidas a la inspección, vigilancia y control de la extinta Superintendencia Bancaria, el cual estaba fundado en los criterios de supervisión de entidades financieras recomendados por el Comité de Basilea I, relacionados fundamentalmente con la verificación del cumplimiento de estándares y normas para minimizar los riesgos de mercado, de crédito y de liquidez en función del perfil del riesgo de la entidad y la relación rentabilidad-riesgo. Ahora las entidades vigiladas están obligadas a adoptar un nuevo Sistema de Administración de Riesgo de Lavado de Activos y de la Financiación del Terrorismo “SARLA/FT”⁽³⁾ estructurado bajo las recomendaciones del Comité de

-
- (1) Esta Circular Externa 022 de 2007 ha sido modificada en aspectos puntuales por las circulares externas 026 de 2008 y 008 y 009 de 2009.
 - (2) “La Superintendencia Financiera de Colombia surgió de la fusión de la Superintendencia Bancaria de Colombia con la Superintendencia de Valores, según lo establecido en el artículo 1º del Decreto 4327 de 2005. La entidad es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio” (cfr., <<http://www.superfinanciera.gov.co/>>, consultado el 8 de septiembre de 2009).
 - (3) En el Concepto 2002046102-1 del 12 de septiembre de 2002, la Superintendencia Bancaria (hoy Superintendencia Financiera) expuso lo siguiente: “Así pues, en

Basilea II (2004-2006), el cual se fundamenta en criterios de control y administración de los diferentes riesgos a los que se encuentran expuestas las

(Cont. nota 3)

relación con su inquietud y refiriéndose a las instituciones vigiladas por esta Superintendencia, los artículos 102 y 107 del Estatuto Orgánico del Sistema Financiero (D. 663 de 1993), establecen un régimen dirigido a la prevención de actividades delictivas en dichas entidades, señalándose fundamentalmente la obligatoriedad de adoptar medidas de control apropiadas y suficientes orientadas a evitar que en la realización de sus operaciones puedan ser utilizadas como instrumento para el ocultamiento, manejo, e inversión o aprovechamiento en cualquier forma de dinero u otros bienes provenientes de actividades delictivas, o para dar apariencia de legalidad a las mismas o a las transacciones y fondos vinculados con las mismas". En concordancia con lo anterior, en el numeral 6 del capítulo noveno del Título I de la Circular Básica Jurídica (Cir. Externa 007 de 1996) se contempla el denominado Sistema Integral para la Prevención del Lavado de Activos (SIPLA), el cual debe comprender medidas de control apropiadas y suficientes dirigidas a los propósitos antes indicados.

De tal forma, las entidades vigiladas deben adoptar mecanismos como el conocimiento del cliente y del mercado, control de operaciones, detección de operaciones inusuales y determinación de operaciones sospechosas, control de transacciones en efectivo, realizar capacitación sobre la materia y efectuar, entre otros, reportes de transacciones en efectivo y transacciones sospechosas.

Se establece además la necesidad de adoptar un Código de Conducta que debe contener los criterios que sean necesarios para resolver los "Conflictos de Interés" y anteponer la observancia de unos principios éticos al logro de metas comerciales, comprometiendo con ello a toda la entidad.

También se indica que los mecanismos de control adoptados por la entidad vigilada deben consagrarse en un manual de procedimientos específicos, aprobado por la junta directiva, que considere la naturaleza jurídica y las características propias de cada institución y de sus diferentes productos, constituyendo un listado de órdenes claras, como desarrollo de la política institucional de la entidad contra el lavado de activos.

Adicionalmente y de acuerdo con lo dispuesto en el numeral 3 del artículo 102 del Estatuto Orgánico del Sistema Financiero las entidades vigiladas tienen la obligación de designar oficial de cumplimiento, cuya función principal es verificar la adecuada observancia de los procedimientos específicos diseñados por la institución con el fin de prevenir el lavado de activos.

Las sanciones administrativas por la inobservancia de las citadas normas corresponden a las previstas en los artículos 209 y 211 del citado Estatuto Orgánico del Sistema Financiero, tanto personal como institucionalmente. Es oportuno destacar que dichas disposiciones fueron adicionadas por los artículos 21 y 22 de la Ley 365 de 1997 respectivamente, estableciéndose la posibilidad de imponer sanciones más severas cuando las infracciones cometidas se refieren al régimen para la prevención de actividades delictivas. (En este mismo sentido puede consultarse el Concepto 2000069551-1 del 20 de dic. de 2000).

entidades financieras, y entre los cuales se halla el de lavado de activos y financiación del terrorismo⁽⁴⁾.

En la actualidad el SARLA/FT debe ser obligatoriamente adoptado por todas las entidades sometidas a la inspección, vigilancia y control de la nueva Superintendencia Financiera, lo cual significa que aplica para todos los intermediarios del mercado financiero, asegurador, cambiario y de valores.

El punto de partida para entender el SARLA/FT es el artículo 102 del Estatuto Orgánico del Sistema Financiero (D. 663 del 2 de abril de 1993,

-
- (4) Al respecto, la presidenta de la Asociación Bancaria de Colombia, María Mercedes Cuellar, en el discurso de clausura del *VII Congreso Panamericano de Control y Prevención del Lavado de Activos y Financiación del Terrorismo* pronunciado el 27 de julio de 2007, sostuvo: “Siguiendo la óptica de supervisión del Acuerdo de Basilea II, la principal característica de la nueva norma es que agrupa las prácticas de control y prevención que los bancos venían adelantando de tiempo atrás, en un modelo de riesgos que amplía la perspectiva de gestión”. Recordemos que Basilea II, además de vincular de manera más precisa los requerimientos de capital al nivel de riesgo de las entidades financieras, establece pautas para la administración de los mismos y reconoce que las nuevas realidades del sistema financiero imponen a los reguladores y supervisores centrarse en los procesos de administración de riesgos más que en sus estados financieros o en el cumplimiento de las normas establecidas. A este respecto es importante destacar un aspecto en particular: que el riesgo de lavado de activos y financiación del terrorismo presenta características y especificidades propias, que lo diferencian de manera sustancial de los riesgos financieros propiamente dichos. Por ello, la experiencia previa de las instituciones financieras en la implementación de otros sistemas de administración de riesgos, si bien es valiosa y constituye un marco de referencia, no es necesariamente apropiada o adaptable a la implementación del SARLA/FT. Esto, por supuesto, agrega dificultades por la inexistencia de parámetros o guías en la orientación de su aplicación. En efecto, como lo indica la misma Circular 022 relativa al SARLA/FT, mientras que los mecanismos para la administración del riesgo de lavado de activos y de financiamiento del terrorismo se dirigen a prevenirlo, detectarlo y reportarlo en forma oportuna y eficaz, los mecanismos para la administración de los riesgos de mercado, de crédito, de liquidez y operativos se dirigen a asumirlos íntegra o parcialmente en función del perfil de riesgo de la entidad y de la relación entre rentabilidad y riesgo. Esto implica que las instituciones financieras tienen que ser especialmente cuidadosas en la forma en que evalúan sus riesgos, porque aun cuando un evento de lavado de activos no necesariamente afecta los resultados de una entidad de manera significativa, existe un enorme riesgo reputacional que podría tener consecuencias mayores.

modificado por la L. 1121 de 2006⁽⁵⁾). Este artículo dispone como obligación de todas las instituciones sometidas a la inspección, vigilancia y control de la Superintendencia Financiera adoptar medidas de control, que contribuyan a prevenir que puedan ser utilizadas para movilizar, adquirir, administrar, depositar, aprovechar, invertir, manejar, ocultar o encubrir el origen de recursos ilegalmente obtenidos, o destinados a financiar organizaciones terroristas⁽⁶⁾. Así mismo, este artículo también señala que las

-
- (5) Diario Oficial N° 46.497 del 30 de diciembre de 2006.
 - (6) En el Concepto 2000069551-1 del 20 de diciembre de 2000, la Superintendencia Bancaria (hoy Superintendencia Financiera) explicó que los profesionales dedicados a la compra y venta de divisas que no sean intermediarios cambiarios –también conocidos como cambistas profesionales–, están obligados a adoptar un sistema para la prevención del lavado de activos y la financiación del terrorismo aun cuando ellos no están sometidos a la inspección, vigilancia y control de esa Superintendencia. Textualmente sostuvo la Superintendencia lo siguiente: “Se advierte por lo tanto que de conformidad con el nuevo Estatuto Cambiario contenido en la Resolución Externa 8 de 2000, las actividades que constituyan el objeto exclusivo de las casas de cambio autorizadas para funcionar en las categorías cambista y especial bajo la vigencia de la derogada Resolución Externa 21 de 1993 de la Junta Directiva del Banco de la República, es decir, la compra y venta de divisas, en adelante pueden ser desarrolladas profesionalmente por los residentes en el país previa inscripción en el registro mercantil, sin que se requiera autorización previa por parte de esta Superintendencia”.

En concordancia con lo anterior, el nuevo conjunto de disposiciones sobre casas de cambio establecido mediante la mencionada Resolución Externa 8 de 2000 no contempla las categorías cambista y especial de casas de cambio, razón por la cual las sociedades y establecimientos de comercio autorizados que pertenecían a dichas categorías no están sometidos al control y vigilancia de esta Superintendencia desde el pasado 11 de mayo de 2000, fecha en la cual entró a regir la citada normativa.

Debe indicarse además que la denominación casa de cambio está reservada desde la entrada en vigencia de la Resolución Externa 8 a las entidades definidas como tales en el artículo 62 de la misma.

En ese sentido destacamos que actualmente compete únicamente a esta Superintendencia ejercer el control de las casas de cambio, entidades a las que alude el artículo 62 de la Resolución Externa 8 de 2000 y que corresponden a las autorizadas en vigencia de la Resolución Externa 21 de 1993 en la categoría propiamente dicha o plena, o a las que sean autorizadas posteriormente como tales en los términos del nuevo Estatuto Cambiario.

Efectuadas las anteriores aclaraciones, que son imperativamente necesarias para comprender el régimen vigente sobre el ejercicio profesional de la actividad de compra y venta de divisas, reiteramos, en punto a su inquietud, que resulta viable para los residentes en el país desarrollar la actividad profesional de compra y

medidas adoptadas deben consistir en mecanismos y reglas de conducta de obligatoria observancia por parte de todos sus directivos, administradores y funcionarios. Estos mecanismos y reglas de conducta deben además estar diseñados de tal forma, que existan procedimientos específicos que permitan a la entidad conocer adecuadamente a los clientes, conocer

(Cont. nota 6)

venta de divisas de acuerdo con lo previsto en el artículo 75 de la Resolución Externa 8, sin que se requiera, insistimos, autorización de esta Superintendencia (...).

Ahora, el desarrollo profesional de la compra y venta de divisas en los términos señalados resulta viable a la luz del régimen cambiario. Asunto diferente es que en desarrollo de dicha actividad se pueda incurrir en el tipo penal de lavado de activos previsto en el artículo 247A del Código Penal, responsabilidad que, se recuerda, no compete establecer a esta Superintendencia.

Sobre este aspecto, reiterando que no es función de la Superintendencia Bancaria ejercer el control y vigilancia de aquellos residentes que desarrollen profesionalmente la compra y venta de divisas conforme al citado artículo 75 de la Resolución 8, destaquemos la obligación a cargo de éstos y prevista en dicha normativa de “suministrar la información y la colaboración que requieran las autoridades competentes, en especial la Fiscalía General de la Nación o la Unidad de Información y Análisis Financiero, para efectos de la prevención de actividades delictivas y de lavado de activos”.

Se tiene entonces que quienes desarrollen dicha actividad en los términos citados deben adoptar medidas dirigidas a cumplir dicho precepto y, naturalmente, a evitar que en desarrollo de tal gestión profesional puedan incurrir en conductas punibles.

La norma actualmente vigente en materia de prevención de lavado de activos aplicable a los depósitos públicos y privados, a las sociedades de intermediación aduanera, a las sociedades portuarias, a los usuarios operadores, industriales y comerciales de zonas francas, a las empresas transportadoras, a los agentes de carga internacional, a los intermediarios de tráfico postal y envíos urgentes, a las empresas de mensajería, a los usuarios aduaneros permanentes, a los usuarios altamente exportadores, a los demás auxiliares de la función aduanera y a los profesionales del cambio de divisas es la Circular Externa 0170 del 10 de octubre del año 2002 emitida por la Unidad Administrativa Especial Dirección de impuestos y Aduanas Nacionales, DIAN. Así mismo, las normas que definen las características, términos, condiciones y plazos en los que los profesionales de cambio deben reportar las operaciones sospechosas, son la Resolución 062 del 12 de junio de 2007 y la Resolución 111 del 21 de agosto de 2007, emitidas por la UIAF. En cuanto a los demás sujetos que realizan actividades de comercio exterior, la Resolución 285 de 2007 impone a los depósitos públicos y privados; sociedades de intermediación aduanera; sociedades portuarias; usuarios de zona franca; empresas transportadoras; agentes de carga internacional; usuarios aduaneros permanentes y usuarios altamente exportadores, la obligación de reportar de manera directa a la Unidad de Información y Análisis Financiero.

suficientemente el mercado en el que actúa y reportar oportunamente las operaciones sospechosas.

Paralelamente, el artículo 103 del EOSF impone a estas mismas entidades la obligación de adoptar mecanismos para llevar a cabo un control eficaz sobre las transacciones en efectivo⁽⁷⁾. A tal efecto, la entidad debe diseñar un formulario tipo que le permita recolectar la información necesaria y suficiente, para evaluar la razonabilidad de las transacciones en efectivo realizadas por sus clientes e identificar oportunamente las operaciones sospechosas. De acuerdo con el artículo 104 *ibidem*, las entidades están obligadas a reportar periódicamente a la unidad de información y análisis financiero (UIAF) las operaciones en efectivo realizadas, siguiendo las instrucciones que para el efecto imparta la Superintendencia Financiera. El reporte de esas operaciones y demás información suministrada a las autoridades se encuentra sometido a reserva⁽⁸⁾, de tal manera que por disposición del artículo 105 del EOSF⁽⁹⁾, ni la entidad ni sus fun-

-
- (7) En el Concepto 2008061356-001 del 8 de enero de 2009, la Superintendencia explicó que: “Así mismo, es del caso resaltar que de conformidad con lo dispuesto en el numeral 1 del artículo 103 del EOSF, toda institución financiera debe dejar constancia de la información relacionada con las transacciones en efectivo que realice su clientela cuyo valor sea igual o superior a diez millones de pesos (\$ 10.000.000) si es en moneda legal o a cinco mil dólares de los Estados Unidos de Norteamérica (US \$5.000) o su equivalente en otras monedas, según la tasa representativa del mercado del día en que se realice la operación, tal como lo señala el numeral 2.8, Capítulo XIII, Título I de la Circular Básica Jurídica (Cir. 007 de 1996) proferida por esta Superintendencia. En consecuencia, las instituciones vigiladas (entre ellas los bancos) están obligados a llevar un registro acerca de las transacciones en efectivo que se realicen (v.gr consignaciones en cuentas de depósito), cuyo valor sea igual o superior al señalado, así como también cuando se trate de operaciones inusuales o sospechosas.
- (8) En relación con la naturaleza, fundamento y alcance de la reserva a la que está sometida la información reportada a la UIAF, puede consultarse el concepto emitido por esa agencia gubernamental el 21 de junio de 2007, el cual está disponible en página web <http://www.uiaf.gov.co/index.php?idcategoria=1340&uiaf_2008=f88de3cb178328aa37926f25a09340fa#>> (consultada el 16 de septiembre de 2009). Así mismo, mediante la Carta Circular N° 001 del 12 de marzo de 2009, la UIAF insistió que la información reportada a esa entidad está sometida a una reserva obligatoria.
- (9) En Sentencia C-851 del 17 de agosto de 2005, M.P. Manuel José Cepeda Espinosa, la Honorable Corte Constitucional se pronunció sobre la exequibilidad del artículo 11 de la Ley 526 de 1999, el cual modificó el artículo 105 del EOSF.

cionarios pueden notificar al cliente cuando una de sus operaciones sea reportada a la UIAF⁽¹⁰⁾.

(Cont. nota 9)

En esa oportunidad, “la Corte ratificó que en un Estado democrático la regla general es la publicidad de la información de que disponen las autoridades estatales y la excepción su reserva, por motivos legítimos, en los casos expresamente previstos en la ley. En este sentido, sostuvo que para el logro de los fines legítimos de orden constitucional (arts. 1º y 2º C.P.), el legislador puede imponer, sin contradecir el ordenamiento constitucional, a las entidades vigiladas por la Superintendencia Bancaria y de Valores, el deber de reportar a la unidad de información y análisis financiero, información sobre operaciones sospechosas de la comisión de un delito de lavado de activos, sin que haya lugar a deducir responsabilidad a esas entidades, sus directivos o empleados, puesto que se trata de conductas acordes con el ordenamiento constitucional. De igual forma, la Corte estimó que la obligación de guardar la reserva de esa información no contradice los artículos 15 y 29 de la Constitución, en la medida en que se refiere al acopio de información sobre manejo de fondos que permita detectar operaciones sospechosas, sin que implique por sí misma el adelantamiento de una investigación penal, evento en el cual debe garantizarse la presunción de inocencia y el derecho de defensa de la persona involucrada en dichas operaciones. Además, señaló que la guarda de esa reserva corresponde a unos fines legítimos y al cumplimiento de compromisos internacionales asumidos por el estado colombiano en la prevención del delito de lavado de activos”.

- (10) En Concepto 2009017224-003 del 22 de abril de 2009, la Superintendencia hace una explicación del marco constitucional y legal de la reserva que protege la información suministrada por el cliente, así como aquella que es producto del trabajo de análisis llevado a cabo por la entidad. En ese mismo concepto, la Superintendencia explicó que: “Sea lo primero señalar, que de las normas antes citadas se desprende que únicamente el cliente es quien puede autorizar que la información personal que le ha suministrado a la entidad en virtud del formulario de vinculación, así como la derivada de su relación contractual, esto es, la información relativa a sus transacciones y movimientos (consignaciones, pagos, retiros, extractos, etc.) y a su comportamiento comercial, sea divulgada a quien él designe. Por tratarse de un derecho fundamental protegido por la Constitución, la autorización del cliente para que se divulgue a un determinado tercero la información de la cual puede disponer, debe ser clara y expresa; para poder probar que ello fue así, debe constar por escrito”.

En relación con el resto de la información, es decir, aquella que ha sido “trabajada” “desarrollada” “analizada” “comparada” o “manipulada” por la entidad, como es la obtenida en desarrollo de los mecanismos previstos en los artículos 102 a 104 del EOSF, la misma está sujeta a reserva de acuerdo con lo consagrado en el citado artículo 105. El cliente no tiene facultad para levantar tal reserva, pues este tipo de información no le pertenece, y la entidad tiene prohibición legal de divulgarla, salvo a quienes la ley expresamente ha señalado como usuarios de tal información.

(Cont. nota 10)

Por su puesto, el incumplimiento de alguna de las obligaciones previstas en los artículos 102, 103, 104 y 105 del EOSF tiene como consecuencia la imposición de sanciones administrativas, sin perjuicio de la responsabilidad penal que pueda tener lugar (art. 107 *ibidem*). Para evaluar la sanción administrativa procedente en caso de incumplimiento, la Superintendencia Financiera tiene en cuenta que la realización de operaciones sin observar los mecanismos para la administración del riesgo de lavado de activos y financiación del terrorismo constituye una práctica insegura y no autorizada de la intermediación financiera, aseguradora, cambiaria o de valores. Por esta razón, y conforme lo establecido en el literal a) del numeral 5 del artículo 326 EOSF, la Superintendencia Financiera tiene la facultad de impartir órdenes para que suspendan de inmediato las prácticas ilegales e inseguras, y para que se adopten de inmediato las medidas correctivas procedentes. En caso de incumplimiento de las instrucciones impartidas para enervar las prácticas inseguras frente al riesgo de lavado de activos y financiación del terrorismo, la Superintendencia está facultada para imponer sanciones (por ejemplo multas) a la entidad, a sus directivos, a sus administradores, a su revisor fiscal o a sus funcionarios. En los casos más graves, cuando se presente un reiterado e injustificado incumplimiento de las obligaciones por parte de la entidad, la Superintendencia podría llegar

Es decir que el nivel de acceso a la información de los clientes y de la que ha sido obtenida en desarrollo de los artículos 102 a 104 del EOSF y la contemplada en el artículo 105 del citado estatuto, es totalmente restringido. Sólo tendrán acceso a ella: (1) Los administradores y funcionarios de la entidad vigilada que de acuerdo con el Capítulo 11 citado y el SARLA/FT adoptado, les hayan sido asignadas funciones sobre tal información, y sólo en lo relacionado con el cumplimiento de tales funciones; (2) La UIAF; (3) La Fiscalía General de la Nación; (4) La Superintendencia Financiera de Colombia; (5) Quienes de acuerdo con la ley deban “Colaborar con las entidades gubernamentales que ejerzan la inspección y vigilancia de las compañías...” (Revisores fiscales).

En cuanto al nivel de confidencialidad o reserva sobre la misma es total. Las entidades y sus funcionarios sólo podrán suministrar este tipo de información a las personas que de acuerdo con lo señalado en el párrafo precedente tengan acceso a la misma.

En relación con este mismo tema, en el Concepto 2006017379-002 del 9 de agosto de 2006, la Superintendencia aclaró que: “El silencio del cliente frente a la solicitud del Banco para que autorice la divulgación de su información, no puede considerarse en ningún caso como una autorización; la misma debe ser expresa, constar por escrito y recaer sobre información de la cual legalmente el cliente puede disponer”.

a decretar la toma de posesión de sus bienes, haberes y negocios, conforme al literal f) del artículo 114 del EOSF⁽¹¹⁾.

Las obligaciones previstas en los artículos 102 a 105 del EOSF se encuentran actualmente desarrolladas en el Título I Capítulo XI de la Circular Básica Jurídica 7 de 1996, modificado por la Circular Externa 022 de 2007. En esta circular básica jurídica se encuentran definidas las características mínimas, que debe tener el SARLA/FT y que están obligadas a adoptar las entidades vigiladas por la Superintendencia Financiera.

Visto de una manera esquemática, el SARLA/FT definido en la circular básica jurídica está integrado por unas etapas y por unos elementos. Las etapas pueden definirse como el conjunto de actividades que debe llevar a cabo la entidad, para administrar adecuadamente el riesgo de lavado

(11) En Concepto 2008003821-001 del 28 de enero de 2008, la Superintendencia Financiera sostuvo que: “En punto a las normas sobre prevención y control del lavado de activos, a la fecha se encuentran vigentes los artículos 102 y siguientes del Estatuto Orgánico del Sistema Financiero y el capítulo XI, Título 1 de la Circular Básica Jurídica 007 de 1996 de esta Entidad. El incumplimiento a las mencionadas normas, previo agotamiento del procedimiento descrito en el numeral 4 del artículo 208 del EOSF, podría conllevar la imposición de las sanciones a que hubiera lugar, a las entidades y/o personas naturales sujetas a inspección y vigilancia de este Organismo de Control”. En relación con el tipo de sanciones que podrían imponerse, el artículo 9º del Decreto 4327 de 2005 dispone que la Superintendencia podrá imponer las siguientes sanciones de carácter administrativo: “a) Amonestación o llamado de atención; b) Multa pecuniaria a favor del tesoro nacional. Cuando se trate de las sanciones previstas en el artículo 209 de este estatuto, la multa podrá ser hasta de ciento diez millones de pesos (\$ 110.000.000) del año 2002. Cuando se trate de las sanciones previstas en el artículo 211 de este estatuto y no exista norma especial que establezca la respectiva sanción, la multa podrá ser hasta de quinientos cincuenta millones de pesos (\$ 550.000.000) del año 2002; c) Suspensión o inhabilitación hasta por cinco (5) años para el ejercicio de aquellos cargos en entidades vigiladas por la Superintendencia Bancaria que requieran para su desempeño la posesión ante dicho organismo; d) Remoción de los administradores, directores, representantes legales o de los revisores fiscales de las personas vigiladas por la Superintendencia Bancaria. Esta sanción se aplica sin perjuicio de las que establezcan normas especiales, y e) Clausura de las oficinas de representación de instituciones financieras y de reaseguros del exterior. Las sumas indicadas en este numeral se ajustarán anualmente, en el mismo sentido y porcentaje en que varíe el índice de precios al consumidor suministrado por el DANE. Las multas pecuniarias previstas en este artículo podrán ser sucesivas mientras subsista el incumplimiento que las originó”.

de activos y financiación del terrorismo al que están expuestas. Los elementos son el conjunto de instrumentos o mecanismos con que cuenta la entidad, para llevar a cabo las actividades que requiere la administración de ese riesgo.

Para otras entidades distintas a las vigiladas por la Superintendencia Financiera, la ley colombiana establece también una regulación específica que las obliga a tener instrumentos mínimos de prevención, dentro del marco de un sistema integral (SIPLA/FT) cuyo alcance específico será materia de examen en el capítulo siguiente, lo que permite concluir que en Colombia subsisten dos regímenes de prevención: el SARLA/FT para las entidades vigiladas por la Superintendencia Financiera; y el SIPLA/FT para otras empresas particularmente dedicadas a operaciones de comercio exterior, actividad cooperativa, casinos y juegos de azar, comercio exterior y venta de divisas, entre otras.

1. ETAPAS DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO (SARLA/FT)

De acuerdo con la reglamentación prevista en la Circular Externa 022 de 2007, en Colombia el SARLA/FT está integrado por cuatro fases claramente diferenciables: (i) identificación del riesgo, (ii) medición del riesgo, (iii) control del riesgo, y (iv) monitoreo del riesgo.

La Superintendencia Financiera entiende que los intermediarios financieros, aseguradores, cambiarios o de valores están seriamente expuestos al riesgo de ser utilizados para canalizar, aprovechar, invertir, ocultar o encubrir el origen de recursos ilícitos, o para financiar grupos al margen de la ley, dado el importante papel que cumplen en el círculo económico⁽¹²⁾. Así mismo, la entidad asume que la materialización del riesgo depende de diversos factores tales como las características de los clientes o usuarios de

(12) Cfr., Concepto 2008009451-001 del 2 de abril de 2008, en el cual la Superintendencia Financiera “anuncia y describe de manera general algunos de los riesgos que se han identificado como propios de la actividad financiera”.

la entidad, las propiedades de los productos ofrecidos, la naturaleza de los canales utilizados para comercializar y/o distribuirlos, y las particularidades del sistema jurídico aplicable. Por esta razón no es sencillo establecer exactamente cuáles son las consecuencias desfavorables que podría eventualmente afrontar, una entidad que sea utilizada para llevar a cabo operaciones de lavado de activos o de financiación del terrorismo.

Teniendo en cuenta lo anterior, al hablar de “riesgo” en el marco de la legislación vigente en materia de prevención del lavado de activos y financiación del terrorismo, la Superintendencia Financiera intenta aglutinar los diferentes tipos de consecuencias desfavorables que podría sufrir la entidad en cuatro categorías diferentes a saber: (a) el *riesgo reputacional*, definido como la posibilidad de que el nombre y la imagen corporativa de la entidad se vea menoscabada; (b) el *riesgo legal*, entendido como la posibilidad de que la entidad sea sancionada o condenada al pago de indemnizaciones; (c) el *riesgo operativo*, comprendido como la posibilidad de sufrir pérdidas económicas a causa de fallas humanas, técnicas o procedimentales⁽¹³⁾, y (d) el *riesgo de contagio*, entendido como la posibilidad de que

(13) Al respecto cfr. KPMG Colombia, Basilea II: “Una mirada más cercana. Administración del riesgo operacional”, *Boletín Financiero*, ed. abril de 2004, p. 2. En este documento se explica: “El riesgo operacional es definido por el Comité de Basilea como ‘el riesgo de pérdida resultante de inadecuados o fallidos procesos internos, de la gente, y de sistemas, o de acontecimientos externos’ incluyendo el riesgo legal pero excluyendo los riesgos estratégico y reputacional. Los ejemplos de riesgos operacionales se enumeran abajo:

Área de negocios	Riesgos potenciales
Procesos	<ul style="list-style-type: none"> – Incumplimiento de los mandatos – Incorrecta/inoportuna captura, ejecución, y registro de la transacción – Pérdida de activos del cliente – Equivocación en la tasación de los productos – Asignación incorrecta del activo – Asuntos de cumplimiento – Errores de acciones corporativos – Errores en las reservas de préstamos – Errores de la contabilidad y en los impuestos – Inadecuada contabilización de registros contables – Errores en abonos y liquidaciones

(Cont. nota 13)

la entidad pueda sufrir una afectación reputacional, legal o económica a causa de la acción propia de una persona relacionada o asociada a ella⁽¹⁴⁾.

La posibilidad de que la entidad sufra alguna de las consecuencias desfavorables definidas como *riesgo reputacional, legal, operativo o de contagio* es lo que la circular básica jurídica define como “riesgo de lavado de activos y de la financiación del terrorismo”. Este riesgo es inherente a las entidades vigiladas, ya que su importante papel en el circuito económico legal las hace propensas a ser utilizadas para canalizar, aprovechar, invertir, ocultar o encubrir el origen de recursos ilícitos, o para financiar grupos al margen de la ley. El propósito de la ley es obligar a las entidades a adoptar un SARLA/FT que reduzca el riesgo al que se encuentran inherentemente expuestas, de manera que el nivel resultante des-

Área de negocios	Riesgos potenciales
Gente	<ul style="list-style-type: none"> – Negocios no autorizados – Abuso de información privilegiada – Fraude – Enfermedades y lesiones de los empleados – Demandas por discriminación – Asuntos de remuneración, beneficios, y terminación de contrato – Problemas de reclutamiento o retención del personal – Actividades laborales organizadas – Otros asuntos legales
Sistemas	<ul style="list-style-type: none"> – Fallas en el hardware y/o software – Indisponibilidad e integridad dudosa de los datos – Acceso no autorizado a la seguridad de la información y de los sistemas – Fallas en las telecomunicaciones – Interrupción de los sistemas – Piratería o virus en la computadora
Eventos externos	<ul style="list-style-type: none"> – Fallas operacionales en los proveedores o en las operaciones de <i>outsourcing</i> – Incendios o desastres naturales – Terrorismo – Vandalismo, hurto, robo

(14) Las definiciones de riesgo previstas en la regulación colombiana son coincidentes con las definiciones adoptadas por el Comité de Supervisión Bancaria. Al respecto ver BCBS, *Debida diligencia con la clientela de los bancos*, p. 10.

pués de aplicar el sistema (riesgo residual) sea lo más cercano a cero (0) posible.

Para reducir el riesgo residual de lavado de activos y de financiación del terrorismo, las entidades vigiladas deben adoptar un sistema que les permita un mínimo de seguridad frente a aquellas operaciones, por medio de las cuales se pretende utilizarla para lavar activos o para financiar el terrorismo. Esto significa que el sistema ha de asegurar que la entidad pueda detectar oportunamente aquellas operaciones de lavado de activos o financiación del terrorismo que se pretendan realizar o que se hayan realizado, y ofrecer pautas de conducta que permitan a los funcionarios una adecuada gestión de esas operaciones y de los riesgos asociados a ellas.

1.1. Identificación del riesgo

La primera condición para una adecuada gestión del riesgo asociado al lavado de activos y a la financiación del terrorismo es su identificación. De acuerdo con lo previsto en la circular básica jurídica, esta identificación debe hacerse antes del lanzamiento de cualquier producto, de la modificación de las características de productos existentes, de la incursión en nuevos mercados, de la apertura de nuevas operaciones en otras jurisdicciones, o del lanzamiento o modificación de nuevos canales de distribución. Para identificar el riesgo la entidad debe segmentar los diferentes factores que lo determinan, y evaluar de qué forma cada uno de ellos puede crear o aumentar el peligro de que la entidad sea utilizada para lavar activos o financiar el terrorismo. Así, la entidad debe estudiar de qué manera las características de los potenciales clientes o usuarios, las propiedades de los nuevos productos, la naturaleza de los nuevos canales de comercialización y/o distribución, o las particularidades del sistema jurídico aplicable en el mercado al que se incursiona, pueden representar un mayor riesgo de lavado de activos o de financiación del terrorismo. A guisa de ejemplo, el ofrecimiento de un nuevo producto financiero debe estar precedido de un estudio acerca de la manera en que los potenciales clientes, los canales de distribución y las características de este nuevo producto podrían incrementar el riesgo de lavado de activos y financiación del terrorismo, al que ya de por sí se encuentra expuesta la entidad.

La identificación del riesgo es una tarea que supone previamente la definición de las metodologías que deben aplicarse, no sólo para segmentar los factores que lo determinan, sino también para determinar los alcances de estos en su incremento o disminución. Es decir, cada entidad debe definir unas metodologías para diferenciar los factores que pueden crearlo o incrementarlo el riesgo, con ocasión del nuevo producto, de la modificación de las características de productos existentes, de la incursión en nuevos mercados, de la apertura de nuevas operaciones en otros mercados, o del lanzamiento o modificación de nuevos canales de distribución. Así mismo, cada entidad debe definir unas metodologías para evaluar los diferentes factores, y determinar cuál es su incidencia en el lavado de activos y financiación del terrorismo al que se expone la entidad, con ocasión del nuevo producto, de la modificación de las características de productos existentes, de la incursión en nuevos mercados, de la apertura de nuevas operaciones en otros mercados, o del lanzamiento o modificación de nuevos canales de distribución. Estas metodologías deben ser definidas por cada entidad, y las mismas deben ser descritas y explicadas en un manual de procedimientos que pueda ser conocido y comprendido, por los funcionarios de la entidad encargados de la identificación del problema.

De acuerdo con la circular básica jurídica, “como resultado de esta etapa las entidades vigiladas deben estar en capacidad de identificar los factores de riesgo y los asociados a los cuales se ven expuestas en relación al riesgo de LA/FT [lavado de activos o financiación del terrorismo]”⁽¹⁵⁾.

1.2. Medición del riesgo

Una vez identificado el riesgo, la entidad debe llevar a cabo una medición cuantitativa o cualitativa de la probabilidad de su realización frente a cada uno de los factores que lo determinan. Así mismo realizar una medición, para determinar cuál sería el impacto que tendría para ella la realización efectiva del mismo. Según lo anterior, se debe definir la metodología que se aplicará para establecer el valor de la probabilidad de realización

(15) Artículo 4.1.1 del Título I Capítulo XI de la Circular Básica Jurídica 7 de 1996, modificado por la Circular Externa 022 de 2007.

del riesgo, y para determinar el valor del impacto que dicha realización tendría para ella. Dichas metodologías deben estar definidas y explicadas en el manual de procedimientos, para que pueda ser conocido y comprendido por los funcionarios encargados de la medición.

Por supuesto, no siempre es sencillo asignar valores a una probabilidad. Menos cuando se trata de la ocurrencia de un evento futuro que depende de las voluntades individuales de muchos sujetos independientes. Sin embargo, la ley exige que las entidades lleven a cabo la medición de la probabilidad de realización del riesgo, y del impacto que ello tendría en la entidad, aunque sea de forma cualitativa. Esto significa que la metodología para la medición podría orientarse a clasificar la probabilidad de realización del riesgo en diferentes categorías (alta, media y baja), y no necesariamente asignando un valor numérico porcentual o probabilístico. Así mismo, la medición del impacto que tendría la realización efectiva del riesgo en la entidad podría ser valorada cualitativamente, mediante la clasificación en diferentes categorías según su intensidad (grave, normal y leve), sin que sea indispensable indicar un valor numérico o una cantidad de dinero para fijarlo. Lo importante es que la entidad pueda determinar con base en una medición racional, cuál es su perfil frente al riesgo de lavado de activos y financiación del terrorismo a la que se encuentra expuesta.

La identificación y la medición del riesgo requieren de metodologías que tengan en cuenta las diferentes tipologías de lavado de activos y financiación del terrorismo, así como una aproximación a la frecuencia con que se presenta cada una de estas. Por ejemplo, saber que el “pitufeo” es una de las tipologías más comunes de lavado de activos es importante, porque permite establecer que las operaciones de envío o recepción de giros internacionales expone a las entidades que incursionan en ese tipo de productos, a un incremento significativo del riesgo de lavado de activos y financiación del terrorismo. Por esta razón, dependiendo del perfil de los potenciales clientes a quienes se vaya a prestar ese servicio de envío o recepción de giros internacionales, dependiendo de los canales que se vaya a utilizar para comercializar ese producto, y dependiendo de la fortaleza de la legislación sobre lavado de activos aplicable en el país desde o hacia el cual se recibirán o enviarán los giros, la entidad puede determinar en qué medida se incrementa para ella el riesgo al que se encuentra expuesta.

De acuerdo con lo anterior, para la definición de las metodologías se requiere que se preste especial atención a los diferentes estudios teóricos y empíricos realizados respecto del lavado de activos y la financiación del terrorismo, así como a las estadísticas sobre estas formas de criminalidad. Por este motivo, la colaboración entre los organismos estatales y las entidades vigiladas en materia de intercambio de información es fundamental. Es importante entender que para que la política de prevención del lavado de activos y la financiación del terrorismo sea exitosa, no sólo las entidades deben suministrar información sobre sus clientes y sus operaciones a las autoridades, sino que estas también deben compartir información con las entidades acerca de las nuevas tipologías y la frecuencia con que ellas se presentan. De allí la importancia del papel que debe cumplir la UIAF como fuente de información y apoyo a las entidades vigiladas, en cuanto tienen que ver con estos delitos.

1.3. Control del riesgo

Una vez identificado y medido el riesgo, la empresa debe adoptar mecanismos concretos para controlarlo. Esto significa que la entidad debe definir las medidas y los procedimientos, los recursos que utilizará para esa labor, y las competencias que cada funcionario de la entidad tendrá respecto de ellas.

En primer lugar, la entidad debe adoptar mecanismos para obtener un adecuado conocimiento tanto de sus *clientes*⁽¹⁶⁾ como de los mercados en

(16) En Concepto 2008024244-001 del 5 de junio de 2008 (reiterado en el Cpto. número 2008072629-001 del 15 de dic. de 2008), la Superintendencia Financiera explicó que: “Para que se predique de una persona el concepto de ‘cliente’, es claro que la definición dada al mismo en el numeral 1.3 del Capítulo Undécimo del Título I de la Circular Externa 007 de 1996 involucra los siguientes elementos:

1. Que se trate de una persona natural o jurídica.
2. Que con esa persona la entidad vigilada no solo establezca, sino que mantenga una relación.
3. Que tal relación tenga origen legal o contractual.
4. Que la citada relación tenga por objeto el suministro de un producto.
5. Que la prestación de ese producto tenga relación con la actividad de la entidad vigilada, es decir, con el desarrollo de su objeto social”.

que actúa. En las etapas de identificación y medición del riesgo, la entidad debe tomar en consideración el perfil de los potenciales clientes a quienes se ofrecerán los productos y servicios de la entidad, y de los potenciales mercados en que incursionará. En esta etapa de control del riesgo, la entidad ya no sólo debe tomar en consideración las características generales y abstractas de los potenciales clientes o de los potenciales mercados, sino también adoptar mecanismos para valorar el riesgo concreto que se vincula a un cliente o a un mercado específico. Esto significa que la entidad debe aprobar mecanismos para obtener la información necesaria y suficiente, que se requiere para conocer de manera completa a sus clientes y

(Cont. nota 16)

Adicionalmente, en ese mismo concepto la Superintendencia Financiera explicó que: “Para efectos de la Circular Externa 061 de 2007, el concepto de ‘cliente’ no incluye a las personas naturales o jurídicas con las cuales Leasing (...) S.A. establece y mantiene una relación de origen legal o contractual derivada de actividades que son necesarias para el adecuado funcionamiento de la entidad, pero que son ajena, en estricto sentido, al objeto social, como son v. gr.: contratos asesoría, convenciones laborales, seguridad, papelería, arrendamiento o adquisición de bienes para operar, etc. (lit. c) citado) y que adicionalmente no suponen el suministro de un producto de la entidad vigilada hacia tales personas naturales o jurídicas.

“Finalmente, debe señalarse que el hecho de que tales personas no queden comprendidas dentro del concepto de ‘cliente’ para efectos de la circular citada, no significa que la entidad no deba obrar con la prudencia y diligencia necesarias para conocer a todas las personas con quienes pretenda relacionarse contractualmente y eventualmente efectuar la respectiva valoración del riesgo LA/FT al cual pudiera estar expuesta y los mecanismos de prevención y control aplicables según corresponda en estos eventos” (en este mismo sentido Cfr. el Cpto. número 2008060521-002 del 16 de octubre de 2008).

Por otra parte, en el Concepto 2008072629-001 del 15 de diciembre de 2008 la Superintendencia Financiera explicó que, en relación con las operaciones de transferencia internacional de recursos desde o hacia Colombia, “La entidad que frecuentemente está canalizando recursos de un mismo ordenante o hacia un mismo beneficiario debe tener un conocimiento profundo de quien provee o hacia quien se dirigen los recursos, conocimiento que le permite aplicar su SARLAFT y mitigar el riesgo implícito”. A tal efecto es necesario tener en cuenta, que el numeral 5º de la Circular Externa 026 de 2008 dispone textualmente que se considerará cliente de la entidad vigilada “Quien realice como ordenante, o reciba como beneficiario, tres (3) o más operaciones de transferencia en el trimestre, o cinco (5) o más en el semestre, o seis (6) o más en un año, se considerará como cliente”.

Sumado a lo anterior, en el Concepto 2008060521-002 del 16 de octubre de 2008 la Superintendencia concluyó que: “En lo relativo al ‘conocimiento del cliente’ se involucra en el caso de las aseguradoras al tomador, asegurado y beneficiario”.

sus mercados. Es decir, la entidad debe adoptar procedimientos y herramientas que le permitan conocer adecuadamente sus clientes y el mercado en el que se mueve, así como definir metodologías para la segmentación, clasificación y definición del perfil de sus clientes y mercados⁽¹⁷⁾.

La circular básica jurídica contiene una prolífica regulación acerca de cómo deben ser esos mecanismos para el conocimiento de los clientes y de los mercados. Allí se prevé que la entidad debe diseñar unos formularios para la vinculación de sus clientes, a través de los cuales se obtiene una información mínima que es necesaria para definir el perfil de riesgo de cada uno de ellos, y de los mercados a los que pertenecen⁽¹⁸⁾. En esa

(17) En Concepto 2008027339-001 del 15 de mayo de 2008, la Superintendencia Financiera explicó que: “El Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo que debe ser puesto en marcha por las entidades vigiladas por la Superintendencia Financiera de Colombia a partir del 1º de julio del año en curso, debe abarcar todas las actividades que realizan las entidades en desarrollo de su objeto social principal y deberá prever además procedimientos y metodologías para que las entidades se protejan de ser utilizadas como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades delictivas.

“En este sentido, las entidades deben contar con procedimientos adecuados para obtener un conocimiento efectivo, eficiente y oportuno de todos los clientes actuales y potenciales, así como para verificar la información y los soportes pertinentes provenientes de los mismos.

“En estrecha armonía con lo anterior, el conocimiento del cliente supone recoger la información prevista en el artículo 4.2.2.1.1, literales a); b); c) y d), con el propósito de cumplir los objetivos descritos en los numerales I), II) y III) del mismo artículo, incluyendo la información mínima señalada en el formulario para la vinculación de las personas naturales como de las personas jurídicas propuesta en el párrafo tercero de la misma norma, sin perjuicio de la información adicional que cada entidad haya determinado como relevante y necesaria para controlar el riesgo de LA/FT”.

(18) En Concepto 2008072629-001 del 15 de diciembre de 2008, la Superintendencia Financiera explicó que: “Para que una persona sea considerada como cliente, su vinculación se efectúa mediante el diligenciamiento del formulario de solicitud de vinculación por parte del cliente y la aceptación de tal solicitud por parte de la entidad vigilada, previo el cumplimiento de las partes de los requisitos legales y de los establecidos por la propia entidad para ello, y no mediante la suscripción de tal o cual contrato.

“Finalmente, frente a su pregunta de si ‘...solo bastaría para ser considerado cliente, ser usuario de la entidad y haber diligenciado un formulario de vinculación’, la respuesta es afirmativa si el formulario de vinculación es un formulario

misma norma se señala también que es obligación de la entidad realizar una entrevista personal, para alcanzar un conocimiento efectivo, eficiente y oportuno de cada uno de sus clientes. Adicionalmente, que la entidad tiene la obligación de llevar a cabo las gestiones necesarias, tendientes a confirmar que la información suministrada en el formulario sea verídica, y que dicha se mantenga permanentemente actualizada⁽¹⁹⁾.

(Cont. nota 18)

diseñado con esa finalidad específica, es decir, que la entidad tenga definido y documentado que dicho formulario será diligenciado únicamente por quienes de acuerdo con sus políticas y la normatividad aplicable son considerados como clientes, o, si el denominado formulario de vinculación contiene un espacio en el que se señale claramente que la entidad vigilada aprobó la vinculación de quien lo diligenció. Si se trata del formulario denominado en la norma SARLAFT como ‘formulario de solicitud de vinculación’, –cuyo diligenciamiento es apenas la expresión de la voluntad del potencial cliente de ser admitido como tal por la entidad–, la respuesta es negativa salvo que en el cuerpo del documento citado quede claro que la entidad –luego de cumplir con los requisitos normativos y los que ella haya establecido para el efecto– ha aprobado su vinculación a la misma”.

Adicionalmente, en el Concepto 2008027339-001 del 15 de mayo de 2008, la Superintendencia Financiera explicó que: “Las instituciones financieras vigiladas por la Superintendencia Financiera de Colombia a partir de la entrada en vigencia del SARLAFT deberán solicitar el diligenciamiento del formulario de conocimiento del cliente a los representantes legales y a las demás personas encargadas de la disposición de los recursos del cliente que se vincula a la sociedad, como quiera que tales personas obran por cuenta de un tercero y en su nombre”.

- (19) En Concepto 2009010745-001 del 10 de marzo de 2009, la Superintendencia Financiera sostuvo lo siguiente: “Esta Superintendencia ha proferido instrucciones pertinentes a efectos de que las instituciones vigiladas adopten requerimientos mínimos en el conocimiento efectivo, eficiente y oportuno de todos los clientes actuales y potenciales, así como para verificar la información y los soportes de la misma, preceptos que están contenidos en el numeral 4.2.2.1.1 del Título I, Capítulo XI de la Circular Básica Jurídica (Cir. Externa 007 de 1996)”.

Por otra parte, en el Concepto 2008088852-001 del 26 de enero de 2009, la Superintendencia respondió la consulta formulada por una sociedad comisionista de bolsa, quien preguntaba si la negativa de un cliente a actualizar la información suministrada al momento de su vinculación autorizaba a la entidad a negarse a realizar las operaciones solicitadas por él, e incluso a negarse a terminar la relación comercial y a trasladar el portafolio a otra sociedad comisionista. En respuesta a esa consulta, la Superintendencia explicó que las entidades están obligadas a “diseñar y poner en práctica los procedimientos que le permitan realizar las diligencias necesarias para actualizar anualmente la información

(Cont. nota 19)

Los procedimientos mínimos para el conocimiento del cliente exigidos por la normatividad dependen de la naturaleza jurídica de cada uno de ellos⁽²⁰⁾. Por ejemplo, la información requerida y los procedimientos de verificación y actualización de la misma dependen de si el cliente es una persona natural o jurídica. Además, la circular básica jurídica también establece excepciones al deber de diligenciar el formulario o de realizar entrevista en ciertos casos especiales: por ejemplo, cuando el cliente es un organismo multilateral, una entidad pública, cuando se trata de la vinculación de un mismo cliente por parte de diferentes entidades pertenecientes a un mismo grupo financiero, etc.⁽²¹⁾.

Por otra parte, estos mecanismos para el conocimiento del cliente y del mercado son fundamentales, porque gracias a ellos la entidad obtiene la información necesaria para procesar adecuadamente sus operaciones, en orden a controlar los riesgos que la asechan. En efecto, una parte importante del control del riesgo de lavado de activos y financiación del terrorismo es la identificación, gestión y reporte de operaciones inusuales o

de los clientes que por su naturaleza puedan variar”. Así mismo, aclaró que las entidades cuentan con libertad para elegir los mecanismos que implementarán para garantizar que la información del cliente se mantenga actualizada, “no siendo competencia de esta Superintendencia determinar cuál debe ser la posición de una entidad vigilada frente a un hecho o circunstancia particular surgida de la actuación o no actuación de su/s cliente/s”.

- (20) En Concepto 2008026810-001 del 7 de julio de 2008, la Superintendencia informó que “mediante Circular Externa 26 de 2008, esta entidad pública realizó algunas precisiones al Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo, relacionadas con el alcance de la verificación de la información que suministren los clientes cuando se trate de cuentas de ahorro y planes de ahorro contractual de bajo monto, de que trata el Decreto 1119 de 2008”.
- (21) En Concepto 2005062113-1 del 27 de enero de 2006, la Superintendencia aclaró que: “Las reglas relativas a la prevención y control del lavado de activos prevén, cuando aplique, la exigencia de los estados financieros cuando la persona detenta la calidad de comerciante (...). “Así las cosas, debe entenderse que sólo hay lugar a exigir estados financieros certificados o dictaminados a la última fecha de corte disponible al momento de la apertura, cuando aplique, es decir, cuando la persona detente la calidad de comerciante, es decir, aquellas que profesionalmente se ocupan en alguna de las actividades que la ley considera mercantiles en los términos del artículo 20 del Código de Comercio”.

sospechosas, las cuales permiten a la entidad adoptar los cursos de acción más convenientes para gestionar el riesgo al que se encuentra expuesta, y cumplir satisfactoriamente su deber de colaborar con las autoridades en su política de prevención y represión del delito.

Además de los mecanismos para conocimiento del cliente y del mercado, la entidad debe diseñar metodologías para definir medidas de control de otras fuentes de riesgo como los canales de distribución y la legislación aplicable en los diferentes mercados en los que actúa. Esto significa que la entidad debe establecer procedimientos y criterios para definir de qué manera intentará mitigar los riesgos identificados y medidos en las dos etapas anteriores.

En relación con los canales de distribución, las entidades deben establecer mecanismos para asegurar que los riesgos de lavado de activos inherentes a ellos sean debidamente controlados. Esto significa que deben adoptar políticas y reglamentos sobre la forma de comercialización y distribución de sus bienes y servicios, y sobre la forma de efectuar o recibir pagos. Por ejemplo, las empresas deben fijar políticas y reglamentos que restrinjan la comercialización de sus productos o servicios entre grupos con alto perfil de riesgo de lavado de activos, o como mínimo adoptar controles adicionales. Así mismo, podría tomar medidas para restringir el acceso a ciertos productos o servicios sólo a clientes ampliamente conocidos. Este tipo de medidas debe asegurar al máximo que los productos de la entidad no lleguen a manos de personas que puedan utilizarlos, para el aprovechamiento, inversión, manejo, transporte, administración, ocultamiento o encubrimiento del origen de recursos ilícitos. Así mismo, estos mecanismos deben procurar garantizar que la entidad no pueda ser utilizada para colaborar, financiar, apoyar o encubrir a grupos terroristas.

En cuanto a la legislación aplicable, las entidades vigiladas deben tener en cuenta la legislación vigente en materia de prevención y represión de lavado de activos en los diferentes mercados en los que actúa. Especialmente aquellas que tienen filiales o corresponsales en el exterior, y/o aquellas que prestan servicios financieros internacionales; también, deben tener en cuenta que la legislación en esta materia no es igualmente estricta en todos los países. Hay Estados donde la legislación en materia de prevención del lavado de activos es mucho más laxa, y ello puede facilitar

tar la realización de operaciones de esa naturaleza hacia Colombia. El hecho de realizar operaciones directamente o a través de corresponsales, filiales o socios en aquellos países en los que la legislación es menos rígida, expone a las entidades vigiladas a un riesgo mayor de lavado de activos y financiación del terrorismo. Por esta razón, las entidades deben tomar en cuenta las características propias de la legislación aplicable en los diferentes mercados en que incursiona, y tomar medidas de protección adicionales en caso de que la normatividad sea exigua o insuficiente, procurando incluso no realizar negocios con los llamados “paraísos fiscales” identificados así por la OCDE. Así mismo, las entidades podrían exigir a sus filiales, corresponsales o socios internacionales, que tomen medidas adicionales a las previstas en su legislación, para prevenir este tipo de delitos.

Al final de esta etapa, luego de definir todos los mecanismos para controlar el riesgo, la entidad debe llevar a cabo una medición del riesgo residual. Es decir, una medición del riesgo resultante al que queda expuesta la entidad, después de adoptar todo el SARLA/FT. A tal efecto, debe definir metodologías para establecer cuáles son los límites máximos de riesgo tolerable, y debe procurar que los mecanismos de control definidos reduzcan el riesgo residual por debajo de ese nivel. Como consecuencia de lo anterior, la etapa de control del riesgo sólo puede quedar concluida, cuando este sea no sólo inferior al riesgo inherente al que estaba originalmente expuesta la entidad, sino incluso inferior al nivel máximo de riesgo tolerable definido por ella.

1.4. Monitoreo del riesgo

La etapa de monitoreo del riesgo está constituida fundamentalmente por dos clases de actividades: 1. por todas las actividades que debe llevar a cabo la entidad, en orden a garantizar el correcto funcionamiento del SARLA/FT; 2. por todas las que son necesarias para la detección y reporte de operaciones inusuales o sospechosas.

Frente a lo primero, una de las principales actividades que debe realizarse es la definición de una metodología para la supervisión periódica del SARLA/FT. De acuerdo con la circular básica jurídica, las entidades vigiladas están obligadas a desarrollar procedimientos para determinar

y corregir periódicamente las deficiencias del sistema (mínimo cada seis meses). Estos procedimientos deben garantizar que la entidad esté en capacidad de identificar y corregir eficaz y eficientemente los defectos del sistema.

En términos prácticos, el monitoreo del riesgo implica actualizar periódicamente los datos obtenidos en la etapa de medición o evaluación del mismo, mediante la reaplicación periódica de las metodologías definidas entonces. Esta actualización ha de permitir que la entidad obtenga periódicamente información renovada acerca de su perfil de riesgo residual (riesgo resultante después de implementar el SARLA/FT). Con base en esta información actualizada es posible determinar si en ese momento el riesgo residual es menor o mayor al inherente (riesgo al que se encuentra inherentemente expuesta dada la naturaleza de su objeto social), y de esa forma establecer si la entidad ha mejorado o no su perfil de riesgo durante un período determinado.

En efecto, para garantizar el correcto funcionamiento del sistema, las entidades vigiladas deben definir metodologías que les permitan realizar una comparación entre el riesgo inherente y residual. Esta diferencia es un indicador importante del estado actual de la entidad y debe arrojar un índice o indicador en materia de prevención de lavado de activos y financiación del terrorismo. Al comparar el índice actual con los correspondientes a períodos anteriores es posible obtener un diagnóstico siquiera aproximado del desempeño del SARLA/FT en un período determinado. Esta información es fundamental no sólo para tomar decisiones orientadas a mejorar el sistema, sino para evaluar la eficacia de decisiones adoptadas anteriormente.

Además de este índice comparativo entre el riesgo inherente y el residual, las entidades vigiladas están en la obligación de establecer otros indicadores que les permitan medir el riesgo actual al que se encuentran expuestas, y predecir el comportamiento futuro del mismo. El propósito de estos otros indicadores es garantizar que el riesgo residual se mantenga siempre dentro de niveles tolerables para la sociedad.

Ahora bien, ya en lo que hace a lo segundo, la circular básica jurídica prevé que las entidades vigiladas deben definir las metodologías que les permitan identificar oportunamente las operaciones inusuales y sospecho-

sas. De acuerdo con la definición legal prevista en la circular básica jurídica, las operaciones inusuales son aquellas que no guardan relación con la actividad económica del cliente, que se salen del rango de normalidad fijado por la entidad para el cliente o para determinado segmento de mercado, o aquellas respecto de las cuales la entidad no ha encontrado una justificación razonable. A su turno, la circular básica jurídica también define las operaciones sospechosas como aquellas que además de ser inusuales, ofrecen motivos para pensar que pueden ser constitutivas de una actividad de lavado de activos o de financiación del terrorismo.

En relación con la identificación de operaciones inusuales, la entidad debe crear mecanismos que le permitan conocer cuándo una operación se sale del rango de normalidad definido para un cliente o para un mercado específico. Al respecto, la circular básica jurídica indica que las entidades deben elaborar un catálogo de señales de alerta que permitan llamar la atención, cuando una operación se salga de su rango de normalidad⁽²²⁾.

-
- (22) La Unidad de Información y Análisis Financiero (UIAF) elabora un documento relacionado con las señales de alerta, el cual es de mucha utilidad. Este documento es de carácter reservado, y a él sólo pueden tener acceso las personas que tienen la obligación de realizar reporte de operaciones sospechosas a la UIAF. La UNODC también ha publicado un documento similar titulado “Riesgo de Lavado de Activos en Instrumentos Financieros, Usuarios y Empleados de Instituciones Financieras”, en el que se relacionan 451 señales de alerta clasificadas de acuerdo a los diferentes productos financieros en los que pueden encontrarse. Este documento es público y puede consultarse en la página web http://www.superbancos.gob.pa/aspec_prevencion/documentos/UNODC_Instrumentos_Financieros200608.pdf (consultada el 6 de octubre de 2009).

Ahora bien, en relación con este tema la UNODC ha explicado lo siguiente: “Una señal de alerta es simplemente un hecho, información o circunstancia particular que rodea la realización de una transacción o actividad (vinculación, comportamiento o transacción) de un cliente, usuario o funcionario de una entidad financiera que supera lo normal.

La particularidad del hecho o circunstancia debe ser notoria pues por sus características debe superar lo puramente normal, habitual y corriente. Por lo anterior, las situaciones detectadas deben ser objeto de una validación y de un estudio cuidadoso y detallado para establecer su frecuencia, particularidades y acciones a tomar.

Cuando se ha identificado una señal de alerta, a partir de la determinación de múltiples situaciones disímiles, es preciso realizar un análisis más profundo y (Cont. nota 22)

exigente para cada una de ellas, sobre todo si el propósito es detectar o analizar

Por ejemplo, la entidad debe estar en condiciones de saber cuál es la cuantía normal de las operaciones de un determinado cliente, dado su perfil económico y comercial. Si una transacción excede notablemente la cuantía normal de las operaciones de un cliente, este hecho debe ser considerado por la entidad como una señal de alerta acerca de que esa operación puede ser inusual.

Por supuesto, la identificación de operaciones inusuales depende de que la entidad haya definido previamente metodologías para: 1. establecer cuál es el rango de normalidad para determinado cliente o segmento de mercado; 2. establecer si una operación en concreto se sale o no del rango de normalidad definido. Estas metodologías deben ser definidas mediante la indicación de los procedimientos y criterios que deben tenerse en cuenta en cada caso, para determinar el rango de normalidad o para establecer en un caso concreto si una operación específica se encuentra dentro de la normalidad. Así mismo, la entidad debe definir quiénes son los funcionarios competentes para aplicar esas metodologías, cuáles son las calidades que deben tener esos funcionarios, y el alcance de su responsabilidad frente a dichas tareas.

La información que sirve de materia prima para la identificación de las operaciones inusuales es producto de la aplicación de los mecanismos para el conocimiento del cliente y del mercado que ya se ha mencionado. Es decir, la información que se procesa a través de las metodologías definidas para la identificación de las operaciones inusuales proviene en su mayoría, de la aplicación de los mecanismos de conocimiento del cliente y del mercado. A la sazón, nótese que la información obtenida acerca del

una posible operación de lavado de activos y/o financiación del terrorismo.

Las señales de alerta que provienen exclusivamente del movimiento transaccional de un cliente no son suficientes para identificar alguna actividad ilícita. Se requiere analizar las operaciones, durante un periodo de tiempo adecuado, de manera comparativa con su respectivo perfil de actividad. Es importante relacionar su actividad económica, con el tipo de persona (natural o jurídica), con su ubicación geográfica y con la frecuencia y características de sus operaciones. En todo caso, se debe tener en cuenta que “cualquier señal de alerta puede ser desvirtuada si concurren hechos o circunstancias que expliquen de manera razonable los hechos que la originó” (*Riesgo de lavado de activos en instrumentos financieros, usuarios y empleados de instituciones financieras*, p. 8).

perfil económico y comercial del cliente es la que permite determinar, cuáles son los rangos dentro de los que puede considerarse que una operación suya es normal. Así mismo, la información obtenida acerca de la dinámica económica de los diferentes mercados en los que participa la entidad permite establecer, cuáles son los rangos dentro de los que puede considerarse que determinado tipo de operación es normal. Teniendo en cuenta lo anterior, puede observarse que esta información acerca de los rangos de normalidad de los clientes y de los mercados es útil para establecer, si una operación determinada es o no inusual.

La detección de las operaciones sospechosas es diferente, porque allí se necesita una valoración adicional. A diferencia de las operaciones inusuales, la identificación de operaciones sospechosas requiere que la entidad haga una valoración de todo el contexto en el que se llevó a cabo la operación, adicionando al estudio la información disponible acerca de las diferentes modalidades o tipologías de lavado de activos y financiación del terrorismo (en esta tarea resulta de vital importancia el trabajo que realiza la Unidad de Información y Análisis Financiero (UIAF), quien se ocupa de compilar y publicar las diferentes tipologías de lavado de activos descubiertas por esa entidad⁽²³⁾). Esto significa que la identificación de las operaciones sospechosas exige que la entidad proceda a realizar un estudio, en el cual debe tenerse en cuenta no sólo la información acerca de la operación específica, sino también todo el conocimiento y experiencia adquirida acerca de las tipologías de lavado de activos y financiación del terrorismo. Es decir, es necesario cruzar la información disponible sobre la operación inusual, con todos los conocimientos y experiencia criminológica y criminalística acumulada respecto del lavado de activos y la financiación del terrorismo.

Este tipo de estudio le permite a la entidad determinar si hay o no ra-

(23) Mediante la página web de la UIAF se puede acceder al documento titulado “Compilación y descripción de las tipologías producidas por la unidad de información y análisis financiero. Documento público” (versión de septiembre de 2006) publicado de forma institucional por esa entidad, el cual es accesible a través de la dirección URL http://www.uiaf.gov.co/index.php?idcategoria=35&uiaf_2008=f88de3cb178328aa37926f25a09340fa (consultada el día 16 de septiembre de 2009).

zones para pensar, que una operación que en principio era simplemente inusual puede ser constitutiva de lavado de activos o financiación del terrorismo. Dicho de otra manera, luego de realizar una valoración de las circunstancias de modo tiempo y lugar en que se produjo la operación inusual, a la luz de lo que se sabe sobre las distintas modalidades de este tipo de delitos, la entidad debería estar en condiciones de establecer si existen serios motivos para pensar que la operación es sospechosa, y que debe ser reportada a las autoridades para una mayor investigación⁽²⁴⁾.

Ahora bien, en ningún caso el sistema de administración del riesgo de lavado de activos y financiación del terrorismo puede agotarse con la identificación de las operaciones sospechosas. Para que el sistema de prevención sea efectivo se requiere que la entidad defina además, la manera en que deben gestionarse ese tipo de operaciones. Es decir, debe definir con claridad el curso de acción que debe seguirse en caso de identificar una operación sospechosa. También, debe indicar en cada caso qué actitud debe asumirse frente al cliente y frente a la operación sospechosa. Por ejemplo, la entidad debe definir si dentro de sus políticas se hace prevalecer la moralidad sobre la obtención de las metas económicas, y en consecuencia si debe siempre abstenerse de realizar operaciones sospechosas, o si por el contrario procede a realizarlas y luego a reportarlas⁽²⁵⁾.

-
- (24) En Concepto 2009017224-003 del 22 de abril de 2009 la Superintendencia aclaró lo siguiente: “Sea lo primero señalar que lo que se reporta son las operaciones que realizan los clientes, no los clientes como tales”.
- (25) En Concepto 2005049770-004 del 27 de febrero de 2006, la Superintendencia aclaró lo siguiente: “Conforme a lo anteriormente expuesto, es dable concluir que en la medida en que las entidades vigiladas por esta Superintendencia sean diligentes en relación con el conocimiento del cliente, en el sentido de conocer sus hábitos de consumo, sus preferencias, sus especiales características frente a los demás clientes, segmento del mercado en el que se desarrollan, etc., ello facilitará al banco, como profesional de la actividad financiera, detectar comportamientos irregulares que de manera objetiva y razonable le sirvan de causa para finiquitar determinados vínculos comerciales. En todo caso, es preciso advertir que el ROS no constituye per se una causa objetiva y razonable para dar por terminado el vínculo con el cliente, porque, además de que la ley le atribuye el carácter de reservado (art. 105 del EOSF), el ROS por sí solo no hace que se configure el tipo delictivo de lavado de activos. Para que el ROS se constituya en factor objetivo, debe traducirse en incautaciones e investigaciones efectivas y éstas, a su turno, en sentencias condenatorias (Cont. nota 25)

Por lo demás, tal como se encuentra prevista la estructura del SARLA/FT en la circular básica jurídica puede decirse, que el monitoreo de las operaciones debe hacerse mediante un procedimiento caracterizado por la concurrencia de diferentes metodologías y por la división de roles y funciones. Para comenzar, los funcionarios que tienen un contacto más directo e inmediato con las operaciones estarían a cargo de la identificación de las señales de alerta de operaciones inusuales. Una vez advertida la existencia de una señal de alerta, la información debe ser remitida al funcionario que indique la entidad, para que con base en una metodología previamente definida se determine si la operación se sale efectivamente del rango de normalidad establecido para el cliente o para el mercado correspondiente. En esta tarea tiene vital importancia el procesamiento de la información obtenida mediante la aplicación de los mecanismos de conocimiento del cliente y del mercado, porque de este procesamiento de información resulta el perfil económico y comercial que permite establecer cuándo una operación es normal para el cliente, o para el segmento de mercado correspondiente. Ahora bien, en caso de encontrarse que la operación es inusual, la información sobre la operación debe remitirse al departamento de cumplimiento para que, a partir de una metodología previamente definida, el funcionario que señale la entidad valore si hay razones para pensar que la operación puede ser constitutiva de lavado de activos o financiación del terrorismo. De ser así, el oficial de cumplimiento de la entidad debe reportar la operación a las autoridades, para que ellas abunden en la investigación sobre la licitud de la operación.

2. ELEMENTOS DEL SARLA/FT

Para la realización de las diferentes fases que componen el SARLA/FT se hace necesario que la entidad adquiera una infraestructura especialmente dedicada a la administración del riesgo de lavado de activos y financiación del terrorismo. Esta infraestructura debe comprender todo lo necesario para realizar adecuadamente las diferentes etapas del SARLA/FT, especialmente los recursos humanos, físicos, económicos y tecnológicos requeridos en cada una de ellas. La Circular Externa 022 de 2007 contem-

proferidas por la autoridad judicial competente”.

pla una regulación en la que se prevé cuáles son los elementos mínimos que debe tener el SARLA/FT, agrupándolos en ocho categorías a saber: políticas, procedimientos, documentación, estructura organizacional, órganos de control, infraestructura tecnológica, divulgación de la información y capacitación.

2.1. **Políticas**

Las entidades vigiladas se encuentran obligadas a definir sus políticas frente a la prevención del lavado de activos y la financiación del terrorismo. Para tal efecto, ellas deben elaborar un código de ética en el que se establezcan los principios y reglas generales que orientan la manera en que deben actuar los funcionarios de la entidad en cada etapa del SARLA/FT. Los principios y las reglas de conducta definidos por la entidad deben promover el eficaz, eficiente y oportuno funcionamiento del sistema. De igual manera, estos principios y reglas deben ofrecer criterios para resolver los conflictos de interés, promoviendo el cumplimiento de las normas en materia de prevención de lavado de activos y financiación del terrorismo al logro de las metas comerciales de la entidad.

En el mismo sentido, el código de ética debe contener un régimen sancionatorio que defina, no sólo las responsabilidades en materia de prevención de lavado de activos y financiación del terrorismo para cada uno de los funcionarios de la entidad dependiendo de sus funciones y jerarquía, sino también las consecuencias que puede causar el incumplimiento de las responsabilidades a su cargo. En este sentido, las disposiciones del código de ética en materia sancionatoria podrían y deberían entenderse incorporadas a las obligaciones laborales de los funcionarios, de manera que la entidad pueda legalmente exigir su cumplimiento e imponer sanciones en caso de incumplimiento.

2.2. **Procedimientos**

Para poder cumplir las actividades correspondientes a las diferentes etapas del SARLA/FT, las entidades vigiladas deberán previamente definir las metodologías que se aplicarán en cada una de ellas, y de igual manera describir los procedimientos que deben seguirse en cada caso. Por esta

razón, la circular básica jurídica obliga a las entidades vigiladas a elaborar un manual para tal evento.

El manual adoptado por la entidad debe definir principalmente los procedimientos que deben aplicarse en cada una de las etapas del SARLA/FT, y al mismo tiempo establecer quiénes son los funcionarios responsables de su ejecución⁽²⁶⁾. De esta manera, el manual debe establecer, por ejemplo, los procedimientos para el conocimiento del cliente, para el conocimiento del mercado, para la segmentación y clasificación de los factores de riesgo, para la medición y evaluación del riesgo residual, para la determinación de los rangos de normalidad, para la detección de operaciones inusuales y sospechosas, para el reporte de operaciones sospechosas, para monitorear periódicamente el funcionamiento global del SARLA/FT, etc.

De igual manera, el manual ha de fijar un procedimiento para la imposición de las sanciones definidas en el código de ética, como consecuencia del incumplimiento de las responsabilidades atribuidas en materia de prevención del lavado de activos y financiación del terrorismo a cada funcionario. Dicho procedimiento debe asegurar que los funcionarios de la entidad gocen de las garantías mínimas fundamentales previstas en la Constitución y en el Régimen Laboral, tales como el derecho de defensa y el debido proceso. Así mismo, el manual debe establecer criterios para la graduación de la sanción, y para valorar su necesidad, razonabilidad y proporcionalidad.

(26) En materia de reporte de operaciones sospechosas, la Superintendencia Bancaria (hoy Superintendencia Financiera) sostuvo en el Concepto 2003044819-1 del 15 de septiembre de 2003 lo siguiente: “En tal sentido, es del resorte de cada entidad establecer dentro de sus manuales internos, orientados bajo principios de armonía, eficiencia y coordinación, a cargo de quién está la obligación de remitir el reporte, previa la información remitida por los diferentes funcionarios de la institución a fin de que haya una gestión proactiva en materia de prevención de lavado de activos, sin que sea dable a esta Agencia Gubernamental determinar a cargo de quien está dicha responsabilidad. Lo anterior, sin perjuicio del cumplimiento de la instrucción de este organismo en torno al nombramiento del *oficial de cumplimiento* quien debe velar porque se observen las normas referentes al lavado de activos”.

2.3. Documentación

Por expresa disposición de la circular básica jurídica, todas las actividades realizadas a lo largo de las diferentes etapas del SARLA/FT deben quedar registradas y documentadas por la entidad. Esto supone que las entidades vigiladas están obligadas a implementar sistemas para el manejo de la documentación relacionada con las actividades de prevención del lavado de activos y financiación del terrorismo. Dichos sistemas pueden ser implementados directamente por la entidad, o también es posible que la entidad contrate a un tercero que se encargue del manejo, archivo y conservación de la documentación. En este último caso, el tercero debe cumplir con los requisitos exigidos por la Superintendencia Financiera para garantizar la reserva, seguridad, autenticidad, integridad y accesibilidad de la información contenida en los documentos⁽²⁷⁾.

Los sistemas de manejo de la documentación adoptados por las entidades vigiladas deben cumplir los requisitos mínimos exigidos por la

-
- (27) En la Circular Externa 052 de 2007 se dispone que es posible que las entidades vigiladas celebren contratos de *outsourcing* para que un tercero realice la captura y/o procesamiento de datos de la entidad y/o de sus clientes. No obstante, como se trata de información confidencial sujeta a reserva, este tercero deberá cumplir como mínimo con los siguientes requerimientos:
1. Definir los criterios y procedimientos a partir de los cuales se seleccionará el tercero y el servicio que será atendido por él.
 2. Incluir en el contrato que se celebre con el tercero o en aquellos que se prorroguen a partir de la entrada en vigencia de la norma, por lo menos, los siguientes aspectos: a) Niveles de servicio y operación; b) Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas; c) Propiedad de la información; d) Restricciones sobre el software empleado; e) Normas de seguridad informática y física a ser aplicadas; f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información, y g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.
 3. Exigir que el tercero contratado disponga de planes de contingencia y continuidad debidamente documentados. La entidad deberá verificar que los planes, en lo que corresponden a los servicios convenidos, funcionen en las condiciones esperadas.
 4. Establecer procedimientos que permitan identificar físicamente, de manera inequívoca, a los funcionarios de los terceros contratados.
 5. Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con el tercero contratado.

circular básica jurídica. Los requisitos exigidos por esta normatividad consisten fundamentalmente en que el sistema de manejo de la documentación debe contar con un respaldo físico, con medidas de seguridad que garanticen que la información sólo pueda ser conocida y consultada por las personas autorizadas, y con medidas de protección que garanticen su adecuada conservación⁽²⁸⁾. Adicionalmente, el sistema de manejo implementado debe hacer posible que la entidad o las autoridades judiciales puedan consultar fácilmente cualquier documento o registro en poder de la entidad, para obtener de modo rápido, eficaz y eficiente cualquier dato. Por esta razón, el sistema de manejo de documentos debe contar con mecanismos de búsqueda de información que permitan responder de manera ágil y eficaz cualquier consulta.

2.4. Estructura organizacional

En materia de recursos humanos, la entidad debe contar con personal especialmente dedicado al control y monitoreo del riesgo de lavado de activos y financiación del terrorismo. Este personal normalmente hace parte del departamento de cumplimiento, control, prevención o como quiera que se llame al interior de cada entidad. En los términos de la circular básica jurídica, este personal debe estar capacitado en materia de prevención de lavado de activos, ya que su principal función es apoyar técnica y operativamente al oficial de cumplimiento en el ejercicio de sus tareas. Es una función exclusiva y excluyente, que no debe realizarse de manera conjunta con otras tareas, dada la importancia que reviste.

(28) En Concepto 2008040297-002 del 10 de octubre de 2008, la Superintendencia sostuvo que: “El Estatuto Orgánico del Sistema Financiero en su artículo 96 establece, ‘*Conservación de archivos y documentos*. Los libros y papeles de las instituciones vigiladas por la Superintendencia Bancaria deberán conservarse por un período no menor de cinco años (5) años, desde la fecha del respectivo asiento, sin perjuicio de los términos establecidos en normas especiales. Vencido este lapso, podrán ser destruidos siempre que, por cualquier medio técnico adecuado, se garantice su reproducción exacta...’.

“En este orden de ideas debe entenderse que una vez transcurran los cinco años a que alude el artículo 96 precitado, la correspondencia, libros y papeles de las entidades aseguradoras pueden destruirse siempre y cuando se asegure su reproducción por cualquier medio técnico adecuado”.

Paralelamente la entidad debe identificar, quiénes son los funcionarios que debido a su ubicación dentro de la estructura organizacional se encuentran en contacto directo con las fuentes y factores de riesgo. A estos funcionarios debe asignarse una serie de competencias para identificar, medir, controlar y monitorear el riesgo de lavado de activos y financiación del terrorismo. Dichas competencias deben ser desarrolladas a través de la definición de actividades y procedimientos asignados a cada funcionario, según su cargo y nivel de responsabilidad dentro de la entidad. Así mismo, los procedimientos y actividades asignados deben ser descritos y explicados en un manual de procedimientos, el cual ha de ser conocido y comprendido por los funcionarios involucrados en el SARLA/FT.

Entre los órganos o funcionarios más importantes a quienes deben asignarse competencias en materia de administración del riesgo, la circular básica jurídica menciona los siguientes:

1. La junta directiva o Directorio, que como órgano corporativo tiene una función de dirección estratégica de la política de prevención del lavado de activos y financiación del terrorismo. Es la junta directiva quien tiene, entre otras, la responsabilidad de aprobar el código de ética y el manual de procedimientos adoptado por la entidad, aun cuando estos elementos del sistema hayan sido proyectados o preparados por otros funcionarios. La junta directiva debe también designar al *oficial de cumplimiento* de la entidad, y ejercer un control periódico sobre el desempeño global del SARLA/FT a partir de los informes presentados por éste o por cualquier otro órgano de control de la entidad. Este órgano tiene así mismo la obligación de ordenar la apropiación de los recursos humanos, físicos, económicos y tecnológicos necesarios para el funcionamiento del SARLA/FT. Además, tiene la responsabilidad de autorizar la vinculación de clientes o la realización de operaciones, cuando en ellas se advierta que aumenta el nivel de riesgo al que se encuentra expuesta la entidad.

2. El representante legal es el funcionario encargado de la ejecución de las políticas de prevención definidas por la junta directiva. No obstante, este funcionario tiene responsabilidades en todas las etapas del SARLA/FT, incluyendo el período de diseño y monitoreo del sistema. Por ejemplo, el representante legal tiene el deber de coordinar con el *oficial de cumplimiento* la preparación del código de ética y del manual de procedimientos,

para someterlo a la aprobación de la junta directiva. Así mismo, el representante legal también debe adoptar –dentro de la órbita de sus competencias– las medidas necesarias para corregir los defectos del sistema, o informar a la junta directiva para que ésta las tome.

Fundamentalmente, el representante legal debe velar por el cumplimiento de todos los procedimientos, y por la eficacia de todos los mecanismos de prevención que integran el SARLA/FT. Esto significa que el representante legal debe adoptar las medidas necesarias para asegurar que el sistema funcione adecuadamente, proporcionando los recursos necesarios para ello. En este sentido, el representante legal debe prestar el apoyo administrativo, financiero y técnico que necesite el *oficial de cumplimiento* para el adecuado funcionamiento del SARLA/FT.

3. El *oficial de cumplimiento* es un funcionario de alto nivel jerárquico dentro de la entidad, cuya principal función es velar por el adecuado funcionamiento del SARLA/FT⁽²⁹⁾. De acuerdo con la circular básica

-
- (29) En Concepto 2005060654-1 del 24 de enero de 2006, la Superintendencia explicó que: “Comoquiera que es obligación de las instituciones sometidas a inspección y vigilancia de esta Superintendencia designar un funcionario como *oficial de cumplimiento*, su inobservancia da lugar a la imposición de sanciones administrativas, para cuyos efectos está facultada esta entidad, en virtud de los artículos 209 y 211 del EOSF, que prevén que las sanciones pueden ser de carácter personal o institucional, respectivamente.

Tales sanciones, pueden consistir en amonestación, multa pecuniaria, suspensión, inhabilitación para el ejercicio de cargos en entidades vigiladas, remoción de los administradores y clausura de las oficinas de representación, en los términos del numeral 3º del artículo 208.

Por su parte, la Ley 964 de 2005 del Mercado de Valores tipifica como infracción en el literal t) del artículo 50: “Incumplir las normas sobre designación de defensor del cliente, miembros independientes de la junta directiva, oficial de cumplimiento o miembros del comité de auditoría, contralor normativo; no efectuar las apropiaciones necesarias para el suministro de los recursos humanos y técnicos que quienes ejercen los mencionados cargos requieran para su adecuado desempeño o no proveer la información que los mismos necesiten para el ejercicio de sus funciones. Para quienes actúen como defensor del cliente, miembros de junta directiva, oficial de cumplimiento, miembros del comité de auditoría y contralor normativo incumplir con los deberes y obligaciones establecidos para el desarrollo de sus funciones. Esta infracción únicamente será aplicable a las personas sujetas a la inspección y vigilancia permanente de la Superintendencia de Valores y a los emisores de valores sometidos a su control exclusivo”.

jurídica, el *oficial de cumplimiento* debe pertenecer como mínimo al segundo nivel jerárquico de la entidad, es decir, sólo puede estar por debajo de la junta directiva al mismo nivel del representante legal. Este funcionario debe tener capacidad decisoria, no puede pertenecer a los otros órganos de control ni realizar funciones propias del objeto social de la entidad. Se trata de un funcionario designado por la junta directiva, cuya posesión se realiza ante la Superintendencia Financiera previa verificación de su idoneidad⁽³⁰⁾.

(Cont. nota 29)

En consecuencia, incurrir en tales infracciones dará lugar, en los términos del artículo 53 de la referida Ley 964, a la imposición de las siguientes sanciones: amonestación, multa, suspensión o inhabilitación, hasta por cinco (5) años para realizar funciones de administración, dirección o control de las entidades sometidas a vigilancia; remoción de los administradores, suspensión y cancelación de la inscripción, en cualquiera de los registros previstos en la Ley”.

Por otra parte, la Superintendencia Financiera impartió instrucciones mediante la circular externa 060 de 2008, en el sentido de que el emisor que coloque directamente una emisión en el mercado primario tiene la obligación de adoptar un SARLAFT, aun cuando no esté sometido a la inspección, vigilancia y control de la Superintendencia. De acuerdo con lo previsto en esa circular externa, en el Concepto 2009044020-001 del 9 de julio de 2009 la Superintendencia Financiera aclaró lo siguiente: “Si el proceso de colocación de la emisión que se proyecta sacar al mercado lo asume directamente el emisor de los valores, sin la intervención de ninguna entidad vigilada, corresponde a este emisor darle plena y total aplicación a las instrucciones relativas a la prevención y control de riesgo de lavado de activos y de la financiación del terrorismo y en este caso el emisor deberá crear al interior de la misma sociedad la figura del *oficial de cumplimiento*. Cuando la colocación en el mercado primario se haga a través de una entidad vigilada por la Superintendencia Financiera de Colombia, corresponderá a dicha entidad darle aplicación a las instrucciones relativas a la administración del riesgo de lavado de activos y de la financiación del terrorismo y, por tanto, tener la figura del *oficial de cumplimiento*” (en este mismo sentido cfr., también el Cpto. 2006018977-001 del 23 de mayo de 2006, el Cpto. 2008009513-001 del 11 de marzo de 2008 y el Cpto. 2008031221-001 del 9 de junio de 2008).

- (30) En Concepto 2005060654-1 del 24 de enero de 2006, la Superintendencia Financiera explicó que: “No obstante, dada la naturaleza de las actividades que las instituciones sujetas a control realizan, se ha considerado que el funcionario que se designe como oficial de cumplimiento, debe gozar de las más altas calidades de idoneidad, responsabilidad y carácter que le permitan desempeñar el cargo. “En ese orden de ideas todo funcionario obligado a posesionarse ante esta entidad, debe observar lo previsto de manera general en el artículo 53 del EOSF, en cuanto es deber de la Superintendencia Financiera de Colombia abstenerse de autorizar las participación en las entidades sujetas a control de las personas en

Adicionalmente, el *oficial de cumplimiento* tiene la obligación de presentar a la junta directiva informes periódicos (por lo menos trimestralmente) sobre el funcionamiento del sistema. Paralelamente, el *oficial de cumplimiento* debe adoptar –dentro de la órbita de sus competencias– las medidas necesarias, tendientes a corregir los problemas del SARLA/FT. En caso de no tener las facultades necesarias para hacerlo, debe promover ante el órgano competente la implementación de los correctivos.

2.5. Órganos de control

A pesar de que la junta directiva, el representante legal y el oficial de cumplimiento tienen la función de evaluar periódicamente el sistema y adoptar las medidas para corregir sus defectos, la circular básica jurídica atribuye a otros órganos de control interno de la entidad la responsabilidad de reforzar la supervisión del cumplimiento y funcionamiento del SARLA/FT. La normatividad vigente establece que es deber de la revisoría fiscal y de la auditoría interna efectuar evaluaciones periódicas del sistema, en orden a identificar sus fallas y debilidades.

En el caso del revisor fiscal, éste debe elaborar como mínimo un informe trimestral dirigido a la junta directiva, en el cual indique y explique las conclusiones obtenidas luego de evaluar el cumplimiento de las normas, códigos y manuales que integran el SARLA/FT⁽³¹⁾. Así mismo debe-

(Cont. nota 30)

quienes concurran los supuestos previstos en el numeral 5º del mismo precepto, modificado por el artículo 8º de la Ley 795 de 2003 (...).

“Así las cosas, aunque no exista un régimen específico de inhabilidades e incompatibilidades aplicable a los funcionarios que se desempeñen como *oficiales de cumplimiento* en las instituciones vigiladas por la Superintendencia Financiera de Colombia, se estima que no por ello escapan de la observancia de la normativa general prevista para el funcionamiento de las instituciones vigiladas, dispuesta en la norma citada en precedencia”.

(31) Debe recordarse que ya el artículo 207 del Código de Comercio establece que es función del revisor fiscal: “Colaborar con las entidades gubernamentales que ejerzan la inspección y vigilancia de las compañías, y rendirles los informes a que haya lugar o le sean solicitados”. Adicionalmente, en el Concepto 2009017224-003 del 22 de abril de 2009, la Superintendencia sostuvo que “el revisor fiscal tiene acceso a la totalidad de la información de la entidad que audita. Su función la debe adelantar de acuerdo con las técnicas y prácticas

rá poner en conocimiento de la junta directiva, inmediatamente, cualquier irregularidad que llegue en relación con el sistema⁽³²⁾.

La auditoría interna por su parte debe llevar a cabo, como mínimo, una evaluación anual del funcionamiento del sistema, dirigida tanto al oficial de cumplimiento como a la junta directiva. Esta debe valorar el funcionamiento del sistema en todas sus etapas, determinar las deficiencias, sugerir soluciones, evaluar el desempeño de los procesos y metodologías implementadas, revisar los procedimientos y criterios de exoneración de controles frente a clientes, y evaluar los modelos e indicadores cualitativos y/o cuantitativos utilizados por la entidad con base en metodologías de reconocido valor técnico⁽³³⁾.

Es importante señalar que ni el revisor fiscal ni la auditoría interna tienen responsabilidad alguna en las etapas de administración del riesgo del SARLA/FT. Su responsabilidad se contrae a una evaluación de su funcionamiento⁽³⁴⁾.

(Cont. nota 31)

de auditoría generalmente aceptadas”. De manera que ningún funcionario puede alegar la existencia de una reserva para restringir o limitar el acceso del revisor fiscal a cualquier información o documentación de la entidad.

- (32) En relación con las funciones y facultades del revisor fiscal, la Superintendencia expidió la Circular Externa 054 de 2008, incorporada en el Título I Capítulo III de la Circular básica jurídica 007 de 1996, la cual determina en el numeral 4.2 las funciones de ese órgano de control. Ahora bien, en lo que hace a su papel dentro del SARLAFT, el subnumeral 4.2.8 párrafo 5º señala que la revisoría fiscal: “Además, deberá poner oportunamente en conocimiento del representante legal, y cuando sea del caso del oficial de cumplimiento, del Comité de Auditoría y del Auditor Interno, según corresponda, las inconsistencias y fallas detectadas en cada uno de los Sistemas de Administración de Riesgo, así como todo incumplimiento que detecte a las disposiciones que regulan la materia”. Así mismo, el párrafo 2º del numeral 4.2.9 de la circular mencionada establece que: “Para efectos de cumplir en forma adecuada las funciones antes relacionadas, dentro del ámbito de fiscalización del revisor fiscal estarán todas las operaciones, actos y áreas de la entidad, así como todos sus bienes, sin reserva alguna”.
- (33) En Concepto 2009017224-003 del 22 de abril de 2009, la Superintendencia sostuvo que la auditoría interna estaba facultada para realizar pruebas de conocimientos específicos sobre el SARLAFT al *oficial de cumplimiento*, siempre y cuando la entidad la hubiera autorizado expresamente.
- (34) En relación con este tema, en el Concepto 2009017224-003 del 22 de abril de 2009, la Superintendencia explicó lo siguiente: “El papel que el SARLAFT le ha asignado

2.6. Infraestructura tecnológica

En cuanto a los recursos tecnológicos, la entidad debe adquirir herramientas informáticas para el control y monitoreo de las operaciones, tales como equipos (*hardware*), programas (*software*), acceso a redes o bases de datos, etc. Esto significa que las entidades vigiladas deben tener los sistemas informáticos y los recursos tecnológicos necesarios para evitar el riesgo de lavado de activos y financiación del terrorismo.

Las características de los sistemas y demás recursos tecnológicos dependen de las actividades, operaciones, tamaño y nivel de exposición al riesgo de cada entidad. La circular básica jurídica no determina expresamente qué sistema, qué equipos o qué *software* deben tener las entidades vigiladas. La ley ha dejado que cada entidad defina con qué recursos tecnológicos contará para aplicar su SARLA/FT. Cuanto mayor sea su tamaño, seguramente serán mayores los requerimientos de control y supervisión del riesgo.

No obstante lo anterior, la normatividad vigente sí determina que las entidades vigiladas deben adquirir un soporte tecnológico que les permita, como mínimo: 1. Llevar a cabo la captura oportuna de la información y su permanente actualización. 2. Consolidar las operaciones de los distintos factores de riesgo conforme a los criterios definidos por la entidad. 3. Centralizar los registros correspondientes a cada factor de riesgo y a cada uno de los clientes. 4. Generar de forma automática los reportes que se requieran para el control de las operaciones.

(Cont. nota 34)

a los órganos de control es el de evaluar el cumplimiento que la entidad le ha dado al mismo. Su función es la de pronunciarse, en el caso de la revisoría fiscal, sobre el cumplimiento de las normas e instructivos del sistema; en el caso de los auditores su pronunciamiento debe versar sobre la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del mismo. En relación con los reportes de operaciones sospechosas, evaluarán si la entidad ha diseñado e implementado de acuerdo con las normas y sus propias políticas y procedimientos lo relacionado con la determinación y reporte de operaciones sospechosas. Los órganos de control están facultados para pedir los soportes de las operaciones que hayan sido seleccionadas como objeto de evaluación de acuerdo con las técnicas de auditoría aplicables. Normas sobre la información que está sujeta a reserva, cuál debe ser reportada y/o suministrada y a quién, y quiénes deben guardar reserva sobre tal información”.

Aun cuando ninguna agencia gubernamental ha impartido instrucciones acerca de qué tipo de soporte deben tener las entidades vigiladas, en la actualidad la UIAF ofrece a través de su página web la posibilidad de obtener de manera gratuita acceso a un programa informático que facilita la elaboración de los reportes de operaciones sospechosas. Se trata del *software ROS Stand Alone*, el cual está diseñado específicamente para el *reporte de operaciones sospechosas* por parte de los sujetos obligados, y puede ser descargado gratuitamente desde la página web de la UIAF⁽³⁵⁾.

2.7. Divulgación de información

Las entidades vigiladas están obligadas a adoptar sistemas que permitan la producción oportuna y eficiente de reportes, acerca del resultado de la aplicación de los mecanismos de prevención del lavado de activos y financiación del terrorismo en cada una de sus diferentes etapas. El propósito de esta obligación es garantizar que las entidades vigiladas puedan suministrar rápidamente a las autoridades, la información que ellas requieran en el curso de sus investigaciones. De igual manera, esta obligación también busca que las entidades vigiladas produzcan información que pueda ser conocida por el mercado, para que los diferentes intermediarios puedan diseñar sus SARLA/FT o evaluar los existentes a partir de datos actualizados.

En desarrollo de esta obligación, la circular básica jurídica le impone a las entidades vigiladas el deber de producir *reportes internos* (RI) para el uso exclusivo de la entidad correspondiente, y *reportes externos* (RE) para el uso de las autoridades y del mercado.

Entre los reportes internos que cada entidad debe generar, la circular básica jurídica menciona como mínimo los siguientes: el reporte de transacciones inusuales, el reporte de operaciones sospechosas y el reporte del resultado de la etapa de monitoreo del riesgo. Los reportes de transacciones inusuales son aquellos que produce el funcionario que ha detectado

(35) Descargar en <http://www.uiaf.gov.co/index.php?idcategoria=889&uiaf_2008=f88de3cb178328aa37926f25a09340fa>.

que una operación se sale de su rango de normalidad, para que el departamento dé cumplimiento o el funcionario que la entidad designe evalúe si hay razones para pensar que puede ser constitutiva de lavado de activos o financiación del terrorismo. Por su parte, el reporte interno de operaciones sospechosas es aquel en el que se informa a la persona encargada de remitir los reportes a la UIAF, la relación de operaciones que se consideran sospechosas y las razones objetivas que llevaron a tal calificación. Con base en este reporte, la persona competente deberá elaborar el reporte externo de operaciones sospechosas dirigido a la UIAF⁽³⁶⁾. Finalmente, el reporte del resultado de la etapa de monitoreo es el informe que las entidades deben elaborar como mínimo trimestralmente, para estimar el perfil de riesgo residual al que están expuestas. Este informe es importante porque no sólo ofrece elementos de juicio acerca del desempeño global del SARLA/FT, sino porque permite a la junta directiva y demás órganos de administración adoptar los correctivos necesarios para mejorar el funcionamiento del sistema.

Por otra parte, las entidades vigiladas también están obligadas a elaborar los siguientes reportes externos: el reporte de operaciones sospechosas⁽³⁷⁾,

(36) En materia de reporte de operaciones sospechosas, la Superintendencia Bancaria (hoy Superintendencia Financiera) sostuvo en Concepto 2003044819-1 del 15 de septiembre de 2003, lo siguiente: “En tal sentido, es del resorte de cada entidad establecer dentro de sus manuales internos, orientados bajo principios de armonía, eficiencia y coordinación, a cargo de quién está la obligación de enviar el reporte, previa la información remitida por los diferentes funcionarios de la institución a fin de que haya una gestión proactiva en materia de prevención de lavado de activos, sin que sea dable a esta Agencia Gubernamental determinar a cargo de quien está dicha responsabilidad. Lo anterior, sin perjuicio del cumplimiento de la instrucción de este organismo en torno al nombramiento del *oficial de cumplimiento* quien debe velar porque se observen las normas referentes al lavado de activos”.

(37) En Concepto 2005049770-004 del 27 de febrero de 2006, la Superintendencia Financiera explicó la importancia del reporte de operaciones sospechosas en los siguientes términos: “Así las cosas, el Reporte de Operación Sospechosa, en adelante (ROS), constituye uno de los mecanismos más significativos en todo el sistema de prevención y control de lavado de activos, por cuanto su detección, complementado con el oportuno suministro de pruebas, permite la acertada administración de justicia.

Por ello, ha ocupado la atención de la comunidad internacional, teniendo como ejemplo la emisión de diversos documentos y regulaciones en la materia, tales

el reporte de transacciones en efectivo⁽³⁸⁾, el reporte de clientes exonerados del reporte de operaciones en efectivo, el reporte sobre operaciones de transferencia, remesa, compra y venta de divisas⁽³⁹⁾, el reporte de informa-

(Cont. nota 37)

como la Convención de Viena, la Declaración de Basilea, las 40 Recomendaciones del Grupo de Acción Financiera Internacional (GAFI), la Convención de las Naciones Unidas contra el Crimen Transnacional Organizado (Convención de Palermo) y en el reglamento Modelo de la OEA-CICAD.

A la luz de tales documentos y regulaciones, el ROS, de conformidad con el artículo 105 del EOSF, desarrollado por el numeral 2.3.1.4. del Capítulo Décimo Primero, Título Primero de la varias veces citada Circular 007, goza en nuestro medio de características especiales como es el hecho de que no constituye una denuncia de carácter penal y es absolutamente confidencial. Así mismo, el envío de ROS a las autoridades exoneran a las entidades vigiladas de responsabilidades administrativas y penales que pudieran derivarse de dichas operaciones”.

- (38) Es sumamente importante tener en cuenta lo aclarado en el Concepto 2003044819-1 del 15 de septiembre de 2003, en el cual la Superintendencia Bancaria (Hoy Superintendencia Financiera) explicó que: “Sobre el particular cabe precisar que ni a la fecha objeto de investigación ni en este momento se puede asimilar el reporte de operaciones sospechosas con el reporte de transacciones en efectivo, toda vez que, aunque las dos son mecanismos para prevenir el lavado de activos, obedecen a obligaciones y conceptos diferentes”.
- (39) En Concepto 2005004064-001 del 14 de septiembre de 2005, la superintendencia Bancaria (hoy Superintendencia Financiera) aclaró que: “Al respecto, es pertinente resaltar que, tal como lo señala la Circular Externa 040 de 2004, la finalidad de la Circular y, por ende, del reporte adoptado radica en la necesidad de evolucionar en los sistemas de prevención de las entidades y de los mecanismos de recaudo de información que confieran más eficiencia en la investigación y represión del lavado de activos. Por ello, en su numeral 2 se destaca el propósito de fortalecer ‘la detección de prácticas asociadas con el lavado de activos en las operaciones de transferencia, remesa, compra y venta de divisas’. Conforme lo ha sostenido esta Superintendencia sólo debe suministrarse la información de las transacciones en comento que son realizadas por las entidades en su calidad de intermediarios del mercado cambiario (IMC), de acuerdo con los conceptos previstos en el instructivo adoptado.

Tal precisión, que pareciera obvia, es fundamental para entender cuáles transacciones deben ser reportadas. En efecto, si bien los IMC pueden realizar las operaciones de cambio contempladas en el Estatuto Cambiario (Res. Externa 8 de 2000 de la Junta Directiva del Banco de la República), la Dirección de Regulación de esta Superintendencia ha precisado que el propósito del instructivo es recaudar y transmitir a la UIAF única y exclusivamente información de los movimientos de divisas efectuados en virtud de las operaciones de transferencias, remesas o compras y ventas por ventanilla, conclusión que se comparte por esta

(Cont. nota 39)

ción sobre transacciones realizadas en Colombia con tarjetas crédito o débito expedidas en el exterior, el reporte sobre productos ofrecidos por las entidades vigiladas y el reporte de los almacenes generales de depósito a otras autoridades. Haciendo abstracción del contenido y especificidades de cada uno de estos reportes, lo importante es que todos ellos son informes que las entidades vigiladas deben remitir a la UIAF o a otras autoridades competentes en materia de prevención del lavado de activos y financiación del terrorismo. Para efectos de realizar estos reportes externos, las diferentes agencias gubernamentales han desarrollado instructivos, formularios, y cuadros de criterios para la evaluación de la calidad de estos⁽⁴⁰⁾.

Subdirección. Ahora, si con ocasión de la realización de otras operaciones de cambio se efectúan transferencias, remesas o compra y venta de divisas, será imperativo suministrar la información correspondiente.

De tal forma, por ejemplo, si un IMC otorga a un residente en el exterior una financiación en moneda extranjera (art 59, lit. f, Res. Externa 8), dicha operación, por sí sola, no genera un reporte. No obstante, es claro, según las instrucciones impartidas, que los movimientos de divisas originados en dicha operación (por ej., transferencias) sí deben ser reportados.

En este orden de ideas, reiteramos que las transacciones que se reportan a la UIAF son aquellas que generan un movimiento de divisas en desarrollo de las operaciones que realizan los intermediarios del mercado cambiario (IMC), denominadas transferencia, remesas y compra y venta por ventanilla.

Ahora bien, en tratándose de aquellas operaciones que no se realizan en calidad de intermediario del mercado cambiario pero que llevan implícitas un movimiento de divisas (transferencia, remesas y compra y venta de divisas por ventanilla), tales como las descritas en los numerales 1) y 6) de su consulta no requerirán del reporte anotado. Dicho de otro modo, los movimientos de transferencia, remesas y compra y venta de divisas que se originen en operaciones e inversiones realizadas directamente por la entidad financiera con sus propios recursos y no por cuenta de terceros en calidad de intermediario no son susceptibles de ser reportadas a la UIAF en los términos de la Circular Externa 040 del 2004.

Lo anterior en la medida en que es claro el origen de los dineros de las operaciones que realiza la entidad por cuenta propia, mientras que en aquellas operaciones en que el intermediario es utilizado por un tercero para movilizar sus divisas no se conoce el origen de los mismos; de ahí que sea necesaria la remisión de la información a la UIAF, en los términos de la Circular Externa 040 del 2004, a fin de evitar que los intermediarios de cambio sean utilizados como instrumentos de prácticas asociadas con el lavado de activos, delimitando para el efecto el universo reportable”.

(40) En Concepto 2009017224-003 del 22 de abril de 2009, la Superintendencia Financiera sostuvo que: “Las entidades sometidas a la vigilancia de esta Su-

(Cont. nota 40)

perintendencia sólo deben realizar los reportes contemplados en los numerales

En el caso de la UIAF, por ejemplo, este organismo ha realizado estudios comparativos entre diferentes períodos, para evaluar el comportamiento de los diferentes reportes externos remitidos por las entidades vigiladas. Estos estudios buscan determinar la calidad de los reportes, con miras a mejorar los procedimientos de remisión y procesamiento de la información remitida⁽⁴¹⁾. En la actualidad, se han implementado plataformas tecnológicas para hacer posible el envío de los reportes de operaciones sospechosas a través de Internet, para facilitar la actividad de las entidades vigiladas⁽⁴²⁾.

4.2.7.2.1 a 4.2.7.2.7 del Capítulo 11 citado, ya discriminadas en el punto de reportes correspondiente al desarrollo de la respuesta a la pregunta 2. Debe señalarse que ninguno de tales reportes se denomina ‘Reporte de operaciones consolidadas’.

“Finalmente, de la simple lectura de los numerales citados se desprende que todos los reportes tienen un instructivo y una proforma que señalan claramente qué información debe contener cada uno de ellos”.

- (41) La Unidad de Información y Análisis Financiero ha producido un documento titulado “Instrumento de calificación de reporte de operaciones sospechosas” (versión mayo de 2005), publicado institucionalmente por esa entidad, el cual ofrece los criterios que deben tenerse en cuenta para evaluar la calidad de los reportes remitidos por las entidades vigiladas. Dicho documento está disponible en la página web de la UIAF en la dirección http://www.uiaf.gov.co/index.php?idcategoria=316&download=Y&uiaf_2008=f88de3cb178328aa37926f25a09340fa (consultado el día 16 de septiembre de 2009).
- (42) En relación con los procedimientos, características y plazos para realizar los reportes de operaciones sospechosas, puede consultarse el documento titulado “Guía de Reporte y Control” (versión 2009) publicado de manera institucional por la UIAF. Este documento puede descargarse en la dirección http://www.uiaf.gov.co/index.php?idcategoria=2516&uiaf_2008=f88de3cb178328aa37926f25a09340fa# (consultada el día 16 de septiembre de 2009). Adicionalmente, es importante mencionar que mediante el Oficio número 29020 enviado al señor Superintendente Financiero de Colombia, la UIAF informó que partir del 1º de marzo de 2009 todas las entidades vigiladas por dicha superintendencia deberán reportar por medio del sistema de reporte en línea.

CAPÍTULO 4

Características y alcances de la Lista Clinton

Uno de los temas que más controversia suscita en nuestro medio tiene que ver con los efectos que provoca en Colombia la inclusión de una persona en la *Office of Foreign Assets Control's SDN List* (“Lista OFAC”, también conocida como “Lista Clinton”), y los riesgos potenciales que pueden surgir para quienes efectúen operaciones comerciales con quienes se encuentran en ella.

Sobre el particular, se aclara que la Orden Ejecutiva 12978 dictada por el presidente de Estados Unidos constituye una decisión soberana adoptada por un gobierno extranjero, cuyo ámbito de validez se encuentra reducido a los ciudadanos y sociedades estadounidenses. El propósito de esta normativa es suministrar la información necesaria para evitar el establecimiento de relaciones jurídico-comerciales con personas extranjeras de quienes se sospecha, pueden estar involucradas en la ejecución de conductas calificadas como crímenes que atentan contra la seguridad de Estados Unidos de América. Dada esta circunstancia, esta orden no es válida como legislación directamente aplicable en nuestro derecho interno, ni existe mecanismo coercitivo alguno que obligue a un nacional colombiano –ya se trate de persona natural o jurídica, o de sucursales nacionales de personas jurídicas extranjeras– a abstenerse de establecer relaciones jurídico-comerciales con sujetos incluidos en la Lista OFAC.

No obstante, el contenido de esta lista tiene profundos efectos y riesgos de reputación comercial y de exposición en el ámbito interno para las personas que mantienen vínculos comerciales con ciudadanos o sociedades estadounidenses. Si un nacional o una sociedad colombiana, a partir del conocimiento que tiene de la inclusión de una persona en la lista de la OFAC, lleva a cabo operaciones comerciales con dicho individuo, corren

el riesgo de que la *Treasury's Office of Foreign Asset Control* también los incluya en la lista, al asumir que estos pueden estar contribuyendo a la realización del presunto crimen por el que fue originalmente incluido el primer individuo.

Aun cuando la realización de una operación comercial con una persona incluida en la Lista OFAC no constituye una circunstancia que pueda dar pie al inicio de acciones judiciales o a la imposición de sanciones por ese hecho, lo cierto es que esta genera doble riesgo: por un lado jurídico, ya que las personas incluidas en esa lista se consideran sospechosas de haber incurrido en conductas calificadas como crímenes por la ley penal federal estadounidense, de manera que al llevar a cabo operaciones con ellas se corre el peligro de estar contribuyendo al perfeccionamiento de ese tipo de conductas; y por otro, comercial, pues al efectuar operaciones con dichas personas se corre el peligro de ser también incluido en la lista OFAC, con las consecuencias que ello supone en cuanto al ejercicio de las relaciones comerciales con ciudadanos estadounidenses.

Los efectos que se generan en Colombia por la inclusión de una persona en la lista OFAC han sido fijados por la Corte Constitucional para el ámbito de la actividad financiera, bursátil y aseguradora, a partir de argumentos jurídicos que bien pueden extenderse a otros ámbitos de la actividad económica, y que actualmente se consideran criterios orientadores de buenas prácticas comerciales y de buen gobierno corporativo. En efecto, al resolver diversas acciones de tutela originadas en el bloqueo financiero a personas incluidas en la Lista OFAC, la Corte Constitucional colombiana ha sostenido que el ejercicio de la actividad financiera es de “*alto riesgo social*”, en atención a la necesidad que existe de preservar la confianza del público en el sistema y en su servicio, tal como se desprende del artículo 35 de la Ley 510 de 1999. Por tal motivo y, sin perjuicio del principio de universalidad del ahorro, las entidades vigiladas pueden rehusarse a aceptar una persona como cliente, siempre que dicha decisión obedezca “a criterios objetivos y razonables que impliquen un riesgo para la solvencia y/o estabilidad patrimonial de las entidades financieras”⁽¹⁾, y no a causas de discriminación o a la imposición de barreras irrazonables para

(1) Corte Constitucional, Sentencia T-468 de junio 5 de 2003.

la prestación de algún servicio financiero⁽²⁾. En resumen, la jurisprudencia de la Corte Constitucional respalda la posibilidad de que las entidades vigiladas impidan a ciertos usuarios del sistema financiero el acceso a sus servicios, siempre que éste no resulte *injustificado*⁽³⁾.

-
- (2) En el Concepto 2005049770-004 del 27 de febrero de 2006, reiterado en el 2009006724-001 del 6 de marzo de 2009, la Superintendencia Financiera explicó que por regla general, la actividad financiera se rige por los principios de autonomía de la voluntad privada, autonomía negocial y libertad contractual, de tal manera que las entidades vigiladas tienen en principio el derecho a escoger con quien celebran contratos para la prestación de servicios financieros. No obstante, esta libertad negocial no es absoluta ya que la intermediación financiera es una actividad de interés público, y por esta razón el acceso al sistema financiero debe ser garantizado por el Estado. Debido a esta circunstancia, las entidades financieras sólo pueden rehusarse a prestar sus servicios a un particular, cuando existan motivos realmente objetivos y razonables que justifiquen su negativa. De tal suerte que el deber de conocimiento del cliente y la segmentación del mercado exigido como parte del SARLA/FT no puede ser utilizado, como pretexto para discriminar injustificadamente a un individuo y negarle el acceso al sistema financiero. Además, ya en la Circular Externa 023 de 2005, la Superintendencia explicó que: “Si bien corresponde a las entidades vigiladas definir los segmentos de mercado en los cuales desarrollan su actividad, una vez definidos éstos, el acceso a los servicios que prestan no puede ser discriminatorio, desigual, negado o suspendido injustificadamente (...). De tal forma, cuando la prestación de un servicio no sea impuesta obligatoriamente por su régimen respectivo, la negativa para suministrarlo o su terminación unilateral debe basarse, estrictamente, en la evaluación de las condiciones y los riesgos inherentes a las operaciones que se realizan o se realizarían con cada consumidor, de forma tal que la abstención de prestarlos esté plenamente justificada en criterios objetivos y razonables que deben ponerse en conocimiento del consumidor cuando lo solicite”.
- (3) Ver Corte Constitucional, Sentencia SU-157 de 1999, M.P. Alejandro Martínez Caballero. En esta sentencia, la Corte Constitucional sostiene que existe *bloqueo financiero* injustificado en los siguientes casos:
- “b.1. Cuando al cliente le es imposible actuar de manera efectiva para neutralizar los efectos de las decisiones de los bancos. Por lo tanto, no constituye una situación de bloqueo financiero si existen medios administrativos o jurídicos que le permitan acceder al sistema financiero.
- “b.2. También se presenta el bloqueo financiero cuando el usuario está frente a la imposibilidad de ingreso al sistema público bancario.
- “b.3. Cuando la decisión de las entidades financieras produce consecuencias graves para la capacidad jurídica del usuario del servicio público.
- “b.4. Cuando la negativa de negociación no responde a causas objetivas y razonables que justifican la decisión”.

En relación con el alcance de la justificación que se requiere para que la restricción al acceso a los servicios financieros sea legal, la Corte Constitucional sostiene que el derecho de las personas a obtener la prestación de dichos servicios por intermedio de las entidades vigiladas: “Se encuentra limitado por el cumplimiento de las obligaciones previstas por el legislador, dentro de las cuales la Ley 35 de 1993, señala las siguientes, a saber: (i) la capacidad de pago del solicitante, y (ii) *el riesgo de la operación*”⁽⁴⁾. Esto significa que existen claros eventos en los cuales una entidad financiera puede rehusarse a prestar sus servicios a determinada persona, por constituir un “riesgo latente” la operación⁽⁵⁾. Este es el caso de los inclui-

-
- (4) Corte Constitucional, Sentencia T-468 de junio 5 del 2003, M.P. Rodrigo Escobar Gil.
- (5) En la Sentencia T-468/03, M.P. Rodrigo Escobar Gil, la Corte Constitucional señaló que la actividad financiera está sometida a cuatro categorías de riesgo a saber:
- “a) *Riesgos de reputación*: consistentes en la publicidad negativa que puede afectar la confianza de los depositantes, como resultado de la ejecución de prácticas anormales o de la utilización de las entidades financieras como medios para la realización de actividades ilegales por parte de sus clientes.
- “b) *Riesgos operativos*: relacionados con la violación a los procedimientos de control y de debida diligencia previstos en la ley y desarrollados por las autoridades de control, los cuales pueden involucrar una afectación o alteración al ejercicio corriente de sus operaciones financieras activas, pasivas o neutras.
- “c) *Riesgos legales*: aquellos vinculados con las posibles multas, responsabilidades penales y sanciones administrativas impuestas por las autoridades de control, como consecuencia de la ausencia de la debida diligencia en el momento de identificar clientes y en la prestación corriente de sus servicios.
- “d) *Riesgos de concentración*: destinados a controlar la concentración indebida del crédito, es decir, tienen como propósito evitar la violación a los cupos individuales de crédito o su asignación a un prestatario único o a un grupo de prestatarios relacionados. Su fundamento constitucional se encuentra en la obligación de democratizar el crédito, de conformidad con el artículo 335 Superior. “En Colombia, el control a los citados riesgos se encuentra regulado en: (i) el Estatuto Orgánico del Sistema Financiero; (ii) la Circular Externa 046 de 2002 de la Superintendencia Bancaria y 022 de abril 19 del 2007 de la Superintendencia Financiera; (iii) la Ley 526 de 1999, y (iv) el Decreto 1497 de 2002. “En dichas disposiciones se plasman normas relacionadas con el conocimiento del cliente, la determinación de los parámetros para evaluar los movimientos de los usuarios y, en general, el conocimiento del mercado, con el objeto de detectar las operaciones inusuales o sospechosas que puedan configurar la práctica o realización de una conducta delictiva”.

(Cont. nota 5)

dos en la lista de la OFAC, en cuyo caso al permitirles la vinculación a la entidad como clientes se compromete la confianza pública en el sistema financiero y se pone en riesgo la estabilidad de la propia entidad. Precisamente, la Corte Constitucional ha sostenido que para evitar que una persona sea excluida injustificadamente de la utilización de los “servicios financieros”, debe acudirse –entre otros– a mecanismos de “control para el acceso” como los señalados por el Comité de Supervisión Bancaria de Basilea, que obligan al conocimiento del cliente y de su actividad económica.

De conformidad con la doctrina anterior, cuando en desarrollo de obligatorias regulaciones normativas y de sus propias políticas internas en materia de prevención y detección de eventuales operaciones de lavado, una entidad resuelve negar la prestación de servicios a personas naturales o jurídicas incluidas en la lista de la OFAC, está excluyendo de su servicio de manera justificada a clientes en relación con los cuales se advierte una causal objetiva y razonable que avala tal decisión, previo el análisis concreto y específico de cada caso⁽⁶⁾. Con ello se protege a la entidad de un riesgo la-

La Corte sostuvo en esa misma providencia, que las entidades vigiladas están legalmente obligadas a mitigar esos riesgos a los que se encuentra expuesta la actividad financiera, y en ese orden de ideas es legítimo negar la prestación de servicios a una persona cuando con ello se contribuye a reducir o evitar los riesgos mencionados.

- (6) La Corte Constitucional manifestó en la Sentencia SU-157 del 10 de marzo de 1999, M.P. Alejandro Martínez Caballero, que la inclusión de una persona en la “lista Clinton” sí es una causal objetiva válida que justifica que una entidad financiera colombiana se abstenga de realizar operaciones o negocios con dicha persona. Textualmente sostuvo ese tribunal: “La banca colombiana considera que la Lista Clinton sí es una causal objetiva que aprueba su decisión, como quiera que el riesgo bancario derivado de la relación comercial con los peticionarios es muy alto, puesto que Estados Unidos sanciona a los norteamericanos que negocian con quienes figuran en la lista. Por ende, si la entidad bancaria colombiana desea mantener relaciones comerciales con personas de esa nacionalidad, no debe ofrecer sus servicios a los presuntos ‘traficantes de narcóticos’.

“La Corte resalta que, en efecto, la mayoría de las entidades financieras colombianas mantienen relaciones comerciales muy importantes con la banca norteamericana, por lo que las medidas adoptadas en nuestro país se dirigen a proteger a las instituciones financieras colombianas de riesgos inminentes propiciados por la fuerte capacidad de intimidación que tiene la banca norteamericana sobre el mercado financiero colombiano. En consecuencia, los efectos ‘reflejo’ (Cont. nota 6)

de la Lista Clinton producen un estado de indefensión indudable para la banca

tente de operación, y se preserva su estabilidad y la del sector. Al respecto la Corte Constitucional sostiene:

“A juicio de esta Corporación, el solo hecho de que una persona figure en la Lista Clinton, sin que haya sido condenada o esté siendo investigada por delitos relacionados con el narcotráfico en Colombia, es una causal objetiva que autoriza la imposibilidad de acceder al sistema financiero, en razón de las graves consecuencias económicas que se producirían en dicho sector y, además, en aras de garantizar el interés general de los ahorradores del sistema bancario”⁽⁷⁾.

Ahora bien, es claro que la Orden Ejecutiva 12978 o Lista Clinton no constituye una decisión administrativa que vincule a las autoridades colombianas o que pueda ser coercitivamente aplicable por ellas. Sin embargo, su incumplimiento a partir del conocimiento que tenga la entidad de la inclusión de una persona en la misma, acarrearía severas consecuencias económicas para las entidades vigiladas por la Superintendencia Financiera⁽⁸⁾. Este aspecto también ha sido reconocido por la Corte Constitucional cuando señala:

colombiana, por lo que se considera que ella debe defender el interés general de los ahorradores. Así las cosas, tal y como se plantean en la actualidad los hechos, la negociación con quienes aparecen en la Lista Clinton podría propiciar un desequilibrio económico desproporcionado para el sistema financiero colombiano, el cual no puede ser controlado por las autoridades de este país (...”).

- (7) Corte Constitucional, Sentencia T-468/03, M.P. Rodrigo Escobar Gil. En esa misma sentencia, la Corte Constitucional reiteró que “(...) la Lista Clinton debe considerarse como un elemento de valoración probatoria que puede ser tenido en cuenta por las instituciones financieras al momento de evaluar el acceso de los particulares a la prestación de los servicios financieros. Máxime si dichas instituciones están directamente comprometidas a nivel nacional e internacional en las políticas de control y erradicación al lavado de activos”.
- (8) En Concepto 2004006247-1 del 2 de abril de 2004 (reiterado en el 2004053989-2 del 15 de octubre de 2004 y en el 2004066219-4 del 21 de diciembre de 2004), la Superintendencia Bancaria (hoy Superintendencia Financiera) sostuvo que: “Los riesgos y consecuencias por contratar con personas incluidas en la llamada ‘Lista Clinton’ deben ser evaluados por las entidades financieras ya que la orden ejecutiva emanada del Departamento del Tesoro de Estados Unidos de América no tiene efectos vinculantes en el estado colombiano (...). Por ello, dicha lista sólo puede ser aplicada por los bancos en virtud de la libertad contractual y de asociación y no porque haya sido adoptada por nuestra legislación como norma”.

“...Sin embargo, para la Corte es claro que las consecuencias de su incumplimiento (de la orden ejecutiva) por parte de la banca nacional, dadas las relaciones comerciales ineludibles que ésta mantiene con la banca norteamericana, puede acarrear una grave alteración de la solidez del mercado financiero colombiano, por lo cual la decisión de las instituciones financieras de negar el acceso a este sistema de la(s) persona(s) que aparezcan incluidas en la Lista Clinton, constituye en realidad una casual objetiva justificada.

“Dentro de éste contexto, en aplicación a las políticas de prevención de lavado de activos a que hace referencia la Ley 526 de 1999, el Decreto 1497 de 2002 y la Circular Externa 046 de 2002, la Lista Clinton debe considerarse como un elemento de valoración probatoria que puede ser tendido en cuenta por las instituciones financieras al momento de evaluar el acceso de los particulares a la prestación de los servicios financieros. Máxime si dichas instituciones están directamente comprometidas a nivel nacional e internacional en las políticas de control y erradicación del lavado de activos”⁽⁹⁾.

Por otra parte, es importante reiterar que los criterios anteriores pueden extenderse en lo pertinente a otros ámbitos del circuito económico. Si una persona dedicada a actividades distintas a la financiera, cambiaria, bursátil o aseguradora realiza operaciones comerciales directas o indirectas con personas vinculadas a la lista OFAC, incurre en una operación que genera un riesgo latente de reputación derivado no solo de la publicidad negativa que llevaría a afectar la confianza pública, sino además en una práctica que podría conducir a la pérdida de sus inversiones en ese país y al compromiso de su propia estabilidad patrimonial. Además, incurría en un riesgo operativo por violentar procedimientos de control establecidos universalmente como instrumentos de prevención del lavado de activos, y en falta a la debida diligencia que le es exigible a los administradores. Valga recordar que de conformidad con lo dispuesto por el artículo 23 de la Ley 222 de 1995, los administradores deben obrar con absoluta buena fe comercial y con la diligencia del buen hombre de negocios, desarrollando su gestión, tomando en consideración los intereses de la sociedad

(9) Corte Constitucional, Sentencia T-468/03, M.P. Rodrigo Escobar Gil.

y de sus asociados.

Teniendo en cuenta lo anterior, cuando una persona natural o jurídica es incluida en la lista OFAC, todos los actores económicos nacionales deben evitar el “riesgo de contagio” mediante la adopción de mecanismos jurídicos necesarios para evitar los perjuicios que puede causar el mantenimiento de vínculos comerciales con ellas. Por esta razón, las empresas no vinculadas al sector financiero, cambiario, bursátil o asegurador también se encuentran legitimadas para adoptar como política interna la no realización de negocios con personas vinculadas a la lista OFAC, efecto para el cual la ley colombina autoriza hacer uso del derecho a la libertad y autonomía contractual. Es decir, toda vez que realizar operaciones con personas incluidas en la Lista OFAC impone a las empresas graves riesgos, estas se encuentran autorizadas para ejercer su autonomía contractual, y con fundamento en esa libertad cesar en el perfeccionamiento de negocios jurídicos con el propósito de asegurar el interés general de sus accionistas, usuarios y en general el de su propia estabilidad.

En conclusión, impedir la celebración, continuación o perfeccionamiento de negocios con personas incluidas en la Lista Clinton no constituye un rechazo o práctica desproporcionada ni irrazonable, como tampoco discriminatoria. Por el contrario, protege la solidez y solvencia moral y patrimonial de las entidades, garantiza la confianza del público en las mismas y estimula la adopción de sanas prácticas de buen gobierno corporativo, cuya aplicación constituye un deber del buen administrador.

CAPÍTULO 5

La prevención del lavado de activos en el sector real

La política de prevención del lavado de activos en Colombia ha estado tradicionalmente enfocada en el sector financiero, por considerar que es el más expuesto a este riesgo. Esto ha llevado a que la legislación y la doctrina existentes en esta materia se hayan desarrollado especialmente para ese sector. Asimismo, el conocimiento y la experiencia adquirida, no solo por las entidades de este sector sino también por el órgano de supervisión (Superintendencia Financiera), han hecho que los sistemas de administración del riesgo de lavado de activos y financiación del terrorismo sean cada vez más eficientes y eficaces.

Las organizaciones criminales tienen una gran capacidad para adaptarse a las condiciones de seguridad que imponga el Gobierno Nacional, y son conscientes de la fortaleza desarrollada por el sector financiero para prevenir el lavado de activos. Por esta razón, han buscado otros sectores de la economía más vulnerables para ocultar, manejar, invertir y aprovechar los recursos derivados de sus actividades delictivas. Específicamente, las organizaciones criminales han buscado la forma de lavar sus activos en el sector real de la economía, por cuanto los agentes que participan en ese sector no solo no tienen sistemas de prevención o de administración del riesgo de lavado de activos, sino que tampoco tienen el conocimiento, la experiencia y la sensibilidad necesarias para detectar y prevenir las operaciones de lavado de activos que ejecuta el crimen organizado.

En efecto, salvo contadas excepciones, los empresarios e industriales del país no estaban hasta ahora obligados a implementar sistemas de prevención o de administración del riesgo de lavado de activos y de financiación del terrorismo, porque se pensaba que este era un problema pro-

pio del sector financiero. No obstante, la obligación de implementar este tipo de sistemas en el sector real viene expandiéndose tímidamente desde hace unos años, exclusivamente a aquellas industrias en las cuales se habían detectado peligrosas tipologías de lavado de activos: la industria del transporte de carga; la de juegos, suerte y azar; la del transporte de valores; la de los giros postales; la del blindaje de vehículos; la de los equipos de fútbol, etc.

Lista de sectores obligados hasta enero de 2014		
Entidad supervisora	Normatividad	Subsector
Superintendencia Financiera de Colombia	Capítulo XI de la Circular Externa 026 de 2008 de la Superintendencia Financiera de Colombia: instrucciones relativas a la administración del riesgo de lavado de activos y de la financiación del terrorismo – SARLAFT Circular Externa 003 de 2009 de la Superintendencia Financiera de Colombia: modificación del medio de envío de los formatos e instructivos relacionados con el reporte de información a la Unidad Administrativa Especial de Información y Análisis Financiero – UIAF	Sociedades corredoras de seguros; organismos financieros del exterior; fondos mutuos de inversión vigilados; comisionistas de bolsas de valores; sociedades fiduciarias; sociedades comisionistas de bolsas agropecuarias; compañías de financiamiento comercial; compañías de seguros generales; establecimientos bancarios; compañías de seguros de vida; instituciones oficiales especiales; emisores no vigilados por la SFC (emisores reales y de servicios públicos); reaseguradoras del exterior; entidades cooperativas de carácter financiero; sociedades administradoras de fondos (de pensiones y cesantías); sociedades administradoras de inversión; oficinas de representación en Colombia sin establecimiento comercial; administradoras de sistemas de pago de bajo valor; entidades administradoras del régimen solidario de prima media; almacenes generales de depósito; sociedades de capitalización; corporaciones financieras; sociedades calificadoras de valores; cooperativas de seguros; casas de cambio plenas; organismos cooperativos de grado superior; organismos de autorregulación; bolsas de valores; sociedades administradoras de depósitos centralizados de valores; fondos de garantías; Banco de la República; bolsas agropecuarias; sociedades administradoras de sistemas de negociación y registro de divisa; Cámara de riesgo central de contraparte; sociedades administradoras de sistemas de compensación y liquidación de divisas; titularizadoras

Lista de sectores obligados hasta enero de 2014		
Entidad supervisora	Normatividad	Subsector
Superintendencia de Notariado y Registro	<p>Instrucción Administrativa 08 de 2007 de la Superintendencia de Notariado y Registro: Lavado de Activos y Financiación del Terrorismo.</p> <p>Circular Externa 11 de 2008 de la Superintendencia de Notariado y Registro: reportes a cargo de los Notarios con destino a la Unidad de Información y Análisis Financiero – UIAF</p>	Superintendencia de Notariado y Registro
Superintendencia de Economía Solidaria	<p>Circular Básica Jurídica – Capítulo XI de Circular Externa 007 de 2008 de la Superintendencia de Economía Solidaria: instrucciones para la prevención y el control del lavado de activos y de la financiación del terrorismo en las cooperativas de ahorro y crédito, y multiactivas e integrales con sección de ahorro y crédito – SIPLAFT</p>	<p>Cooperativas de ahorro y crédito</p> <p>Multiactivas e integrales con sección de ahorro y crédito</p> <p>Multiactivas e integrales sin sección de ahorro y crédito</p>
Superintendencia de Puertos y Transporte	Circular Externa 011 de 2011 de la Superintendencia de Puertos y Transporte: Sistema Integral para la Prevención y Control del Lavado de Activos y la Financiación del Terrorismo – SIPLAFT	Empresas transportadoras de vehículos de carga terrestres (transporte de carga)

Lista de sectores obligados hasta enero de 2014		
Entidad supervisora	Normatividad	Subsector
Superintendencia de Sociedades	Circular Externa 100 – 004 de 2009 de la Superintendencia de Sociedades: reportes a cargo de los notarios con destino a la Unidad de Información y Análisis Financiero – UIAF	Comercio de vehículos Metales preciosos Otras actividades
Superintendencia de Vigilancia y Seguridad privadas	Circular Externa 008 de 2011 de la Superintendencia de Vigilancia y Seguridad Privada: Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT	Empresas blindadoras de vehículos Empresas transportadoras de valores
Superintendencia Nacional de Salud	Resoluciones UIAF 141 y 142 de 2006, 022 y 078 de 2007	Bingos Casinos Chances Loterías Gallística Juego novedoso Poliedros Hípico
Ministerio de la Tecnología de la Información y las Comunicaciones	Resolución 2705 de 2010 del MINTIC: Sistema de Administración y Mitigación del Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT. Resolución 1334 de 2012 del MINTIC: obligaciones de reporte a la UIAF –	Operador postal oficial Operadores postales de pago

Lista de sectores obligados hasta enero de 2014		
Entidad supervisora	Normatividad	Subsector
DIAN	Circular Externa 0170 de 2002 de la DIAN: prevención y control al lavado de activos	Empresas de mensajería
	Circular Externa 0170 de 2002 de la DIAN: prevención y control al lavado de activos	Servicios aduaneros, de carga, zonas francas, sociedades portuarias, agencias de carga, depósitos, entre otros
	Circular Externa 028 de 2011 de la DIAN: Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT	Profesionales de compra y venta de divisas
Coldeportes	Ley 1445 de 2011	Fútbol

Como puede observarse en el cuadro, anteriormente estaban obligados a implementar algún sistema de prevención de lavado de activos aquellos empresarios o industriales del sector real que cotizaran acciones en bolsa o que emitieran títulos de deuda negociados en bolsa (por ej., bonos). Sin embargo, esta obligación resultaba de su relación con el mercado de valores y no de la conciencia acerca de la existencia de un riesgo de lavado de activos inherente a su objeto social o al sector de la industria al cual pertenecen.

Aun así, se debe reconocer que han existido en el sector real algunas empresas que voluntariamente han decidido implementar programas o sistemas para la prevención del lavado de activos por razones de política de buen gobierno corporativo. Como es el caso de aquellas multinacionales altamente preocupadas por su reputación, que están dispuestas a asumir cualquier esfuerzo que las aleje del riesgo de terminar haciendo negocios con personas al margen de la ley.

La ausencia de una norma que obligará de manera general a los grandes empresarios e industriales a tomar medidas para prevenir el lavado de activos hacia más vulnerable al sector real de la economía. Dicha vulnera-

bilidad fue aprovechada por la delincuencia organizada para ocultar, manejlar, invertir y aprovechar recursos de origen ilícito; circunstancia que llevó al Gobierno Nacional a emitir, a través de la Superintendencia de Sociedades, una norma que impone a todas las personas jurídicas sometidas a la inspección, vigilancia y control de esa entidad, la obligación de implementar un programa de prevención de lavado de activos y financiación del terrorismo. Se trata de la Circular Externa 304-000001 del 19 de febrero de 2014, modificada por la Circular Externa 100-000005 del 17 de junio de 2014, ambas emitidas por la Superintendencia de Sociedades.

El propósito de la circular es crear el marco regulatorio necesario para que las empresas del sector real diseñen e implementen sistemas de autocontrol y gestión del riesgo de lavado de activos y financiación del terrorismo, así como lo concerniente a reportes de operaciones sospechosas y en efectivo que se deben hacer a la Unidad de Información y Análisis Financiero, UIAF. Esta normatividad va dirigida principalmente a los socios, accionistas y administradores de las sociedades comerciales, sucursales de sociedades extranjeras, de empresas unipersonales vigiladas por la Superintendencia de Sociedades y demás sociedades obligadas a reportar a la (UIAF).

Inicialmente, esta circular dispuso que la adopción de un sistema de autocontrol y gestión del riesgo de lavado de activos y financiación del terrorismo sea obligatoria para las sociedades que obtuvieron ingresos brutos iguales o superiores a 160.000 salarios mínimos legales mensuales vivientes durante el año 2013. Para las demás sociedades, la adopción de este sistema es una recomendación de prudencia, diligencia, buenas prácticas comerciales y buen gobierno corporativo, cuyo acatamiento cobra gran importancia cuando la empresa se ve lamentablemente enfrentada a un asunto judicial (proceso penal o extinción de dominio), relacionado con temas de lavado de activos, pues la diligencia o prudencia con que se comportan los empresarios es un elemento de juicio muy importante para los operadores judiciales (jueces y fiscales), a la hora de valorar la existencia de responsabilidades penales o de otro tipo.

Ahora bien, el sistema de autocontrol y gestión del riesgo de lavado de activos y financiación del terrorismo previsto en esa Circular debe ser implementado teniendo en cuenta los siguientes parámetros:

1. **Diseño y aprobación.** La responsabilidad de diseñar el sistema de autocontrol y gestión recae en el representante legal de la sociedad. En el caso de que haya varios representantes legales, la responsabilidad será del representante legal que administre el área con mayor exposición al riesgo de lavado de activos y financiación del terrorismo. El diseño debe tener en cuenta que el sistema de autocontrol y gestión se ajuste a la empresa; es decir, debe estar diseñado para atender de manera concreta y exacta las necesidades de la compañía, en función de su tamaño, su objeto, su mercado, su clientela, sus productos, sus procesos, su nivel de riesgo, etc.

Para lograr que el sistema de autocontrol y gestión sea a la medida, la sociedad debe realizar previamente un estudio o evaluación del riesgo para detectar las áreas, los procesos y los productos más expuestos al riesgo de lavado de activos y financiación del terrorismo. Para tal efecto, la sociedad debe ejecutar una metodología que cumpla los estándares internacionales generalmente aceptados en materia de medición de riesgos, para asegurar que la conclusión sobre el nivel de riesgo al que está expuesta sea confiable.

Este estudio o evaluación debe suministrar los elementos de juicio necesarios para diseñar el sistema de autocontrol y gestión que más se adapte a las características de la compañía. Por esta razón, los documentos que describen el sistema de autocontrol y gestión deben estar sustentados en las conclusiones del estudio o evaluación del riesgo.

Por supuesto, el diseño del sistema debe procurar no solo que el control y la gestión del riesgo sea eficaz, sino eficiente. Esto quiere decir que al momento de elegir los mecanismos de control y gestión que conformarán el sistema, la persona responsable debe realizar un análisis de costo-beneficio sobre las diferentes alternativas existentes, para evitar que este sea demasiado costoso o que cargue a la organización con procesos que obstruyan o dificulten el normal desarrollo de su actividad.

Debe tenerse en cuenta que entre más robusto sea el sistema, más costoso, extenso y complejo resultará para la compañía. Asimismo se debe considerar que no existe un sistema absolutamente perfecto que

haga a la compañía inmune o impermeable al lavado de activos o a la financiación del terrorismo. Aún los sistemas más avanzados tienen fisuras que permiten la existencia de un riesgo residual. En consecuencia, el diseño del sistema de autocontrol y gestión debe buscar un balance entre el costo, el tamaño y la complejidad del sistema y el nivel de riesgo que la compañía se puede permitir tolerar.

Una vez diseñado el proyecto de sistema de autogestión y control, éste debe ser sometido a la aprobación de la junta directiva o del órgano de administración que haga sus veces, de acuerdo con los estatutos sociales. Dicho órgano podrá hacerle los ajustes o correcciones que estime necesarios, convenientes y oportunos, antes de aprobarlo.

2. **Ejecución.** Una vez aprobado, el sistema de autogestión y control debe ser implementado y puesto en funcionamiento. Esto supone que la sociedad debe realizar ajustes en su organización y funcionamiento, para garantizar que los mecanismos que componen el sistema puedan actuar eficazmente. Estas correcciones comprenden cambios en la estructura organizacional, entre los cuales se destaca la creación de un área, gerencia o departamento de cumplimiento, a cargo de un trabajador responsable del funcionamiento del sistema: el *oficial de cumplimiento*. Asimismo, la organización debe realizar cambios en algunos de sus procesos, subprocesos y procedimientos, para incluir controles que permitan detectar, prevenir y reportar operaciones sospechosas de lavado de activos.

Por tanto, esta implementación exige un esfuerzo económico de parte de la sociedad, cuando quiera que resulte necesario contratar recurso humano, recurso tecnológico y recurso físico. De lo anterior, lo más costoso es el recurso tecnológico por dos razones:

En primer lugar, porque la compañía tiene que adquirir el servicio de acceso a las bases de datos que permite realizar las consultas de personas en las listas restrictivas, para garantizar un conocimiento apropiado de sus clientes, sus proveedores y en general todas aquellas personas con quienes hace negocios de manera permanente o eventual. En segundo lugar, porque en muchos casos es necesario que la empresa realice desarrollos de software o de aplicativos, para introducir en sus sistemas la capacidad de emitir señales de alerta frente a ope-

raciones inusuales. Esto último no solo resulta dispendioso, sino complejo y demorado, por lo que el proceso de implementación del sistema puede ser más largo y difícil que el de diseño.

La persona responsable de este proceso de implementación es el representante legal quien debe mantener enterada a la junta directiva acerca de los avances sobre la materia.

3. **Seguimiento.** Una vez implementado, el sistema de autocontrol y gestión, éste debe ser monitoreado permanentemente, función que corresponde al *oficial de cumplimiento*. Como producto de esa actividad, éste debe emitir informes periódicos, como mínimo semestrales, dirigidos al representante legal y a la junta directiva. Dichos informes deben explicar las fortalezas y debilidades del sistema, así como contener propuestas para su mejoramiento. Por lo menos anualmente, se debe incluir un estudio de medición del riesgo residual de lavado de activos, para determinar si los mecanismos de control implementados son eficaces para mitigar la exposición al riesgo inherente de la empresa.

Los informes preparados por el *oficial de cumplimiento* deben ser leídos cuidadosamente por el representante legal y por los miembros de la junta directiva para ordenar los cambios o ajustes que sean necesarios en orden a garantizar el mejoramiento continuo del sistema de autogestión y control del riesgo de lavado de activos. En aquellos casos en que la empresa cuenta con un departamento o gerencia de control de calidad, el *oficial de cumplimiento* debe buscar el apoyo de esa área para procurar que los procesos, subproceso y procedimientos que conforman el sistema de autogestión y control sean permanentemente mejorados.

4. **Cumplimiento.** El sistema de autogestión y control debe prever mecanismos que garanticen su cumplimiento. Esto se consigue en la mayoría de los casos, mediante la inclusión de normas que obligan a todos los empleados de la empresa a conocer y acatar las reglas y procedimientos previstos en el manual de prevención de lavado de activos que hace parte del sistema. De igual manera, la junta directiva o el órgano que esté autorizado estatutariamente, pueden emitir una or-

den, circular o directiva en el sentido de disponer que el manual de prevención de lavado de activos haga parte del reglamento de trabajo. De esta manera se consigue que el incumplimiento de las disposiciones del manual de prevención sea considerado asimismo una violación grave al reglamento de trabajo, lo cual daría lugar al despido sin justa causa.

Este tipo de disposiciones se justifica laboralmente por la gravedad de las consecuencias que trae para la sociedad el incumplimiento de las normas en materia de prevención de lavado de activos. Allí debe tenerse en cuenta, que este incumplimiento puede provocar que la sociedad termine involucrada en una actividad de lavado de activos con graves consecuencias desde el punto de vista reputacional, legal, económico y operativo. Incluso, el solo incumplimiento de dichas normas puede acarrear la imposición de sanciones, que van desde multas sucesivas hasta la intervención de la sociedad por parte de la entidad de supervisión. Frente a esto último es importante resaltar, que en algunos sectores como el financiero, la violación de las normas sobre prevención de lavado de activos se considera una práctica insegura y da lugar a la intervención, toma de control y hasta liquidación de la sociedad, por razones de interés público.

5. **Comunicación.** El sistema de autogestión y control debe ser conocido y entendido por cada uno de los empleados de la empresa, en todos los niveles, para que pueda funcionar adecuadamente. Esto supone que la empresa debe hacer un esfuerzo por adquirir e implementar mecanismos que permitan asegurar que los empleados conozcan el sistema, y que sean actualizados permanentemente con las modificaciones que le sean introducidas. Ahora bien, estas actualizaciones también comprenden la información novedosa que surja en relación con el tema de lavado de activos y financiación del terrorismo, como por ejemplo información sobre nuevas tipologías identificadas.

Para efectos de ese conocimiento y actualización, la empresa debe asignar la función de comunicación a algún empleado, quien se responsabilizará de adquirir, capturar, organizar, clasificar, editar y transmitir esa información. La comunicación puede hacerse mediante memorandos, circulares u oficios entregados físicamente a cada em-

pleado, o también utilizando medios electrónicos como el e-mail institucional, la intranet de la empresa o la página web. Lo importante es que la empresa se asegure de que la información llegue efectivamente al personal que labora y, que quede constancia de que cada uno de ellos la recibió, lo que adquiere una particular importancia de cara a un eventual proceso judicial, pues es posible que la empresa deba demostrar su diligencia para prevenir el lavado de activos, y a tal efecto no basta tener el sistema de autogestión y control, sino que se requiere probar que todos los empleados lo conocían y estaban actualizados con las últimas modificaciones.

6. **Capacitación.** El proceso de diseño del sistema de autogestión y control presupone la realización de un estudio organizacional y funcional de la compañía, el cual permite identificar las áreas y los procesos que están más expuestos al riesgo de lavado de activos y financiación del terrorismo. El manual de prevención de lavado de activos debe asignar a esas áreas tareas especiales para mitigar el riesgo, lo cual supone modificar algunos de los procesos de la empresa para introducirle mecanismos de prevención como señales de alerta y control de operaciones.

En atención a lo anterior, la Superintendencia de Sociedades exige que la empresa realice una capacitación para todos los empleados, y especialmente para los funcionarios a cargo de las áreas y procesos más expuestos al riesgo de lavado de activos y financiación del terrorismo. Esta capacitación se debe presentar al menos una vez al año, y debe versar sobre temas y conceptos generales de prevención de lavado de activos y financiación del terrorismo, así como también sobre el sistema de autogestión y control específicamente implementado por la empresa.

Estas capacitaciones deben ser documentadas, quedando constancia de ellas, donde es importante indicar la fecha, el lugar, el tema tratado y los asistentes, para que quede evidencia de la diligencia con que la empresa ha cumplido su obligación, de garantizar que el sistema de autogestión y conocimiento sea conocido y funcione eficaz y eficientemente.

De otra parte, la Circular Externa 100-000005 del 17 de junio de 2014

emitida por la Superintendencia de Sociedades exige a las empresas vigiladas adoptar un amplio catálogo de medidas para la prevención del lavado de activos y financiación del terrorismo. Para facilitar su comprensión, estas medidas pueden ser agrupadas en tres clases:

1. *Medidas para conocimiento del riesgo.* Es el conjunto de acciones o tareas que debe cumplir la empresa para conocer las fuentes del riesgo de lavado de activos y financiación del terrorismo al que está expuesta. Incluyen lo siguiente:

1.1. *Medidas para conocer la contraparte.* Se utilizan para conocer a los clientes, a las personas públicamente expuestas, a los proveedores, a los asociados, a los empleados y en general a toda persona natural o jurídica con la que realice negocios. Estas medidas son consecuencia de la máxima de “conocer bien quién está al otro lado de la mesa”, propia de las prácticas de buen gobierno corporativo.

Es importante precisar que para el conocimiento de estas personas no es suficiente diseñar y exigir el diligenciamiento de un formato de vinculación. Es necesario que la empresa verifique la información suministrada por su contraparte, para cerciorarse de que realmente ella es quien dice ser. Para tal efecto, hay que obtener documentos, llamar a sus referencias personales, profesionales y comerciales, y todo aquello que nos permita verificar los datos suministrados inicialmente. Además debe consultarse a la persona jurídica, a su representante legal, a los miembros de su junta directiva, al igual que conviene hacer visitas a las dependencias, oficina, establecimientos de comercio, locales, bodegas o residencia de la contraparte, complementando el objetivo propuesto.

Por supuesto, un proceso de verificación exhaustivo es muy costoso y dispendioso. Por esta razón, la comprobación de la información debe responder a criterios de segmentación del riesgo: cuanto más riesgoso sea el cliente o proveedor, o el negocio que se va a realizar con el tercero, o el área o proceso que estará a cargo del empleado, más profunda y rigurosa debe ser la verificación de su información. Así, por ejemplo, para la verificación de la información necesaria para la contratación de un operario raso de la línea de producción basta hacer

unas llamadas telefónicas y una visita domiciliaria; en cambio, para la verificación de una empleado con manejo de efectivo o responsable de la vinculación de nuevos clientes se requiere además de lo anterior verificar los antecedentes suyos y de su núcleo familiar, mediante consulta en todas las bases de datos posibles.

1.2. *Medidas para conocer los bienes que se adquieren.* En el giro ordinario de su actividad económica es normal, que las empresas adquieran bienes y servicios. Este proceso expone a la empresa al riesgo de adquirir bienes de origen ilícito. Por esta razón, ella debe llevar a cabo un proceso de conocimiento de los bienes que adquiere, en orden a evitar ser utilizada para el ocultamiento, manejo, inversión o aprovechamiento de activos ilícitos.

Este conocimiento de los bienes debe ser particularmente riguroso en la adquisición de inmuebles, por el valor de los mismos y por la gran cantidad de tipologías de lavado de activos relacionadas con el sector inmobiliario. La empresa también debe ser cuidadosa al adquirir bienes extranjeros a proveedores nacionales. En estos casos, la empresa debería solicitar la documentación que demuestra que los bienes fueron importados legalmente al país, y verificar esa información. No debe olvidarse que el contrabando y el lavado de activos son dos fenómenos criminales que en la actualidad van de la mano, y la empresa debe evitar ser utilizada por las organizaciones de lavadores-contrabandistas.

1.3. *Medidas para conocer el mercado.* El nivel de riesgo de lavado de activos y financiación del terrorismo depende también de los productos que comercializa la empresa y los lugares donde los comercializa. Por esa razón, la empresa debe indagar qué tipologías de lavado de activos se relacionan con los productos que comercializa y cuáles son las amenazas que existen en la jurisdicción donde pretende comercializarlos. Este conocimiento le permite adoptar mecanismos para mitigar la exposición al riesgo de ser utilizada para esos delitos.

1.4. *Medidas para el manejo de efectivo.* La empresa debe tener una política clara para el manejo de efectivo. Es importante tener en cuenta

que su manejo incrementa el riesgo de lavado de activos, por lo cual la empresa debe hacer lo posible por incentivar el uso de otros medios de pago. Sin embargo, como el manejo de efectivo es inevitable en ciertos negocios, el empresario debe prever algún procedimiento que mitigue el riesgo de lavado de activos cuando se realicen estas operaciones por cuantías importantes.

2. Medidas para reducir el riesgo al que está expuesta. Una vez conocidas las fuentes de riesgo, la empresa debe llevar a cabo ciertas acciones para mitigar su exposición. Tales operaciones son las siguientes:

2.1. *Establecer un catálogo de señales de alerta que permita detectar operaciones inusuales.* La empresa puede apoyarse en la tecnología. Por ejemplo, desarrollando sistemas o aplicativos, o actualizando los sistemas existentes, para agregar operaciones, detectar casos en los cuales ellas se salen del rango de normalidad y que el sistema arroje una señal de alerta. Piénsese por ejemplo en el caso de clientes que hacen compras en efectivo por valores cercanos a los \$ 10.000.000, para evitar ser identificados y reportados a la UIAF; una posible solución sería que la empresa buscara un recurso tecnológico que permitiera agregar las operaciones de un mismo cliente en un periodo (por ejemplo un mes), y determinar si éstas superan el tope de operaciones en efectivo que deben ser reportadas.

2.2. *Establecer un mecanismo de reporte interno de las operaciones inusuales detectadas.* A tal efecto, el empleado que identificó la señal de alerta debería contar con un medio seguro para reportar al *oficial de cumplimiento* la operación inusual. Este oficial debería indagar más por la operación, por los activos y por las personas involucradas en ella, para determinar si hay elementos de juicio que lleven a concluir que se trata de una operación sospechosa. En ese caso, la empresa debería tener un mecanismo de reporte de operaciones sospechosas a la UIAF.

2.3. *Sin perjuicio de lo anterior, es recomendable que la empresa tenga un catálogo de políticas frente a las operaciones inusuales y sospechosas.* No debe olvidarse que en muchos casos aparece un

conflicto entre el cumplimiento de las metas comerciales y el cumplimiento de las normas sobre prevención de lavado de activos y financiación del terrorismo, es decir, resulta normal que ante la aparición de una señal de alerta en una operación importante desde el punto de vista comercial, el empleado no sepa si debe o no realizarla, pues de un lado está el cumplimiento de las metas comerciales de la compañía y de otro el riesgo de terminar incursos en una actividad ilícita. La empresa allí debería implementar un Código de Conducta en el cual se establezcan los criterios que deben aplicar los empleados para dirigir esos conflictos de interés.

2.4. *Además del Código de Conducta*, la empresa debe contar con un Manual de Prevención de Lavado de Activos y Financiación del Terrorismo, en el cual se describan las responsabilidades asignadas a las áreas más expuestas a este riesgo, los mecanismos de control introducidos a los diferentes procesos y la manera en que estos funcionan desde el punto de vista operativo. Allí también debe quedar definida, adscrita y descrita la función de supervisión, auditoría y mejoramiento del sistema de autogestión y control, con lo cual debe hacerse referencia al oficial de cumplimiento y al papel que cumplen otros órganos de administración como el representante legal, la junta directiva, la auditoría interna y externa y el revisor fiscal.

2.5. *Finalmente, la empresa debe implementar un sistema de gestión documental y de información, especial para el área de cumplimiento.* Este sistema debe permitir que la empresa identifique, capture, organice, clasifique y custodie la información y documentación relevante en materia de cumplimiento de las normas sobre prevención de lavado de activos. Ese procedimiento debe tener la capacidad de responder de manera inmediata y confiable a cualquier requerimiento judicial de información o documentación, de manera que la empresa no tenga problemas de cumplimiento con las autoridades.

1. CATÁLOGO DE SEÑALES DE ALERTA PARA ALGUNAS INDUSTRIAS DEL SECTOR REAL

1.1. Frente al cliente

- Operaciones que no están de acuerdo con la capacidad económica del cliente.
- Operaciones que aisladas o vinculadas escapan al perfil previsible o ya definido del cliente en cuestión.
- De un momento a otro una persona, sin fundamento, aparece como dueño de importantes negocios.
- El cliente ofrece pagar jugosas comisiones, sin justificativo legal y lógico.
- Cambio de propietarios y el historial de los nuevos dueños que no es consistente con la naturaleza del negocio del cliente o los nuevos dueños están reacios a proporcionar información personal o financiera.
- Cuentas que muestran elevadas transacciones de efectivo para negocios que generalmente no manejan grandes sumas de dinero en efectivo.
- Clientes cuyos estados financieros reflejan resultados muy diferentes frente a las otras empresas del mismo sector o con actividad similar.
- Clientes cuya dirección para envío de correspondencia y estados de cuenta está fuera del país, o utilizan casillas de correo o son recogidos en la sede de la empresa.
- Cancelación repentinamente de grandes obligaciones (prepagos) sin justificación aparente sobre la razón del pago súbito o el origen de los fondos.
- Incrementos en la cantidad de dinero en efectivo manejado sin que se presente el incremento correspondiente en el número de transacciones reportadas.
- Operaciones fraccionadas para eludir normas u obligaciones de reporte.

- Operaciones efectuadas frecuentemente a nombre de terceros, sin que exista justificativo para ello.
- Pago utilizando una suma importante de billetes en moneda extranjera sin justificación clara y acorde con la actividad del cliente.
- Operaciones mediante compañías domiciliadas en los sitios denominados “paraísos fiscales” o en regiones o países calificados como “no cooperantes”.
- Compañías que son financiadas con préstamos otorgados en el exterior sin justificación clara de ello.
- Solicitud de ser incluido en la lista de excepciones de no reporte de transacciones en efectivo, sin causa aparente o justificada.
- Empresas que se abstienen de proporcionar información completa, como actividad principal de la empresa, referencias bancarias, nombre de empleados y directores, localización, etc.
- Rehusar informar sobre sus antecedentes personales, al adquirir un bien o solicitar cualquier servicio.
- Pretender adquirir un bien o solicitar un servicio sin referencias, o dirección, sin documento de identificación (pasaporte, cédula de extranjería, libreta de conducción, cédula de ciudadanía, tarjeta del seguro, etc.) o rehusar facilitar otro tipo de información que la entidad solicita.
- Clientes que presentan identificaciones inusuales o anormales, que la entidad no puede verificar.
- Clientes cuyo teléfono se encuentra desconectado, o el número telefónico al momento de efectuar la llamada de verificación, no concuerda con la información inicialmente suministrada.
- Solicitudes que no incluyen referencias laborales sobre empleos an-

teriores o actuales.

— Clientes que no incluyen referencias laborales sobre trabajos pasados o presentes, pero realizan frecuentemente grandes operaciones.

— Rehúsan facilitar la información sobre su actividad o no proporcionar los estados financieros.

— Clientes que frecuentemente solicitan que se incrementen los límites de excepción.

— Personas que rehúsan dar la información necesaria para el registro obligatorio de transacciones en efectivo o para continuar con la transacción después de informarles que el formato debe ser diligenciado.

— Personas que presionan a cualquier funcionario para no diligenciar formularios que impliquen el registro de la información o el reporte de la operación.

1.2. Frente a los proveedores

Las dividimos en proveedores personas jurídicas y proveedores personas naturales.

1.2.1. *Señales en proveedores personas jurídicas*

— Tienen nuevos propietarios, han sido adquiridas con dificultades económicas, cambian su naturaleza y presentan en corto lapso utilidades desbordadas.

— Tienen como propietarios o directivos personas de estratos bajos y con dificultades económicas y que manejan grandes volúmenes de dinero.

— Han sido constituidas con bajos capitales, recibiendo poco después grandes sumas de inversión, principalmente extranjera.

- Realizan grandes inversiones no obstante haber sido creadas muy recientemente.
- Reciben ingresos no operacionales por mayor cuantía que los ingresos operacionales.
- Tienen un capital suscrito muy bajo y/o un objeto social muy amplio.
- Tienen en común socios, gerentes, administradores o representantes legales con otras personas jurídicas o empresas (*outsourcing*).

1.2.2. *Señales en proveedores personas naturales*

- Actúan a nombre de terceros intentando ocultar la identidad del usuario real.
- Fraccionan transacciones para evitar requerimientos de documentación.
- Amenazan o intentan sobornar al empleado de la entidad con el fin de que acepte información incompleta, falsa o para que no diligencie el formulario de registro de información.
- Inicialmente realizan transacciones por montos bajos, pero al corto tiempo las incrementan en altas cantidades.
- Realizan múltiples operaciones en efectivo.
- Son personas ajena a la entidad quienes tienen firma registrada para el manejo financiero.
- Poseen gran solvencia económica y sin embargo les resulta difícil la consecución de referencias o codeudores.
- Realizan operaciones en cantidades o valores no acordes con su actividad económica.

SEGUNDA PARTE

Metodología para la gestión del riesgo de lavado de activos y financiación del terrorismo

1. INTRODUCCIÓN

La globalización de los servicios financieros, la evolución de la tecnología, la facilidad y diversidad de los medios de pago y la posibilidad de realizar grandes operaciones y transacciones de forma virtual y en tiempo real han impulsado múltiples y modernos caminos, mediante los cuales distintas clases de delitos pueden cometerse de manera más eficaz. Existen dos conductas que canalizan en sí mismas más recursos provenientes de actividades delictivas que cualquier otra: el lavado de dinero y el financiamiento al terrorismo. De ahí la importancia de conocer cuál ha sido su evolución, las nuevas tipologías utilizadas, las herramientas tecnológicas que facilitan su ejecución y, por supuesto, las metodologías y herramientas necesarias para prevenirlas y combatirlas.

En el caso específico de Colombia, el conflicto armado interno ha consolidado una sinergia entre el lavado de dinero y el terrorismo, ya que el primero provee los recursos mediante los cuales este último subsiste y que agudiza el deterioro de la situación nacional.

En esta segunda parte de la obra se identifican las acciones orientadas a una eficiente medición y administración del riesgo de lavado de activos y de la financiación del terrorismo en el desarrollo de los distintos procesos del negocio en la empresa, para que la misma se vea lo menos expuesta posible a riesgos de operación, de reputación, legales o de contagio.

Considerando la amenaza que para la estabilidad del sistema financiero y la integración de los mercados representan el lavado de activos y la financiación del terrorismo, el papel que cumplen los órganos de supervisión y control en cualquier estructura administrativa estatal, debe potenciarse para asegurarse instrumentos apropiados y eficientes para reducir la eficacia de las tipologías empleadas en el ámbito de los negocios. Al efecto, en Colombia, la Superintendencia Financiera (SFC) ha impartido instrucciones para que las organizaciones vigiladas implementen un Sistema de Administración del Riesgo de Lavado de Activos y de Financiación del Terrorismo (en adelante SARLA/FT) más exigente y, con mayores alcances que otros modelos de prevención y control.

Por su parte, las Superintendencias de Notariado y Registro, de Salud, de Economía Solidaria y la Dirección de Impuestos y Aduanas Nacionales (DIAN), han generado a través de actos administrativos de carácter general medidas menos estrictas, pero igualmente eficientes, que componen el Sistema Integral de Prevención y Control del LA/FT (en adelante SIPLA/FT), con el fin de prevenir que sus vigiladas sean utilizadas para dar apariencia de legalidad a activos provenientes de actividades delictivas o para la canalización de recursos hacia la realización de actividades terroristas.

El conjunto de estas instrucciones de obligatoria observancia establece criterios y parámetros mínimos que deben atenderse por las entidades vigiladas, en el diseño, implementación y funcionamiento del SARLA/FT y del SIPLA/FT. Su eficaz aplicación es tarea que compete asumir con mayor responsabilidad a los llamados oficiales de cumplimiento y los gerentes de riesgo u órganos de control interno, según la estructura organizacional de la empresa o negocio de que se trate.

Conocer y comprender entonces el funcionamiento de los dos sistemas de prevención es asunto de la mayor importancia, si se quiere observar una debida diligencia frente a la amenaza del lavado de activos y sus consecuencias en cualquier actividad del circuito económico que demande elevar los estándares de anticipación de la concreción de un riesgo potencial.

Es así que el SARLA/FT se compone de dos fases: la primera, corresponde a la prevención del riesgo y, su objetivo es evitar que se introduz-

can a la empresa y al circuito económico recursos provenientes de actividades relacionadas con el lavado de activos y financiación del terrorismo (en adelante LA/FT); la segunda, abarca el control en la organización y su propósito es detectar y reportar las operaciones que se pretendan realizar o se hayan realizado para intentar dar apariencia de legalidad a operaciones vinculadas al LA/FT.

Por ser el SARLA/FT un verdadero sistema, abarca todas las actividades que realiza la empresa en el desarrollo de su objeto social y su direccionamiento debe constituir uno de los valores esenciales en el establecimiento de las políticas señaladas desde la junta o consejo directivo. Además se aplica a todos los macroprocesos de direccionamiento, de realización (misionales) y de apoyo definidos para la organización en el desarrollo de sus actividades, en los cuales se deben identificar los eventos de riesgo de LA/FT ocurridos y posibles.

Atalefector, la responsabilidad por la aplicación correcta del SARLA/FT está a cargo del jefe de cada proceso como encargado del control de gestión en su respectiva área o unidad de trabajo. Por su parte, la misión del gerente de riesgos es la de evaluar y comprobar permanentemente el funcionamiento de los diferentes controles establecidos por la empresa para proteger sus recursos y optimizar su gestión.

Es necesario destacar que la administración del riesgo de LA/FT es de una naturaleza diferente a la de los procesos de administración de los riesgos típicamente financieros (crédito, técnicos de seguros, mercado, liquidez, etc.), pues mientras los mecanismos para la administración del riesgo de LA/FT se dirigen a prevenirla, detectarla y reportarla (oportuna y eficazmente), los mecanismos para la administración de los segundos se dirigen a asumirlos íntegra o parcialmente en función del perfil de riesgo de cada organización y de la relación rentabilidad/riesgo.

2. APLICACIÓN DE LA METODOLOGÍA EN EL PROCESO PRODUCTIVO

Identificada la importancia y alcance de los sistemas de prevención y detección de operaciones asociadas al LA/FT, corresponde ahora definir

su aplicación en el proceso productivo para: i) implantar el SARLA/FT en la empresa, recurriendo a los procesos del ciclo PHVA (planear, hacer, actuar y verificar); ii) identificar las Unidades Estratégicas (UE), expuestas a eventos de riesgo de LA/FT; iii) desarrollar el concepto de evento de riesgo de LA/FT, el cual conjuga en una sola unidad los eventos de riesgo de LA/FT y las Unidades Estratégicas (UE), que a su vez están integradas por los segmentos de los factores de riesgo: cliente, producto, canal de distribución y jurisdicción; iv) identificar los eventos de riesgo de LA/FT que primero se deben ubicar, localizar y describir, recurriendo a los procesos claves o misionales de la empresa, a la codificación y, para la descripción, a la aplicación de las técnicas metodológicas denominadas “espina de pescado” y de los “cinco por qué”. La primera, ayuda a establecer los elementos que conforman el riesgo y, la segunda, a establecer las causas del mismo. A estas dos metodologías nos referiremos posteriormente.

De lo que se trata entonces es de definir en los distintos niveles de la empresa, el ámbito de las responsabilidades y de su ejecución. Por tanto, a la junta directiva compete establecer o aprobar las políticas que integran el SARLA/FT o SIPLA/FT; a la gerencia general se asigna el direccionamiento sobre la ejecución de los procedimientos; la gerencia de riesgos ejecuta los procedimientos, y tiene la autoridad para identificar, medir, controlar y monitorear eventos de riesgo de LA/FT; así mismo, la gerencia de riesgos y el oficial de cumplimiento tienen la responsabilidad de identificar, medir y monitorear los eventos de riesgo de LA/FT.

Por su parte, los empleados participan en la implementación de las políticas y procedimientos y en la identificación, medición y control de los eventos de riesgo de LA/FT, pero no asumen su monitoreo.

Finalmente, imaginando una matriz de lo expuesto, el cuadro siguiente dibuja el mapa conceptual aplicado.

Tabla 1

Matriz de responsabilidades en SARLA/FT o en el SIPLA/FT en la empresa

EVENTO DE RIESGO DE LA/FT (SARLA/FT)				
	Autoridad: ¿quien decide!	Responsabilidad: ¿quien ejecuta!	Participación: ¿quien colabora!	Aprobación
Políticas	Junta directiva	Gerencia de riesgos	Empleados	Junta directiva
Procedimientos	Gerente general	Gerencia de riesgos	Empleados	Junta directiva
Identificar evento de riesgo de LA/FT	Gerente de riesgos	Oficial de cumplimiento	Empleados	N.A.
Medir evento de riesgo de LA/FT	Gerente de riesgos	Oficial de cumplimiento	Empleados	N.A.
Controlar evento de riesgo de LA/FT	Gerente de riesgos	Jefes de macroprocesos	Empleados	N.A.
Monitorear evento de riesgo de LA/FT	Gerente de riesgos	Gerente de riesgos/ Oficial de cumplimiento	Empleados	N.A.

Cuando se presenta un evento que deriva en una amenaza para que la empresa sea utilizada en una operación de LA/FT, ella se puede ver expuesta a una serie de riesgos asociados en materia legal, operativa, reputacional o por contagio.

Por tanto, los efectos que se derivan de la materialización del riesgo de LA/FT se concretan en las consecuencias que en materia de imagen o reputación, sanciones pecuniarias que envuelven la suspensión de actividades o cancelación de la personería jurídica y el bloqueo financiero que conduce a la exclusión para intervenir en el mercado financiero o bursátil, pueden surgir para la empresa. Igual ocurre cuando alguno de los socios o accionistas, por actividades personales que envuelven un evento de riesgo, exponen a la persona jurídica o a los otros asociados a un contagio.

3. FUENTES PARA LA IDENTIFICACIÓN DE POSIBLES IMPACTOS

La empresa debería emplear herramientas como: revisión de fuentes bibliográficas, diagramas causa-efecto o “espina de pescado”, lluvia de ideas, análisis de escenarios y juicios basados en la experiencia, de los que se obtenga como resultado una lista de los riesgos detectables que pueden impactar negativamente a la empresa.

La revisión de fuentes bibliográficas provenientes de diferentes fuentes de información con datos de riesgos de LA/FT, eventos de riesgo y señales de alerta, basados en la experiencia de los organismos nacionales e internacionales expertos en el tema de prevención de LA/FT, es un instrumento muy importante.

Cada fuente de información se debe revisar con el fin de identificar su aplicabilidad en la organización, de acuerdo a la naturaleza y características propias de cada factor de riesgo y del negocio. De esta manera, se genera un listado de riesgos que en un determinado momento afectan a la empresa.

Las fuentes de consulta se dividen en: i) institucionales o internas, y ii) de origen gubernamental o de organismos internacionales. Las primeras corresponden a los manuales de procesos, políticas y procedimientos y a las circulares o instructivos internos; las segundas, derivan ordinariamente de las experiencias de las unidades de inteligencia financiera o de los organismos de supervisión y control, lo mismo que de las cuarenta recomendaciones del GAFI y sus posteriores modificaciones, las topologías del GAFISUD de los años 2005 y 2006, los 100 casos EGMONT, la guía de señales de alerta para el sector financiero y otros sectores UAF, entre otros.

En todo caso, las señales de alerta, eventos y riesgos resultantes de la evaluación se deben vincular a cada factor de riesgo, teniendo presente su aplicabilidad en la organización.

A la sumatoria de las tipologías anteriores que suponen la concreción de eventos recogidos por la experiencia, se agrega el método de “lluvia de ideas”, con el fin de completar y ajustar el inventario de eventos

posibles que permitan identificar riesgos que, bajo circunstancias extremas y especiales, pudieran suceder, contemplando el futuro de la organización.

El trabajo se debe realizar con un grupo de expertos que proporcionen nuevos enfoques y nuevas opiniones y que, con el conocimiento multidisciplinario, pongan en juego la imaginación, los datos históricos y la memoria, de forma que una idea lleve a concebir nuevas ideas.

De esta manera, se debe obtener la información que será registrada en el diagrama causa-efecto o “espina de pescado”.

Para realizar el proceso de identificación de las posibles pérdidas que puede generar un evento de riesgo de LA/FT, se debe:

- Seleccionar la UE donde se desea buscar eventos de riesgo de LA/FT.
- Seleccionar las actividades en las que se podrían presentar eventos de riesgo de LA/FT.
- Identificar y describir todos los tipos de pérdidas que se podrían presentar en caso de materializarse el evento de riesgo de LA/FT.

Una vez se ha obtenido el listado de posibles eventos de riesgo de LA/FT de una o de todas la UE, este debe ser validado mediante reuniones que involucren a los responsables o dueños de cada proceso analizado. Luego, con el visto bueno del experto, se validan los factores de riesgos asociados, las situaciones de riesgo y sus causas.

Esta etapa tiene como objetivo valorar los eventos de riesgo de LA/FT con base en la información obtenida en el Formato para la Identificación y Descripción de Eventos de Riesgo de LA/FT –registrados en la etapa de identificación–, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se deben implementar.

El análisis del riesgo dependerá de la información sobre el mismo, de su causa y la disponibilidad de datos. Para adelantarla, es necesario diseñar escalas que pueden ser cuantitativas o cualitativas para determinar y evaluar la frecuencia y la pérdida asociadas a los diferentes eventos de

riesgo de LA/FT, según los posibles eventos legales, operacionales, reputacionales y de contagio en los que la organización podría verse involucrada en caso de no desarrollar una correcta administración de este riesgo. La elaboración de los niveles de calificación se realiza mediante la discusión con un grupo de expertos, para contemplar los posibles enfoques y concluir sobre los niveles establecidos para cada nivel de riesgo.

4. PROPUESTA METODOLÓGICA

La metodología que proponemos para el diseño e implementación del SIPLA/FT o del SARLA/FT la podemos esquematizar en los siguientes procesos, la presentamos al inicio de esta segunda parte del libro a fin de familiarizar al lector con el tema:

PRIMER PASO: Realice una autoevaluación personal de su conocimiento, habilidades y competencias sobre prevención y control

Los temas de prevención y control del lavado de activos y de la financiación del terrorismo (SIPLA/FT), así como el de la gestión de este tipo de riesgo (SARLA/FT), probablemente sean nuevos para usted y para su empresa.

Para asegurar el éxito del diseño e implementación de cualquiera de los dos sistemas, consideramos fundamental que realice un diagnóstico de sus habilidades y competencias personales para asumir la responsabilidad del diseño e implementación de estos.

Si usted ha sido recientemente nombrado como oficial de cumplimiento o ya está en el proceso de mejorar la eficacia de su gestión, antes de iniciar el diseño e implementación del sistema lo invitamos a que responda objetivamente las siguientes preguntas:

¿Conoce y comprende la normatividad sobre el sistema y las normas más recientes que han actualizado la prevención y control del lavado de activos y financiación del terrorismo en el país y en el mundo?

¿Tiene claridad sobre las responsabilidades legales que asume el oficial de cumplimiento, los miembros de la junta directiva y, el representante legal como responsables de la prevención y control del lavado de activos y financiación del terrorismo en la empresa?

¿Sus habilidades y competencias están relacionadas con la prevención y el control en la empresa?

¿Posee el efectivo respaldo y comprensión del representante legal y de la junta directiva para ejercer adecuadamente las responsabilidades y funciones que le competen al cargo de oficial de cumplimiento?

¿Posee una visión y comprensión integral y corporativa de la empresa o solamente la del área donde se ha desempeñado?

SEGUNDO PASO: Designe un comité institucional lo más amplio posible, con la participación de la mayor cantidad de funcionarios de alta dirección de las diferentes áreas que integran la empresa

En este comité recomendamos hacer lectura y análisis exhaustivo del contenido de las normas nacionales e internacionales sobre prevención y control del LA/FT.

Otra actividad debería ser que colaboren en la realización del diagnóstico del contexto organizacional mencionado.

La responsabilidad y la autoridad sobre el SIPLA/FT o el SARLA/FT debe ser asignada al oficial de cumplimiento, pero la fuente de información sobre los eventos de riesgo de LA/FT proviene de las áreas operativas de la empresa.

TERCER PASO: Diagnostique el contexto organizacional donde se realizará la prevención y control del LA/FT

Conocer detalladamente las características de la organización y su entorno es el segundo paso para asegurar el éxito del diseño e implementación del SIPLA/FT o del SARLA/FT.

Los eventos de riesgo de LA/FT se pueden encontrar dentro o fuera de la empresa y se pueden presentar en cualquier tipo de organización, porque cualquiera de ellas está expuesta al riesgo de LA/FT.

En los sistemas y cultura aplicados por la empresa es donde se pueden encontrar las causas de los eventos de riesgo de LA/FT. La mayoría de las veces, los eventos de riesgo de LA/FT se gestan fuera de la empresa.

Las características de los valores organizacionales que practica y los sistemas que tenga la empresa o que se deseen imprimir constituyen las determinantes de su vulnerabilidad al riesgo de LA/FT y también las determinantes de las políticas, procesos y actividades de prevención y control que debe implementar tanto en SIPLA/FT como en SARLA/FT.

Determine si existe un alineamiento de la edad de la organización y su entorno, particularmente en sus sistemas y políticas antifraude.

Concentre su atención en el diagnóstico de la prevención y control del LA/FT en la empresa.

CUARTO PASO: Para el diagnóstico, desagregue los elementos que conforman la empresa al menos en tres ámbitos: estratégico, de control y operativo

El *ámbito estratégico* se podría desagregar en dos componentes: la estrategia corporativa y la de mercadeo. Para lo cual, determine cuáles son los elementos del contexto corporativo que cree deben ser de interés para el oficial de cumplimiento a fin de planear y ejecutar la prevención y control del lavado de activos.

La *estrategia corporativa* comprende:

- Los procesos de divulgación y comunicación interna que se podrían utilizar para difundir información sobre el SIPLA/FT o el SARLA/FT.
- La misión definida para la empresa.
- La visión.

- Los objetivos estratégicos corporativos preferencialmente expresados en un mapa de objetivos estratégicos.
- La estrategia de la mezcla de mercadeo.
- La actitud de la alta gerencia hacia el control y en especial hacia la prevención y control del LA/FT.
- Los proveedores de todo tipo de insumos.
- Los sistemas de logística de almacenamiento, transporte y distribución.
- Los entes de vigilancia y control oficial.
- Los *stakeholders*.
- La estructura organizacional.
- Las normas internas y externas.
- La actitud hacia el cambio y la innovación.

En la *estrategia de la mezcla de mercadeo* es donde seguramente encontraremos las mayores vulnerabilidades de la organización al riesgo del LA/FT, porque allí se encuentran los principales factores de riesgo de LA/FT, tales como:

- Los clientes en los diferentes segmentos objetivo de mercado, tanto nacionales como internacionales.
- Los productos o servicios de la empresa.
- Los canales de distribución.
- El recurso humano de la organización.

El *ámbito de control* está conformado por:

- El nivel de conocimiento, sentimientos y acciones de todos los funcionarios de la empresa, en particular los del área de control interno y revisoría fiscal, hacia el control general y hacia el LA/FT.
- Las políticas de control interno.
- Los procesos de control interno.
- La estructura organizacional de control dispuesta por la organización que debe incluir las funciones y responsabilidades.
- Los recursos tecnológicos para control asignados por la empresa.
- Los recursos humanos para control disponibles.

Sugerimos dar respuesta a las siguientes preguntas:

¿Cuáles son los conocimientos, sentimientos y comportamientos del recurso humano, en todos los niveles jerárquicos de la organización, con relación al LA/FT y contra el fraude?

¿La estructura actual de control interno es la más adecuada para asumir las responsabilidades y tareas relacionadas con la prevención y control del LA/FT?

¿Posee la organización una infraestructura tecnológica, de comunicaciones y de sistemas de información adecuada para generar oportunamente y de manera confiable la información que solicita el oficial de cumplimiento?

¿La vinculación contractual y no contractual de cualquier tipo de persona o entidad (empleados, proveedores, clientes) a la empresa está condicionada a rigurosos controles, sobre todo los relacionados con el conocimiento sobre esas personas?

¿Los equipos de *hardware* y *software* que utiliza la empresa le permitirán obtener y procesar para análisis información contable y de quienes tienen vinculación contractual y no contractual con la empresa?

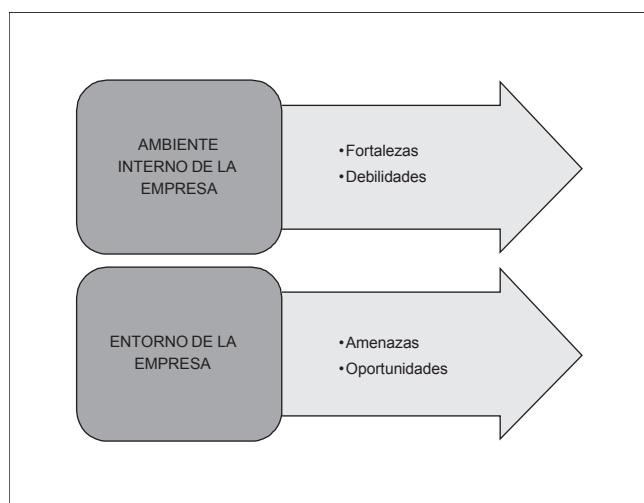
QUINTO PASO: Recomendamos iniciar cualquier proceso de gestión en prevención y control del LA/FT, elaborando un diagnóstico de:

Las fortalezas y debilidades internas que tiene la organización en su contexto corporativo para prevenirlo y controlarlo.

Las amenazas externas a las que está expuesta para ser utilizada por delincuentes con propósitos de LA/FT.

Las oportunidades externas para mejorar los sistemas de control.

Gráfico 1
Elementos para el diagnóstico organizacional



—*Fortalezas para la prevención y control del LA/FT*

Son aquellos elementos internos, positivos y efectivos de que dispone la organización para enfrentar las amenazas de LA/FT; generalmente se refieren a políticas, procesos, recursos, actitudes, mecanismos e instrumentos que se poseen.

—*Debilidades para la prevención y control del LA/FT*

Son aquellos elementos, recursos, habilidades y actitudes que la empresa tiene y que constituyen barreras para lograr una eficiente y eficaz prevención y control del LA/FT.

Las debilidades son problemas internos que, una vez identificados, se pueden y deben eliminar.

Las debilidades o fortalezas siempre estarán referidas a los ámbitos estratégico, de control y operativo de la empresa.

—*Oportunidades para la prevención y control del LA/FT*

Generalmente son aplicativos de *software* o de *hardware*, metodologías, conceptos o enfoques que la empresa puede descubrir en los mercados para implementar o volver más eficientes sus sistemas de control, especialmente el de LA/FT.

—*Amenazas para la prevención y control del LA/FT*

Son retos presentados por acciones de delincuentes, que, ante la ausencia de acciones de prevención y control del LA/FT, afectarían negativamente a la empresa, la estancarían o la llevarían a su desaparición. Son situaciones externas a la organización relacionadas con el delito de LA/FT.

Ante esos retos es necesario responder seriamente la pregunta: ¿En caso de materializarse el riesgo de LA/FT, se podría impedir parcialmente o totalmente la actividad de la empresa?

Algunas de las preguntas que se pueden realizar y que contribuirían a su identificación son:

¿A qué buenas oportunidades de mejoramiento de la prevención y control del riesgo de LA/FT se enfrenta la empresa?

¿Cuáles son las mejores prácticas de prevención y control del LA/FT que se conocen?

¿Qué cambios de tecnología para la prevención y control del LA/FT se están presentando en el mercado?

¿Qué cambios en la normatividad legal sobre prevención y control del LA/FT se están presentando?

Las amenazas y oportunidades por lo general se encuentran en el entorno y particularmente en los elementos que conforman la estrategia de mercadeo.

Como podrá advertirse, a los efectos de la prevención y control del LA/FT, hemos reducido el alcance del ámbito operativo de la empresa a los procesos y actividades que se realizan para alcanzar sus objetivos y al mapa de objetivos estratégicos.

Con seguridad, en este ámbito del contexto organizacional también encontraremos eventos de riesgo de LA/FT y, por supuesto, en ellos podemos aplicar medidas de control que minimicen su severidad.

Cualquiera de los dos sistemas de prevención y control del LA/FT será más fácil de diseñar y ejecutar si la empresa está organizada y funciona mediante procesos claramente establecidos, documentados, conocidos y ejecutados.

Para el diagnóstico del ámbito operativo, le sugerimos que responda las siguientes preguntas: ¿la empresa está organizada y funciona mediante procesos?

Si no es así, le sugerimos que al menos, antes de iniciar cualquier actividad de diseño del sistema, produzca una lista de los procesos y consecuentes actividades correspondiente a los macroprocesos de dirección, miento estratégico, misionales y de soporte o apoyo, sin emprender la tarea de documentarlos.

El mapa de objetivos estratégicos de la empresa se debería diseñar, preferencialmente, utilizando la metodología del *Balanced Scorecard*⁽¹⁾, que define objetivos para cuatro tipos de perspectivas: la financiera, la del cliente, la operativa y la del aprendizaje. Consideramos que esta metodología es de suma utilidad para gestionar la prevención y control de cualquier tipo de riesgo, en especial el del LA/FT (para mayor información, lo invitamos a que visite la dirección web referida en el pie de página). Le recomendamos utilizar los instrumentos y metodologías del *Balanced Scorecard* para gestionar el SIPLA/FT o el SARLA/FT.

Le sugerimos incluir, dentro de cada perspectiva, objetivos relacionados con la prevención y control del LA/FT.

SEXTO PASO: Produzca un glosario propio para la empresa a fin de que se pueda lograr homogeneidad entre los integrantes de la misma en la comprensión y aplicación de la normatividad y del sistema que se debe diseñar e implementar

Es decir, adecúe el contenido de las definiciones que por lo general se incluyen en la normatividad de cada país a las características de la empresa, teniendo especialmente en cuenta su naturaleza y objeto legal.

SÉPTIMO PASO: Identifique la o las tipologías del delito de LA/FT de las cuales podría ser víctima la empresa

No realizar esta identificación podría conducir a la pérdida de recursos al no concentrarlos en la tipología a la que está verdaderamente expuesta la empresa.

Una “tipología de lavado de activos y financiación del terrorismo es el conjunto de técnicas, procedimientos, operaciones o manipulaciones utilizadas por la delincuencia para lavar activos y/o financiar el terrorismo”⁽²⁾.

(1) En: <www.eumed.net/libros/2005/lmr/15.htm> (“Balanced Scorecard: De la estrategia a los resultados” de Luis Sami Ferrer F.).

(2) Esta definición fue elaborada por Sara Magnolia Salazar, ex fiscal delegada para el delito de LA/FT ante la Corte Suprema de Justicia de la República de Colombia.

Estas tipologías han sido producidas y son permanentemente actualizadas por organismos nacionales e internacionales⁽³⁾.

OCTAVO PASO: Documéntese o defina las señales de alerta que podrían evidenciar que la empresa podría estar siendo vulnerada por el LA/FT a través de una de las tipologías mencionadas

Una señal de alerta es un hecho, información o circunstancia particular que rodea la realización de una transacción o actividad (vinculación, comportamiento o transacción) de un cliente, usuario o funcionario de una entidad que supera lo normal y podría ser susceptible de ser sospechoso de lavado de activos o financiación del terrorismo.

NOVENO PASO: Aplique el ciclo PHVA (planear - hacer - verificar - actuar) para cada una de las fases y etapas al gestionar el SIPLA/FT o el SARLA/FT

Al *planear* (P) se identifican, documentan y evalúan los eventos de riesgo de LA/FT inherentes al desarrollo de cada proceso y sus riesgos asociados; y se diseñan los controles necesarios para reducir los riesgos a niveles aceptables de riesgo residual.

Al *hacer* (H) se aplican las metodologías desarrolladas para identificar y evaluar los eventos de riesgo de LA/FT y se colocan en operación o implantan los controles y tratamientos, como parte de los procedimientos del proceso.

Al *verificar* (V) se utilizan métricas para establecer la efectividad real que tienen los controles establecidos para prevenir y controlar los riesgos.

Al *actuar* (A) se definen e implantan acciones de mejoramiento continuo de los controles y procedimientos de administración de los eventos de riesgo de LA/FT.

(3) La Unidad de Información y Análisis Financiero (UIAF) de la República de Colombia (<www.uiaf.gov.co>) es la entidad que ha elaborado las principales tipologías. Estas pueden ser consultadas en su página web, aunque las versiones más actualizadas son información reservada para los intermediarios autorizados.

DÉCIMO PASO: Desarrolle sus propias metodologías o aplique otras ya elaboradas para el diseño de las etapas de la prevención y control del LA/FT

Las etapas del SARLA/FT son identificación, medición, control y monitoreo de eventos de riesgo de LA/FT, mientras que las del SIPLA/FT, en nuestra concepción, excluyen la medición.

—Para la identificación de evento de riesgo de LA/FT

Utilizando nuestra metodología de la “espina de pescado”, proceda de la siguiente manera:

Halle o encuentre cada evento de riesgo de LA/FT.

Denomine el evento de riesgo de LA/FT (póngales un nombre y un código).

Ubique o localice cada evento de riesgo de LA/FT en un proceso.

Segmenta cada factor de riesgo: los principales factores de riesgo en empresas del sector financiero son el cliente, el usuario, los servicios financieros, los canales de distribución del servicio y las jurisdicciones geográficas. (Para empresas del sector real, además de los mencionados para el sector financiero, podrían ser: riesgo sobre el factor humano, riesgo sobre los proveedores de recursos físicos, materias primas, activos fijos, suministro, riesgo sobre los medios de pago y riesgo por operaciones de comercio exterior).

Identifique las Unidades Estratégicas de Negocio (UEN) que podrían estar expuestas al riesgo de LA/FT (estas se pueden deducir de los factores de riesgo).

Describa cada evento de riesgo de LA/FT, utilizando todos los elementos incorporados a la “espina de pescado”: señal de alerta, factor de riesgo, situación de riesgo, causas primarias y causa final. Diseñe un formato-plantilla para consignar el perfil del evento de riesgo de LA/FT.

—*Para la medición de cada evento de riesgo de LA/FT*

Identifique y describa los impactos cualitativos y cuantitativos en términos de pérdidas económicas que se le podría generar a la empresa en caso de materializarse un evento de riesgo de LA/FT.

En este proceso tenga en cuenta los impactos por concepto de riesgo legal, riesgo operativo, riesgo reputacional y riesgo de contagio. Asígnele a cada impacto la ponderación que estime conveniente.

Elabore la escala de medición aplicable a todos los impactos o pérdidas.

Elabore la escala de medición de la probabilidad de ocurrencia para cada evento de riesgo de LA/FT.

Elabore la escala de medición de la severidad aplicable a todos los eventos de riesgo de LA/FT.

Calcule la severidad para cada evento de riesgo de LA/FT.

Con las mediciones de probabilidad de ocurrencia y de impacto y utilizando las escalas de medición anteriores, calcule la severidad de cada evento de riesgo de LA/FT.

—*Para el control de cada evento de riesgo de LA/FT*

Con los valores de severidad anteriores, elabore el mapa de riesgo inherente, sin tener en cuenta el efecto de los controles.

Identifique los eventos de riesgo de LA/FT relevantes, es decir, aquellos que presentan la mayor severidad.

Establezca la causa final que origina cada evento de riesgo de LA/FT.

Diseñe controles para minimizar la severidad de cada evento de riesgo de LA/FT relevante.

Aplique los correctivos de control que reducen la frecuencia y/o el impacto y, por tanto, la severidad.

Después de un tiempo prudente para que los controles surtan su efecto, vuelva a medir la severidad de cada evento de riesgo de LA/FT.

Con los valores resultantes de severidad, vuelva a elaborar el mapa de riesgo para obtener el mapa de riesgo residual.

—*Para el monitoreo de cada evento de riesgo de LA/FT*

Continúe aplicando periódicamente los procedimientos anteriores para todos los eventos de riesgo de LA/FT.

Presente periódicamente ante la junta directiva el mapa de riesgo residual.

DÉCIMO PRIMER PASO: Diseñe e implemente los mecanismos e instrumentos para la prevención y control del LA/FT o para la gestión del riesgo y produzca el manual correspondiente

Recuerde que los mecanismos e instrumentos son similares para ambos sistemas.

DÉCIMO SEGUNDO PASO: Presente el manual respectivo para aprobación de la junta directiva de la empresa

CAPÍTULO 1

Alcance del SARLA/FT y del SIPLA/FT

Se podría afirmar, que las estructuras normativas que someten a las entidades vigiladas por los organismos administrativos de supervisión y control como son las superintendencias o las direcciones de impuestos y aduanas, se extenderán en el futuro cercano a todos los sectores de la economía, como una política de buenas prácticas mercantiles frente a la amenaza que representan el lavado de activos y la financiación del terrorismo. Justamente la tendencia de los organismos internacionales que estudian propuestas normativas para la prevención del lavado y que recomiendan su aplicación en las codificaciones locales, se edifican sobre la base de sugerir su incorporación inicial como herramientas de autorregulación ya no sólo en el sistema financiero, sino en todos los sectores de la economía real. Por ello, una buena práctica radica en que las empresas que no hacen parte del sistema financiero, bursátil o asegurador incorporen políticas e instrumentos de prevención del lavado de activos y financiación del terrorismo en sus operaciones. Seguramente, a futuro, todas las empresas del sector real estarán sometidas a regulaciones obligatorias en materia de prevención y, qué bueno sería empezar procesos de autorregulación estructurados conforme a la naturaleza de sus distintos giros comerciales.

Para el efecto, el SIPLA/FT constituye un buen inicio para incorporar prácticas de prevención y estándares mínimos en entidades no vigiladas. En cambio el SARLA/FT, que constituye un instrumento más desarrollado, aplica para empresas que orientan la prevención hacia la administración del riesgo de lavado. Pero en ambos casos, los instrumentos recogen prácticas mínimas reunidas en manuales que deben ser conocidos por todos los agentes de la empresa. Bajo ese entendido, la totalidad de las instrucciones que se relacionen, bien en el Manual SIPLA/FT o en el Manual SARLA/FT, las políticas, los procesos y los procedimientos, serán de obligatoria observancia para todos los empleados de la empresa.

En nuestra opinión, el SIPLA/FT hace parte integral de los elementos del SARLA/FT. El primero, se refiere a la prevención y control del riesgo de LA/FT, y requiere de las etapas de identificación, monitoreo y control del evento de riesgo de LA/FT; el segundo, se refiere a la administración técnica del riesgo, la medición de los eventos y su control oportuno.

La siguiente tabla, adaptada del contenido de cada una de las normas emitidas por la Superintendencia Financiera de Colombia, evidencia lo expuesto:

Tabla 2
El SARLA/FT contiene al SIPLA/FT

SIPLA/FT	SARLA/FT
	<ul style="list-style-type: none"> — Etapas del SARLAFT • Identificación del riesgo • Medición o evaluación del riesgo • Control del riesgo • Monitoreo del riesgo — Elementos del SARLAFT
Políticas en materia de prevención y control del lavado de activos y de la financiación del terrorismo	<ul style="list-style-type: none"> • Políticas
Procedimientos para implantar los mecanismos de control del lavado de activos y de la financiación del terrorismo	<ul style="list-style-type: none"> • Procedimientos
Mecanismos para el control del lavado de activos y de la financiación del terrorismo	<ul style="list-style-type: none"> • Mecanismos
Conocimiento del cliente	<ul style="list-style-type: none"> • Conocimiento del cliente
Concepto de cliente	Conocimiento del cliente por parte de grupos
Concepto de usuario	Excepciones a la obligación de diligenciar el formulario de solicitud de vinculación de clientes y de realizar entrevista
Formulario de solicitud de vinculación Diligenciamiento	
Confirmación y actualización de la información	
Personas públicamente expuestas	Personas públicamente expuestas
Conocimiento del mercado	Conocimiento del mercado
Segmentación del mercado	

SIPLA/FT	SARLA/FT
Segmentación de los factores de riesgo en relación al mercado	
Identificación y análisis de operaciones inusuales	Identificación y análisis de operaciones inusuales
Determinación y reporte de operaciones sospechosas	Determinación y reporte de operaciones sospechosas
Instrumentos para la adecuada aplicación de los mecanismos de control del lavado de activos y de la financiación del terrorismo	Instrumentos
Señales de alerta	Señales de alerta
Infraestructura tecnológica; monitoreo y consolidación de operaciones	Segmentación de los factores de riesgo
	Monitoreo de operaciones
	Consolidación electrónica de operaciones
	Documentación
Órganos con funciones de control	Estructura organizacional
Funciones y responsabilidades del consejo de administración	Funciones de la junta directiva u órgano que haga sus veces
Funciones y responsabilidades del representante legal	Funciones del representante legal
Oficial de cumplimiento	Requisitos y funciones del oficial de cumplimiento
Funciones del oficial de cumplimiento	Órganos de control
•Revisoría fiscal	•Revisoría fiscal
•Auditoría interna	•Auditoría interna o quien ejecute funciones similares o haga sus veces
	Infraestructura tecnológica
	Divulgación de la Información
Reportes	
Reportes internos	Reportes internos
•Reporte interno sobre operaciones inusuales	•Transacciones inusuales
•Reporte interno sobre operaciones sospechosas	•Operaciones sospechosas
	•Reportes de la etapa de monitoreo
Reportes externos	Reportes externos
•Reporte de operaciones sospechosas (ROS)	•Reporte de operaciones sospechosas (ROS)
•Reporte de ausencia de operaciones sospechosas	
•Reporte de transacciones en efectivo	•Reporte de transacciones en efectivo
•Reporte de transacciones múltiples en efectivo	
•Reporte de transacciones individuales en efectivo	
•Reporte de clientes exonerados del registro de transacciones en efectivo	•Reporte de clientes exonerados
	•Reporte de transacciones múltiples en efectivo

SIPLA/FT	SARLA/FT
	• Reporte de los intermediarios del mercado cambiario
	• Reporte de información sobre campañas políticas
	• Reporte de información sobre transacciones realizadas en Colombia con tarjetas crédito o débito expedidas en el exterior
Capacitación	Capacitación
Reporte sobre productos ofrecidos por las entidades vigiladas	
Documentos y registros del SIPLAFT	
• Manual de procedimientos	
• Código de conducta	
• Reglas para la conservación de documentos y registros que evidencien la operación efectiva del SIPLAFT	
• Los informes de la junta directiva, el representante legal, el oficial de cumplimiento y los órganos de control	

1. ALCANCE DEL SARLA/FT

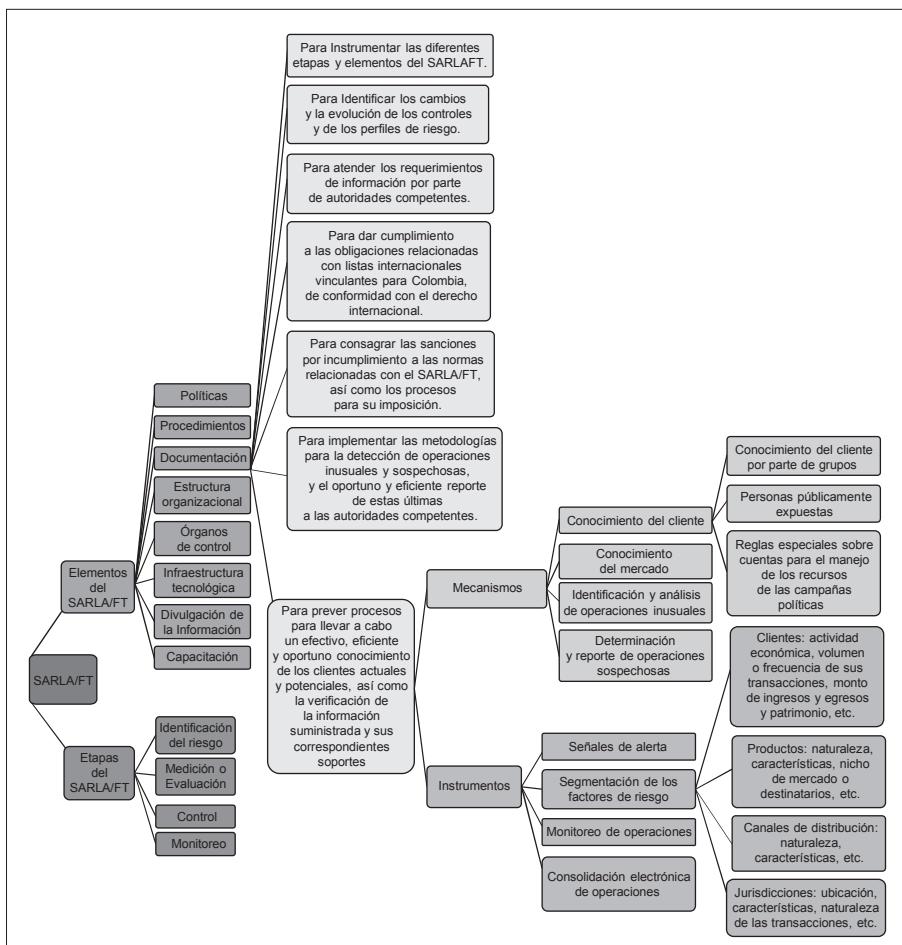
La Circular Externa 22 de 2007 de la Superfinanciera, dirigida a miembros de la junta directiva, representantes legales, revisores fiscales y oficiales de cumplimiento de las entidades sometidas a su inspección y vigilancia, los obliga al diseño e implementación del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLA/FT).

Este es un sistema de administración que deben implementar las entidades vigiladas por la Superfinanciera⁽¹⁾ para gestionar el riesgo de LA/FT, el cual se instrumenta a través de las etapas y elementos que más adelante se describen. Las etapas se refieren a las fases o pasos sistemáticos e interrelacionados mediante los cuales las entidades administran el riesgo de LA/FT; los elementos, al conjunto de componentes a través de los que se instrumenta de forma organizada y metódica la administración del riesgo de LA/FT.

(1) Superfinanciera, Circular Básica Jurídica 007 de 1996, Título I, Capítulo XI.

El SARLA/FT debe abarcar todas las actividades que realizan las organizaciones en desarrollo de su objeto social principal y deberá prever además procedimientos y metodologías para que se protejan de ser utilizadas en forma directa, es decir a través de sus accionistas, administradores y vinculados como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

Gráfico 2
Alcance del SARLA/FT



1.1. Marco normativo del SARLA/FT

La Circular Externa 061 de 2007 de la Superfinanciera, en el numeral 3 presenta el Marco Legislativo para la Prevención y Control del Lavado de Activos, el régimen legal en los ámbitos financiero y penal de la normativa nacional y las normas, estándares y recomendaciones de carácter internacional.

Esta circular comprende las políticas, procesos y procedimientos, relacionados con las etapas del SARLA/FT que se deben aplicar con el objetivo de identificar, medir, controlar y monitorear los riesgos del lavado de activos y la financiación del terrorismo.

También comprende las políticas, procesos y procedimientos, anexos e instructivos, relacionados con los elementos del SARLA/FT, que obedecen, en su gran mayoría, a los controles establecidos para la implementación de las etapas de dicho sistema y que se deben aplicar con el objetivo de prevenir y controlar el LA/FT. Estos elementos contienen los mecanismos e instrumentos de control para: conocer al cliente actual y potencial, conocer el mercado, identificar a los agentes económicos distintos del cliente y usuario, identificar y analizar las operaciones inusuales, determinar y reportar las operaciones sospechosas, establecer señales de alerta acordes con los mecanismos, segmentar los factores de riesgo en relación al mercado, realizar el seguimiento de operaciones y consolidar electrónicamente las operaciones conforme los factores de riesgo.

2. ALCANCE DEL SIPLA/FT

Las entidades obligadas deben implementar un Sistema Integral para la Prevención y Control de Lavado de Activos y de la Financiación del Terrorismo (SIPLA/FT), el cual debe contener como mínimo los siguientes elementos:

- a) Las *políticas* que asumirá la entidad en relación con el cumplimiento de las normas legales sobre prevención y control del LA/FT.
- b) Los *procedimientos* que se desarrollarán para llevar a cabo el SIPLA/FT, los cuales deben contemplar las responsabilidades, deberes y

facultades de los distintos órganos de dirección, administración y control de la entidad en el adecuado cumplimiento del SIPLA/FT.

c) Los *mecanismos e instrumentos* que se aplicarán para implementar el SIPLA/FT.

—*Mecanismos*

- Conocimiento del cliente.
- Personas públicamente expuestas.
- Conocimiento del mercado.
- Segmentación del mercado.
- Segmentación de los factores de riesgo en relación al mercado.

Clientes: actividad económica, volumen o frecuencia de sus transacciones y monto de ingresos, egresos y patrimonio.

Productos: naturaleza, características y nicho de mercado o destinatarios.

Canales de distribución: naturaleza y características.

Jurisdicciones: ubicación, características y naturaleza de las transacciones.

- Identificación y análisis de operaciones inusuales.
- Determinación y reporte de operaciones sospechosas.

—*Instrumentos*

- Señales de alerta.
- Infraestructura tecnológica; monitoreo y consolidación de operaciones.
- Capacitación.

d) Los órganos *con funciones de control* con los cuales contará la cooperativa para implementar el sistema y vigilar su correcto funcionamiento:

- Funciones y responsabilidades de la junta directiva o consejo de administración.
 - Funciones y responsabilidades del representante legal, la revisoría fiscal, la auditoría interna y el oficial de cumplimiento.
- e) Los *reportes relacionados* con el SIPLA/FT
- f) *Documentación*: requisitos y conservación

Los elementos del SIPLA/FT implementados por la entidad deben constar en documentos y registros, de modo que se garantice la integridad, oportunidad, confiabilidad y disponibilidad de la información allí contenida. La documentación deberá comprender por lo menos:

— *Un manual de procedimientos del SIPLA/FT*, el cual deberá contemplar como mínimo:

- Los elementos del SIPLA/FT.
 - Las funciones y responsabilidades de quienes participan en el SIPLA/FT.
 - Los procedimientos para el funcionamiento de los elementos del SIPLA/FT.
 - Los procedimientos de control interno y revisión del SIPLA/FT.
 - Los programas de capacitación.
 - Los demás procedimientos establecidos por la entidad.
- *El código de conducta*.
- Los *documentos y registros* que evidencien la operación efectiva del SIPLA/FT.

—Los *informes* de la junta directiva, el representante legal, el oficial de cumplimiento y los órganos de control.

g) *Sanciones*

El incumplimiento de las disposiciones en materia de prevención y control del lavado de activos y financiación del terrorismo dará lugar a la imposición de las sanciones administrativas.

h) *Práctica insegura*

Se calificará como práctica no autorizada e insegura la realización de operaciones sin el cumplimiento de las disposiciones de ley.

2.1. **Marco normativo del SIPLA/FT**

Las siguientes normas oficiales, según entidad de vigilancia y control, establecen para sus entidades obligadas los elementos que debe tener el SIPLA/FT:

El capítulo XI de la circular básica jurídica de la Superintendencia de Economía Solidaria, dirigido a las entidades cooperativas de ahorro y crédito y multiactivas e integrales con sección de ahorro y crédito vigiladas por dicha superintendencia.

La Circular Externa 081 del 29 de enero de 1999 de la Superintendencia Nacional de Salud, dirigida a gerentes de loterías y concesionarios de apuestas permanentes distribuidores de loterías, el presidente de Ecosalud, gerentes o representantes legales de casinos y demás personas jurídicas dedicadas profesionalmente a la explotación de juegos de suerte y azar.

La Circular Externa 0170 del 10 de octubre de 2002 de la DIAN dirigida a: depósitos públicos y privados, sociedades de intermediación aduanera, sociedades portuarias, usuarios operadores, industriales y comerciales de zonas francas, empresas transportadoras, agentes de carga internacio-

nal, intermediarios de tráfico postal y envíos urgentes, empresas de mensajería, usuarios aduaneros permanentes, usuarios altamente exportadores, los demás auxiliares de la función aduanera y profesionales del cambio de divisas, la cual sustituye la Circular 088 del 12 de octubre de 1999.

La Instrucción Administrativa 08 del 14 de agosto de 2007 de la Superintendencia de Notariado y Registro.

Los elementos mínimos que debe contener el SIPLA/FT para que sea implementado por las organizaciones están expuestos en la Circular Básica Jurídica 007 del 2008, emitida por la Superintendencia de la Economía Solidaria.

CAPÍTULO 2

Contexto organizacional

1. ESTRUCTURA ORGANIZACIONAL

La estructura organizacional para la administración del riesgo de lavado de activos y de la financiación del terrorismo está conformada por los órganos de dirección, administración, control, por el oficial de cumplimiento y por el gerente de riesgos.

El órgano de dirección en la empresa está conformado por la junta directiva o directorio, o consejo administrativo, pero también hacen parte de los órganos de dirección la gerencia general que ordinariamente funge a su vez como representante legal. Con ocasión del SARLA/FT, las entidades vigiladas obligadas a su implementación, están llamadas a incorporar dentro de los órganos de dirección tanto al oficial de cumplimiento como al gerente de riesgos, en el entendido que la ley pretende que la administración del riesgo de lavado de activos y la financiación del terrorismo corresponda al más alto nivel de la organización.

A los órganos de direccionamiento estratégico de la empresa se suman los de control, que corresponden a las auditorías internas u oficinas de control interno y a la revisoría fiscal.

A continuación intentaremos definir los roles que a cada uno de estos órganos de la empresa corresponden frente al manejo del riesgo de lavado de activos y financiación del terrorismo, tomando en consideración que éstos dependerán de la estructura organizacional que se defina en el organigrama respectivo y en los correspondientes estatutos sociales.

1.1. Organigrama

Tomando en consideración los macroprocesos, la estructura de responsabilidades, especialmente en materia de prevención de actividades delictivas se edifica así:

1.1.1. *Junta directiva*

Como máximo organismo de control, le corresponde a la junta directiva (o al órgano correspondiente) ordenar y vigilar que los procedimientos de control interno se ajusten a las necesidades de la empresa con el fin de alcanzar las metas propuestas por los accionistas y garantizar su principal objetivo social: la preservación del entorno ético (arts. 22 y 23 de la L. 222 de 1995 y el num. 3º del art. 73 del EOSF).

Le corresponde definir las políticas y estrategias encaminadas a obtener el más estricto cumplimiento de las normas relacionadas con el SARLA/FT. Por ello, siguiendo las instrucciones de la Circular 22 de la SFC, debe así mismo:

- Adoptar el código de ética en relación con el SARLA/FT.
- Aprobar el manual de procedimientos y sus actualizaciones.
- Designar al oficial de cumplimiento y su respectivo suplente.
- Aprobar el procedimiento para la vinculación de los clientes que pueden exponer en mayor grado a la entidad al riesgo de LA/FT, así como las instancias responsables, atendiendo que las mismas deben involucrar funcionarios de la alta gerencia.
- Hacer seguimiento y pronunciarse periódicamente sobre el perfil de riesgo de LA/FT de la entidad.
- Pronunciarse respecto de cada uno de los puntos que contengan los informes que presente el oficial de cumplimiento, dejando la expresa constancia en la respectiva acta.

- Pronunciarse sobre los informes presentados por la revisoría fiscal y la auditoría interna o quien ejecute funciones similares o haga sus veces y, hacer seguimiento a las observaciones o recomendaciones adoptadas, dejando la expresa constancia en la respectiva acta.
- Ordenar los recursos técnicos y humanos necesarios para implementar y mantener en funcionamiento el SARLA/FT o el SIPLA/FT.
- Aprobar los criterios objetivos y establecer los procedimientos y las instancias responsables de la determinación y reporte de las operaciones sospechosas.
- Establecer y hacer seguimiento a las metodologías para la realización de entrevistas no presenciales y/o la realización de entrevistas por personal que no tenga la condición de empleado de la entidad.
- Aprobar las metodologías de segmentación, identificación, medición y control del SARLA/FT.
- Designar la(s) instancia(s) autorizada(s) para exonerar clientes del diligenciamiento del formulario de transacciones en efectivo.
- Designar la(s) instancia(s) responsable(s) del diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de las operaciones inusuales.

En el caso de grupos en los términos previstos, corresponderá además a las juntas directivas de las matrices impartir los lineamientos y adoptar las medidas necesarias para que cada una de las subordinadas del grupo aplique procedimientos similares a los implementados por la matriz, atendiendo en todo caso las características particulares de la actividad desarrollada por cada una de ellas.

1.1.2. *Representante legal*

El representante legal (o quien haga sus veces) es considerado como un órgano de administración y, para efectos del SARLA/FT, tendrá las funciones y facultades indicadas en la norma por la SFC, tales como:

- Someter a aprobación de la junta directiva, u órgano que haga sus veces en coordinación con el oficial de cumplimiento, el manual de procedimientos del SARLA/FT y sus actualizaciones.
- Verificar que los procedimientos establecidos desarrollos todas las políticas adoptadas por la junta directiva u órgano que haga sus veces.
- Adoptar las medidas adecuadas como resultado de la evolución de los perfiles de riesgo de los factores de riesgo y de los riesgos asociados.
- Garantizar que las bases de datos y la plataforma tecnológica cumplan con los criterios y requisitos establecidos en el presente capítulo.
- Proveer los recursos técnicos y humanos necesarios para implementar y mantener en funcionamiento el SARLA/FT.
- Prestar efectivo, eficiente y oportuno apoyo al oficial de cumplimiento.
- Garantizar que los registros utilizados en el SARLA/FT cumplan con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.
- Aprobar los criterios, metodologías y procedimientos para la selección, seguimiento y cancelación de los contratos celebrados con terceros para la realización de aquellas funciones relacionadas con el SARLA/FT que pueden ejecutarse por estos, de acuerdo con lo señalado en el presente manual.

1.1.3. *Gerente de riesgos*

El gerente de riesgos es considerado como un órgano de administración, hace parte de la estructura organizacional del SARLA/FT y tendrá las funciones y facultades indicadas en la norma, adicional a las funciones establecidas en el respectivo manual de roles y responsabilidades propias de su cargo, así como:

- Diseñar las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para las distintas etapas de la administración del SARLA/FT.
- Actualizar las metodologías e indicadores para las etapas del SARLA/FT, cuando sea necesario, en concordancia con los demás sistemas de administración de riesgos de la compañía, con el fin de mantener unificados los criterios en los distintos sistemas.
- Diseñar conjuntamente con el oficial de cumplimiento, las metodologías de segmentación de factores de riesgo.
- En conjunto con el oficial de cumplimiento, diseñar las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna identificación de operaciones inusuales y detección de operaciones sospechosas.
- En conjunto con el oficial de cumplimiento, adoptar correctivos al SARLA/FT.
- Participar, en conjunto con el oficial de cumplimiento, en el desarrollo de programas internos de capacitación.
- Proponer a la administración la actualización del manual SARLA/FT.
- Incluir dentro de sus informes los temas relacionados con la administración del SARLA/FT.
- Participar en el comité evaluador de operaciones.
- Reportar a la gerencia general.

1.1.4. *Oficial de cumplimiento*

El oficial de cumplimiento debe cumplir, al menos, con los siguientes requisitos, según lo establecido en las normas legales vigentes:

- Ser como mínimo de segundo nivel jerárquico dentro de la entidad y tener capacidad decisoria. El oficial de cumplimiento reporta a la junta directiva.
- Acreditar conocimiento en materia de administración de riesgos.
- Estar apoyado por un equipo de trabajo humano y técnico, de acuerdo con el riesgo de LA/FT y el tamaño de la entidad.
- No pertenecer a órganos de control ni a las áreas directamente relacionadas con las actividades previstas en el objeto social principal.
- Ser empleado de la entidad.
- Estar posesionado ante la SFC.
- Velar por el efectivo, eficiente y oportuno funcionamiento de las etapas que conforman el SARLA/FT o el SIPLA/FT.
- Presentar, cuando menos en forma trimestral, informes escritos a la junta directiva u órgano que haga sus veces, en los cuales debe referirse como mínimo a los siguientes aspectos:
 - a) Los resultados de la gestión desarrollada.
 - b) El cumplimiento que se ha dado en relación con el envío de los reportes a las diferentes autoridades.
 - c) La evolución individual y consolidada de los perfiles de riesgo de los factores de riesgo y los controles adoptados, así como de los riesgos asociados.
 - d) La efectividad de los mecanismos e instrumentos establecidos en el presente capítulo, así como de las medidas adoptadas para corregir las fallas en el SARLA/FT.
 - e) Los resultados de los correctivos ordenados por la junta directiva u órgano que haga sus veces, y

- f) Los documentos y pronunciamientos emanados de las entidades de control y de la Unidad Administrativa Especial de Información y Análisis Financiero (UIAF).

—Promover la adopción de correctivos al SARLA/FT o al SIPLA/FT.

—Coordinar el desarrollo de programas internos de capacitación.

—Proponer a la administración la actualización del manual de procedimientos y velar por su divulgación a los funcionarios.

—Colaborar con la instancia designada por la junta directiva en el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de las operaciones inusuales.

—Evaluar los informes presentados por la auditoría interna, o quien ejecute funciones similares o haga sus veces, y los informes que presente el revisor fiscal, y adoptar las medidas del caso frente a las deficiencias informadas.

—Diseñar, en conjunto con el gerente de riesgos, las metodologías de segmentación, identificación, medición y control del SARLA/FT o del SIPLA/FT.

—Elaborar y someter a la aprobación de la junta directiva, o el órgano que haga sus veces, los criterios objetivos para la determinación de las operaciones sospechosas, así como aquellos para determinar cuáles de las operaciones efectuadas por usuarios serán objeto de consolidación, monitoreo y análisis de inusualidad.

1.1.5. *Oficial de cumplimiento suplente*

El oficial de cumplimiento suplente reemplazará al principal solamente en períodos de vacancia o en ausencia del principal. Su reemplazo debe constar por escrito para efectos de asumir las responsabilidades del caso. En períodos de vacancia del principal, este dejará carta firmada encargan-

do de sus responsabilidades al suplente, y se dejara constancia del período exacto de reemplazo. En ausencia definitiva del principal, el representante legal designará, mediante carta escrita, al suplente como encargado de las funciones del oficial de cumplimiento principal, hasta que sea contratado un nuevo oficial de cumplimiento o este sea promovido como principal por la junta directiva. La copia de una u otra carta, según la situación, debe ser remitida a recursos humanos para dejar, en ambas carpetas, la del principal y la del suplente, constancia del reemplazo y su motivo. Cuando el oficial de cumplimiento suplente sea promovido al cargo del principal, dicha decisión debe ser comunicado a las entidades competentes conforme las normas legales vigentes, en especial, a la UIAF y a la SFC.

1.1.6. *Analista de operaciones inusuales y administrador de datos*

Está a cargo administrativamente del área operativa, pero desempeña funciones de control del SARLA/FT o SIPLA/FT.

En el numeral dedicado a describir la infraestructura tecnológica y consolidación electrónica de operaciones, se podrán observar los recursos tecnológicos con que debería estar dotado el proceso de prevención y control del riesgo de LA/FT, para efectos de administrar el SARLA/FT o el SIPLA/FT.

1.1.7. *Comité evaluador de operaciones*

El comité evaluador de operaciones tiene como principal responsabilidad apoyar la gestión del oficial de cumplimiento y del gerente de riesgos y participar en la toma de decisiones relacionadas con la administración de los mecanismos del SARLA/FT o del SIPLA/FT, conocer al cliente actual y potencial, conocer el mercado, identificar y analizar las operaciones inusuales, determinar y aprobar las operaciones sospechosas, y participar en la toma de decisiones relacionadas con la operación de los instrumentos del SARLA/FT o del SIPLA/FT, revisando y/o estableciendo las señales de alerta, revisando la segmentación de los factores de riesgo en relación al mercado, realizando seguimiento a las operaciones, entre otros instrumentos.

De igual forma, tiene la responsabilidad de discutir el manual del SARLA/FT y del SIPLA/FT y recomendar a la junta directiva la implementación de las políticas y ajuste de los procedimientos que se requieran para la mejorar la administración del riesgo del LA/FT.

En este comité se pueden tratar asuntos relacionados con la normatividad nacional e internacional relacionadas con el tema. Además, este decidirá cuándo una operación debe ser autorizada para continuar el proceso respectivo conforme las señales de alerta reportadas por los empleados de la empresa y según los procedimientos de cada lista de control.

Cuando se presenten conflictos de interés en el análisis de las operaciones inusuales y en la determinación de las operaciones sospechosas, el procedimiento para prevenir y resolver el mismo será resuelto mediante votación, que será aprobada con el voto de la mitad más uno de los miembros del comité evaluador de operaciones, luego de lo cual se dejará constancia en el acta respectiva de tal comité. Ante un empate en la votación, se deberá iniciar nuevamente la misma hasta obtener la mayoría, exponiendo y analizando los argumentos necesarios según el caso.

—Integrantes

El comité evaluador de operaciones podría estar integrado por los siguientes funcionarios:

- a) Representante legal de la compañía;
- b) Oficial de cumplimiento (quien lo preside);
- c) Gerente de riesgos;
- d) Gerente de recursos humanos y físicos (o quien cumpla sus funciones), y
- e) Gerente de operaciones o jefe de operaciones (o quien cumpla sus funciones).

—*Invitados*

Al comité podrán ser convocados aquellos funcionarios que, a criterio de sus miembros, tengan un conocimiento directo de los asuntos a ser tratados o que puedan aportar adecuados elementos de juicio para el análisis pertinente.

—*Frecuencia de las reuniones*

Este comité se debe reunir ordinariamente una vez al mes y extraordinariamente cuando la importancia del tema así lo amerita, a juicio del oficial de cumplimiento o de algún miembro del comité.

La fecha, hora y sitio para la realización de este comité pueden ser informadas verbalmente o por escrito y, para las siguientes reuniones, serán establecidas en la misma reunión del comité y se dejará constancia en el acta respectiva. El oficial de cumplimiento (ordinariamente) u otro de los integrantes de Comité (extraordinariamente) puede citar formalmente a este comité.

El comité podrá tomar decisiones sin necesidad de reunir a sus miembros. Cuando un tema específico deba o quiera ser llevado a comité para su votación, tal tema podrá ser votado por cada integrante por medios electrónicos, en especial por correo electrónico. Esta forma de votación en donde se toma alguna decisión hace parte integral del acta que se elabora como mínimo una vez al mes.

—*Actas del comité*

Como resultado de cada reunión del comité, se redactará un acta para sintetizar los asuntos tratados y/o acordados. Sin excepción, deben quedar actas que formalicen decisiones de reportar operaciones sospechosas u otros requerimientos de las autoridades competentes.

—*Reserva de identidad*

Los nombres de los integrantes de este comité se mantendrán en absoluta reserva, cuando su divulgación pueda representar peligro para su

integridad física, como podría suceder cuando terceras personas (usuarios, remitentes, etc.), a quienes las autoridades investigan por ser reportadas como ejecutoras de operaciones sospechosas, cuestionan a empleados de la organización queriendo conocer la identidad de quien, o quienes, tomaron esa decisión. También puede suceder en caso de anulaciones de operaciones o rechazo de clientes que no cumplen con las condiciones necesarias para garantizar su adecuada y completa identificación y conocimiento.

En estos casos, la persona que atiende la inquietud deberá responder simplemente que ese tipo de decisiones las toma y asume el comité evaluador de operaciones.

1.1.8. *Empleados*

Además de los órganos de dirección, administración y control, del oficial de cumplimiento y del gerente de riesgos, hacen parte de la estructura organizacional del SARLA/FT todos los empleados de la compañía conforme las funciones y responsabilidades indicadas en el manual de roles y en el código de ética y conducta.

—Directores, empleados y/o funcionarios

Son quienes tienen las siguientes responsabilidades respecto del SARLA/FT: garantizar el adecuado conocimiento y vinculación del usuario y del cliente, ejecutar las políticas y metas institucionales, y controlar y revisar las operaciones.

Además deben, reportar al comité evaluador de operaciones, en cabeza del oficial del cumplimiento, las operaciones inusuales detectadas tanto por ellos como por otro personal a su cargo, previa revisión.

Igualmente participar en los programas internos de capacitación y responder las evaluaciones a las mismas, y atender las normas establecidas en el manual del SARLA/FT, su manual de roles y responsabilidades, y lo establecido en el código de ética y conducta.

—*Los empleados vinculados al front office*

Estos empleados tienen las siguientes responsabilidades en el SARLA/FT o en el SIPLA/FT: ayudar al adecuado conocimiento y vinculación del usuario y del cliente, registrar en el aplicativo operativo las señales de alerta detectadas en la prestación del servicio al cliente o usuario, y, reportar al jefe inmediato las operaciones inusuales. Además deben diligenciar debidamente los formatos establecidos, participar en los programas internos de capacitación y responder las evaluaciones a las mismas, y atender las normas establecidas en el manual SARLA/FT o SIPLA/FT, su manual de roles y responsabilidades, y lo establecido en el código de ética y conducta.

—*Otros empleados*

La organización, coherentemente con las leyes aplicables a su actividad comercial, debe asegurar un compromiso de toda la organización para el adecuado cumplimiento del SARLA/FT o del SIPLA/FT. Esta directriz de alto nivel se extiende a todos los responsables de las áreas de dirección, operación y control y a los demás empleados y colaboradores, que, sin exclusión, prestan sus servicios a la compañía, para evitar que sea utilizada con fines criminales.

Todos los empleados de la compañía son responsables por el cumplimiento de la ley, los estatutos, las políticas y objetivos señalados por ella y, en particular, las normas estipuladas en este el manual del SARLA/FT o del SIPLA/FT, en el código de conducta y los manuales internos de procesos.

En especial los directores y los funcionarios del *front office* están en la obligación de reportar cualquier operación o actividad que consideren como inusual a través del correo electrónico o por escrito, dirigido a su jefe inmediato, y este al comité evaluador de operaciones en cabeza del oficial de cumplimiento, explicando los pormenores de las circunstancias observadas.

Adicionalmente, los empleados, administradores y accionistas que, por la naturaleza de sus funciones y procesos dentro de la empresa, deban

establecer vínculos contractuales con usuarios o proveedores de bienes y servicios tienen como responsabilidad hacer la debida gestión para garantizar un adecuado conocimiento del usuario, cliente o agente económico.

1.2. Órganos de control interno y revisión

1.2.1. *Revisor fiscal*

El revisor fiscal de la empresa debe elaborar un reporte trimestral dirigido a la junta directiva, u órgano que haga sus veces, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el SARLA/FT.

Además, tiene que poner en conocimiento del oficial de cumplimiento las inconsistencias y fallas detectadas en el SARLA/FT y, en general, todo incumplimiento que detecte a las disposiciones que regulan la materia.

1.2.2. *Auditoría interna*

La auditoría interna de la empresa o quien ejecute funciones similares, o haga sus veces, debe evaluar anualmente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARLA/FT, con el fin de determinar las deficiencias y sus posibles soluciones. Así mismo, deberá informar los resultados de la evaluación al oficial de cumplimiento y a la junta directiva.

La auditoría interna, o quien ejecute funciones similares o haga sus veces, debería realizar una revisión periódica de los procesos relacionados con las exoneraciones y parametrizaciones de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico.

La empresa podría contratar una auditoría externa en tema SARLA/FT en caso de considerarlo necesario o ante la solicitud de algún agente económico, por los períodos de tiempo que estimen convenientes.

1.3. Infraestructura tecnológica y consolidación electrónica de operaciones

La infraestructura tecnológica debe permitir a la empresa realizar una consolidación electrónica de las operaciones por clientes o usuarios. No obstante, el oficial de cumplimiento y el gerente de riesgos tienen que diseñar las bases de datos necesarias y suficientes con el volumen de operaciones que se deben monitorear, dejando evidencia documental de esta gestión. Así mismo, debe diseñar las bases de datos en las cuales se registran los factores de riesgo, indicadores y demás elementos de información que considere necesarios, dejando igualmente evidencia documental sobre el particular.

Dentro de la infraestructura tecnológica que debería utilizar la empresa están:

Software y equipos: la empresa debe contar con una red de comunicación que permita que las operaciones se consoliden electrónicamente en línea. La consolidación electrónica de operaciones se debería hacer en forma centralizada y por medio de bases de datos. Dichas bases de datos deben contar con las medidas de seguridad acordes con los estándares sobre la materia, todos los empleados deben tener asignados los respectivos roles, al igual que dentro del área de sistemas las funciones tienen que estar debidamente segregadas, todo con el fin de evitar eventos de riesgos tanto operativos como de LA/FT.

Sistema de administración de datos o sea un aplicativo operativo en donde se registren todas las operaciones realizadas.

Una herramienta tecnológica de consulta y reporte de información, que permita acceder a las bases de datos de los aplicativos operativos. Es utilizada para consultar la información que se procese para los reportes que requieren las distintas entidades competentes y para el análisis de información desde el punto de vista de riesgos LA/FT.

Un software utilizado para la consulta y reporte de información relacionadas con las distintas etapas de administración del riesgo que contenga los eventos de riesgo identificados, su medición, los controles, mapas de riesgos inherente y residual.

Un aplicativo de minería de datos que permita detectar vínculos entre los distintos usuarios, beneficiarios o clientes en la operación realizada en la empresa, con el fin de detectar posibles redes que sirvan de base para el monitoreo a clientes y usuarios y para el reporte de operaciones sospechosas.

Ros Stand Alone: programa realizado por la UIAF para que las entidades obligadas puedan remitir los reportes de las operaciones sospechosas de una forma organizada y estandarizada.

AUTOIT: programa que permite el registro automático de la información en el *Ros Stand Alone* a partir de archivos planos que contienen la información que requiere ser digitada. Con este programa se disminuye el tiempo que gastaría una persona en digitar la información en el *Ros Stand Alone*.

WEB Quiz: programa utilizado para evaluar el conocimiento de los empleados según los temas comunicados en cada capacitación. Este programa puede ser utilizado en la intranet o en Internet.

—Divulgación de la información

Las empresas deben producir los siguientes reportes:

a) Reportes internos

- Reporte interno sobre operaciones inusuales.
- Reporte interno sobre operaciones sospechosas.

b) Reportes externos

- Reporte de operaciones sospechosas (ROS).
- Reporte de ausencia de operaciones sospechosas.
- Reporte de transacciones en efectivo: transacciones múltiples en efectivo y transacciones individuales en efectivo.

- Reporte de clientes exonerados del registro de transacciones en efectivo.
- Reporte sobre productos ofrecidos por las entidades vigiladas.

1.4. Programa de capacitación

El coordinador de recursos humanos debe incluir, en el plan anual de capacitación, los eventos relacionados con la capacitación en materia de SARLA/FT a todos los empleados de la empresa. En esta capacitación se consideran aspectos conceptuales y prácticos, dando especial relevancia a estos últimos, a través de talleres y demostraciones de método aplicables a los procesos internos. Igualmente incluye: (a) Políticas y objetivos para la administración de riesgos en la empresa; (b) Conceptos y definiciones relativas al sistema de administración de riesgo operativo, y (c) Metodologías y procedimientos para la identificación, medición, control y monitoreo de eventos de riesgo de LA/FT a los cuales está expuesta la organización.

En los programas de inducción y entrenamiento al personal nuevo vinculado a la empresa serían incluidos igualmente los temas antes mencionados.

Se deben realizar capacitaciones de manera oportuna acerca de cada una de las actualizaciones o eventos asociados al SARLA/F y charlas en las cuales se presenten los resultados obtenidos por cada proceso en lo referente a la gestión de riesgos.

Así mismo realizar evaluaciones con el fin de efectuar los ajustes necesarios, para que todos los empleados puedan comprender el SARLA/FT y sus implicaciones.

—*Procedimientos y medios para evaluar la inducción y/o capacitación*

Se debe contar, por ejemplo, con un programa llamado *WEB Quiz*, el cual se utiliza, a través de la intranet de la empresa, para que todo el per-

sonal responda las respectivas evaluaciones de inducción y/o capacitación. Esta evaluación se realizaría a más tardar dentro del mes siguiente de realizada la inducción y/o capacitación y sería de carácter obligatorio para quienes se les haya efectuado la inducción y capacitación. El oficial de cumplimiento será el responsable de la evaluación y, el auxiliar de soporte del área de sistemas, de su publicación en la intranet.

Las evaluaciones serían almacenadas en bases de datos de acuerdo con los procedimientos internos de programación y almacenamiento de datos utilizados por el *WEB Quiz*.

Los empleados podrían presentar varias veces las evaluaciones y, en todo caso, el *WEB Quiz* guarda en su base de datos los registros de respuesta de cada evaluación. Para las evaluaciones generales se podrían dar plazos no mayores a quince (15) días, para que los empleados presenten las mismas.

En caso de que un empleado pierda una evaluación, debe presentar una nueva, la cual es considerada de carácter especial, dentro de un plazo máximo de quince (15) días, contados a partir de la fecha del vencimiento del plazo para presentar las respectivas evaluaciones de carácter general. Este tiempo podría ser utilizado para que el empleado pueda autocapacitarse o pueda solicitar una nueva capacitación a su jefe inmediato o al oficial de cumplimiento según cada caso.

—Registro de asistencia a capacitación

Los empleados deben firmar, como mínimo una sola vez, al ingreso a la empresa, la constancia de capacitación, lectura, comprensión y compromiso de aplicación del código de ética y conducta y del manual SARLA/FT. El original de esta constancia deber quedar archivada en la carpeta del empleado que se encuentra bajo la custodia de recursos humanos en cabeza de su gerente, o un coordinador, de un jefe o quien cumpla sus veces.

La constancia de capacitación en SARLA/FT debe reposar en el área a cargo del oficial de cumplimiento. Estas constancias deben ser archivadas en orden alfabético.

Los formatos deben ser diligenciados, por cada empleado, en todos sus campos y no aceptar formatos con enmendaduras, tachones o similares.

—*Medios*

Las capacitaciones a empleados pueden ser presenciales, vía telefónica, por el sistema de videoconferencia utilizando la red interna, por medio de Internet o intranet. Puede ser con ayuda de medios escritos como el papel, CD, DVD, cintas, memorias, discos, libros, folletos, videos, grabaciones estereofónicas o similares, o mediante el envío de avisos, presentaciones, diapositivas, archivos electrónicos, clips, en todas sus formas, tanto escritas como electrónicas. En todos estos casos, el empleado debe recibir y/o ver el contenido de la capacitación para efectos de una mejor comprensión en cualquiera de los medios antes descritos.

Una vez ejecutada la capacitación, en señal de constancia se deben dejar los programas escritos y todo el material visual utilizado en la capacitación.

—*Capacitadores*

Las capacitaciones en materia del SARLA/FT pueden ser dictadas o impartidas por el oficial de cumplimiento de conformidad con su función de “coordinar el desarrollo de programas internos de capacitación”. Las capacitaciones también pueden ser realizadas por cualquiera de los miembros del comité evaluador de operaciones o quien esta designe.

Los capacitadores deben revisar constantemente los programas de capacitación y, en caso de encontrar oportunidades de mejoramiento, se deben actualizar dichos programas.

Las oportunidades de mejoramiento pueden surgir como consecuencia de la detección de posibles fallas en la capacitación, incomprensión de los temas por parte de los empleados, por uso técnico del lenguaje que dificulta su aprendizaje, por los resultados observados en las evaluaciones, por cambios en la normatividad interna, por cambios en la normatividad

externa nacional o internacional, por los conceptos entregados por asesores internos o externos, o conceptos de entidades competentes.

Estos programas de capacitación pueden ser revisados y actualizados conforme ocurran eventos de riesgo LA/FT que ameriten utilizar la capacitación como una forma de dar tratamiento al riesgo o de imponer un control al mismo.

Los programas de capacitación también son susceptibles de mejoramiento y, por ende, deben ser actualizados, a petición de la junta directiva, o de cualquier otro funcionario integrante del comité evaluador.

—Periodicidad

Para todos los empleados y/o funcionarios se debe impartir capacitación sobre aspectos relacionadas con el SARLA/FT por lo menos una vez al año.

De igual forma, a todos los empleados nuevos y a los terceros (funcionarios no empleados de la entidad) se les debe dar capacitación como proceso de inducción a los contenidos del SARLA/FT relacionados con sus funciones y responsabilidades dentro del SARLA/FT.

2. CARACTERÍSTICAS DE LA ORGANIZACIÓN Y SU ENTORNO

El primer paso y, por tanto, el más importante es diagnosticar el contexto organizacional de la prevención y control del LA/FT, es decir, conocer las características de la organización y su entorno, para de esta manera asegurar el éxito del diseño e implementación del SIPLA/FT o del SARLA/FT.

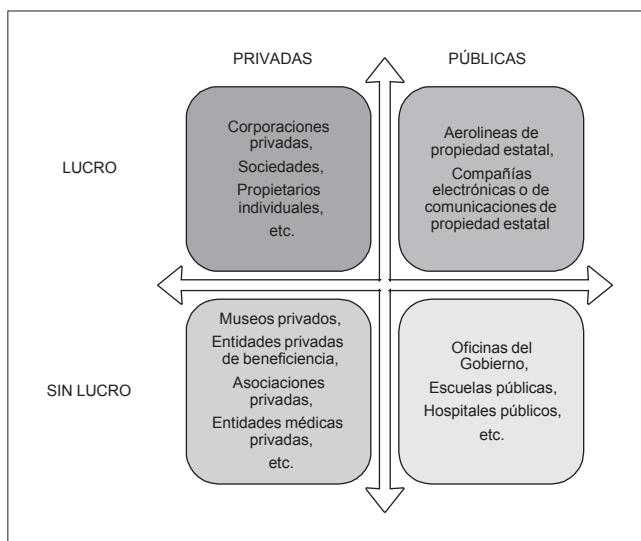
Este tema tiene como objetivos ambientar al lector en lo organizacional y responder a la pregunta de nuestra metodología: ¿dónde debo buscar y hallar eventos de riesgo de LA/FT?

Para nuestros propósitos, los eventos de riesgo de LA/FT se pueden encontrar dentro o fuera de la empresa y se pueden presentar en cualquiera de los siguientes cuatro tipos de organizaciones:

- a) Organizaciones privadas con ánimo de lucro;
- b) Organizaciones públicas con ánimo de lucro;
- c) Organizaciones privadas sin ánimo de lucro, y
- d) Organizaciones públicas sin ánimo de lucro.

En el siguiente diagrama citamos algunos ejemplos de cada tipo:

Gráfico 3
Tipo de organizaciones



Las características de los valores organizacionales que practican las empresas y los sistemas que tengan son determinantes para su vulnerabilidad al riesgo de LA/FT, al igual que las políticas, procesos y actividades de prevención y control que deben implementar tanto en SIPLA/FT como en SARLA/FT.

2.1. Adaptación de la empresa a su entorno (perspectiva del LA/FT)

Cualquier tipo de empresa u organización desarrolla su actividad en un entorno que la expone a muchos tipos de riesgos, entre ellos el del

lavado de activos y financiación del terrorismo; sin embargo, ese mismo entorno le ofrece oportunidades para mejorar sus sistemas de control.

Si estos riesgos no son enfrentados adecuadamente, en particular el del LA/FT, la organización tiene serias posibilidades de ver frenado su crecimiento e incluso puede desaparecer.

Cada organización tiene objetivos y estrategias explícitas, normas internas y externas definidas, una estructura de constitución formal, claras líneas de comunicación y autoridad y está organizada preferencialmente por procesos o por funciones; es en estos elementos donde se presentan debilidades para contrarrestar las amenazas de LA/FT y fortalezas para enfrentarlo.

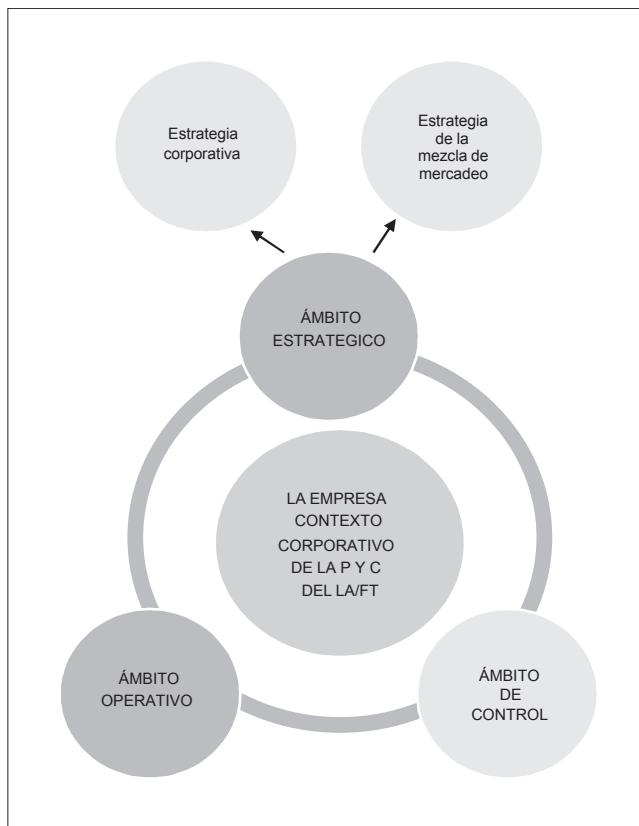
El o los responsables de la planificación, implementación, ejecución y monitoreo del SIPLA/FT o SARLA/FT en la organización deben conocer detalladamente cada una de sus políticas, las áreas, los procesos que ejecuta, los recursos que utiliza, los productos o servicios que ofrece, los mercados que atiende, la normatividad que la rige, es decir, debe tener una comprensión integral de ella. Sólo este conocimiento le permitirá hallar vulnerabilidades al riesgo de LA/FT y le facilitará diseñar políticas, metodologías y procedimientos eficientes y eficaces para la prevención y control del riesgo de LA/FT.

2.2. **Diagnóstico de la prevención y control del LA/FT en la empresa**

2.2.1. *Diagnóstico de fortalezas y debilidades*

Para realizar el diagnóstico de fortalezas y debilidades se debería desagregar la empresa al menos en tres ámbitos: ámbito estratégico, ámbito de control y ámbito operativo.

Gráfico 4
Contexto corporativo de la prevención y control del lavado de activos y financiación del terrorismo



—*El ámbito estratégico*

El ámbito estratégico a su vez está integrado por: la estrategia corporativa y la estrategia de la mezcla de mercadeo. A su vez, la corporativa comprende:

- Los procesos de divulgación y comunicación interna que se podrían utilizar para difundir información sobre el SIPLA/FT o el SARLA/FT.
- La misión definida para la empresa.

- La visión.
- Los objetivos estratégicos corporativos preferencialmente expresados en un mapa de objetivos estratégicos.
- Los preceptos de gobierno corporativo.

Gráfico 5
Elementos de la estrategia corporativa



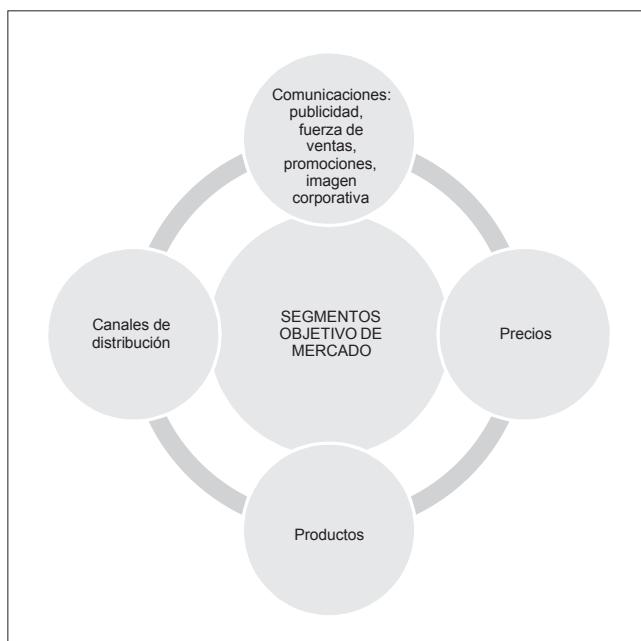
- La actitud de la alta gerencia hacia el control y en especial hacia la prevención y control del LA/FT.
- Los proveedores de todo tipo de insumos.
- Los sistemas de logística de almacenamiento, transporte y distribución.
- Los entes de vigilancia y control oficial.
- Los *stakeholders* o partes interesadas en la organización.

- La estructura organizacional.
- Las normas internas y externas.
- La actitud hacia el cambio y la innovación.

Por otro lado, está la *estrategia de la mezcla de mercadeo*, donde seguramente hallaremos las mayores vulnerabilidades de la organización al riesgo del LA/FT, porque allí se encuentran los principales factores de riesgo de LA/FT, tales como:

- a) Los clientes en el diferentes segmentos objetivo de mercado, tanto nacionales como internacionales;
- b) Los productos o servicios de la empresa;
- c) Los canales de distribución, y
- d) El recurso humano de la organización.

Gráfico 6
La estrategia de la mezcla de mercadeo

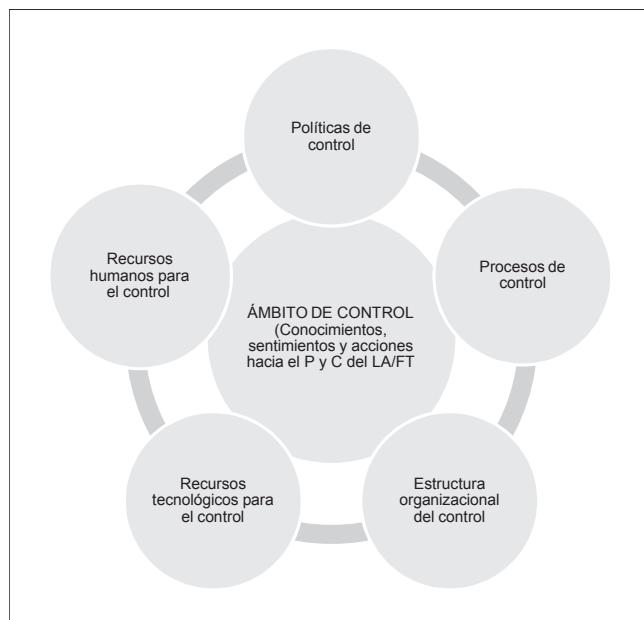


—*El ámbito de control*

Este ámbito está conformado por:

- El nivel de conocimiento, sentimientos y acciones de todos los funcionarios de la empresa, en particular los del área de control interno y revisoría fiscal hacia el control general y hacia el LA/FT.
- Las políticas de control interno.
- Los procesos de control interno.
- La estructura organizacional de control dispuesta por la organización que debe incluir las funciones y responsabilidades.
- Los recursos tecnológicos para control asignados por la empresa.
- Los recursos humanos para control disponibles.

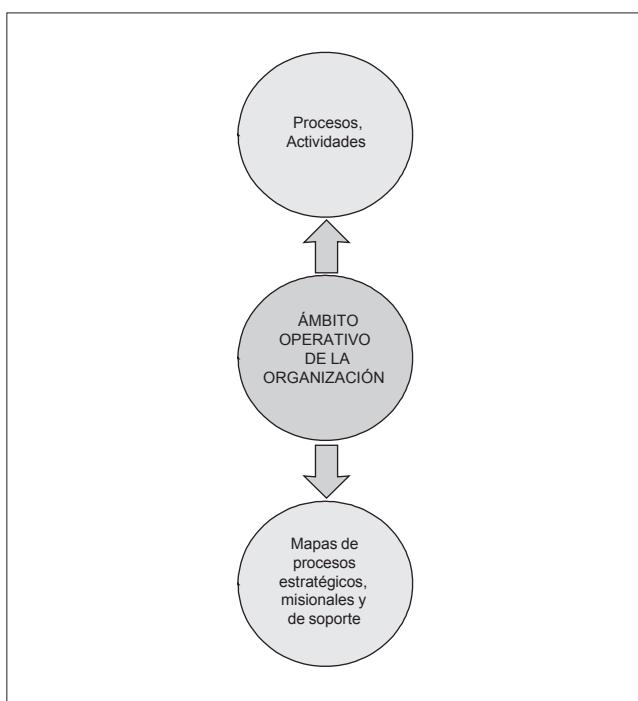
Gráfico 7
Ámbito de control



—Ámbito operativo

El tercer ámbito es el operativo, que se refiere a los procesos estratégicos, misionales (procesos claves) y de soporte y a las actividades ejecutadas por la empresa en cualquiera de sus áreas funcionales para alcanzar el logro de la misión y su visión.

Gráfico 8
Ámbito operativo



2.2.2. *Amenazas del entorno por riesgo de LA/FT*

Son retos presentados por acciones de delincuentes que, ante la ausencia de acciones de prevención y control del LA/FT, conllevarían impactos negativos para la empresa como el estancamiento y su consecuente desaparición.

Las amenazas son situaciones externas a la organización relacionadas con el delito de LA/FT que pueden atentar contra ella, por lo que, llegado al caso, puede ser necesario diseñar una acción adecuada para poder sortearla.

Ante esos retos, es necesario responder seriamente la pregunta: ¿en caso de materializarse el riesgo de LA/FT, se podría impedir parcial o totalmente la actividad de la empresa?

2.2.3. *Oportunidades del entorno para enfrentar el riesgo de LA/FT*

Son aplicativos de *software*, de *hardware*, metodologías, conceptos, sistemas, enfoques que la empresa puede encontrar en los mercados correspondientes para implementar o volver más eficientes sus sistemas de control, especialmente el de LA/FT.

Algunas de las preguntas que se pueden realizar y que contribuyen a su identificación son:

¿A qué buenas oportunidades de mejoramiento de la prevención y control del riesgo de LA/FT se enfrenta la empresa?

¿Cuáles son las mejores prácticas de prevención y control del LA/FT que se conocen?

¿Qué cambios de tecnología para la prevención y control del LA/FT se están presentando en el mercado?

¿Qué cambios en la normatividad legal sobre prevención y control del LA/FT se están presentando?

Las amenazas y oportunidades por lo general se encontrarán en el entorno y particularmente en los elementos que conforman la estrategia de mercadeo.

2.2.4. *Fortalezas internas de la empresa para la prevención y control del LA/FT*

Las fortalezas son todos aquellos elementos internos y positivos de que dispone la organización que se caracterizan por su efectividad para enfrentar las amenazas de LA/FT; generalmente se refieren a políticas, procesos, recursos, actitudes, mecanismos e instrumentos que se poseen.

2.2.5. *Debilidades internas de la empresa para la prevención y control del LA/FT*

Las debilidades se refieren, por el contrario, a todos aquellos elementos, recursos, habilidades y actitudes que la empresa tiene y que constituyen barreras para lograr una eficiente y eficaz prevención y control del riesgo de LA/FT. Son problemas internos que, una vez identificados, se pueden y deben eliminar.

Las debilidades o fortalezas siempre estarán referidas a los ámbitos estratégico, operativo y de control de la empresa

Algunas de las preguntas que se deberían formular para determinar las fortalezas y debilidades son:

¿Qué sistemas o recursos posee la empresa para enfrentar el riesgo de LA/FT?

¿Cuál es su nivel de efectividad?

¿Cuál es la disponibilidad y cantidad de esos recursos?

¿Cuál es el contenido de las políticas?

¿Incluyen la prevención y control del LA/FT?

¿Cuál es la opinión que tiene la alta gerencia y los funcionarios hacia el delito de LA/FT?

¿Cuál es la probabilidad de que en la empresa se materialice un evento de riesgo de LA/FT?

¿Qué se puede mejorar en la prevención y control del LA/FT?

El SIPLA/FT está relacionado con el riesgo legal y de deterioro de reputación a que se exponen las entidades, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera, al ser utilizadas, entre otros, para el ocultamiento, manejo, inversión o aprovechamiento, en cualquier forma, de dinero u otros bienes provenientes de actividades delictivas o destinadas a ellas, o para dar apariencia de legalidad a los mismos.

Algunas de las entidades mencionadas están obligadas a implementar el SIPLA/FT. Otras, tan solo a reportarle a la Unidad de Información y Análisis Financiero (en adelante UIAF) del Ministerio de Hacienda de Colombia las operaciones sospechosas (en adelante OS) que detecten.

2.3. Vulnerabilidad de la empresa al riesgo de LA/FT

Si se quiere ser más exhaustivo, se recomienda efectuar un análisis más completo de la vulnerabilidad de la empresa hacia el riesgo del LA/FT, utilizando la técnica del DOFA (debilidades, oportunidades, fortalezas y amenazas). Cuanto más completas sean las respuestas, mejor conocimiento se tiene del nivel de vulnerabilidad.

El SARLA/FT abarca todas las actividades que realiza la empresa en el desarrollo de su objeto social dentro de las políticas establecidas por la junta directiva. Además, se aplica a todos los macroprocesos de dirección, realización (misionales) y apoyo definidos para la organización en el desarrollo de sus actividades, en los cuales se deben identificar los eventos de riesgo de LA/FT ocurridos y posibles.

Este libro orienta las acciones a seguir para la identificación y administración del riesgo de lavado de activos y de la financiación del terrorismo durante el desarrollo de los procesos del negocio en la empresa.

La responsabilidad por la aplicación correcta del SARLA/FT está a cargo del jefe de cada proceso como encargado del control de gestión en su respectiva área o unidad de trabajo.

La misión del gerente de riesgos será evaluar y comprobar permanentemente el funcionamiento de los diferentes controles establecidos por la empresa para proteger sus recursos y optimizar su gestión.

Diseñar e implementar el SARLA/FT o el SIPLA/FT en cualquier organización no sólo requiere conocer las etapas que se deben seguir para gestionarlo, además es definitivo conocer las debilidades que tiene la empresa para ser permeada por delincuentes que pretenden lavar dinero a través de ella debido a las características de su entorno interno y las que puedan provenir del entorno externo y las fortalezas que tiene la empresa para defenderse.

Antes de iniciar el diseño del SARLA/FT o del SIPLA/FT, con miras a conocer las debilidades y fortalezas, debemos tener respuestas seguras a preguntas precisas. Las preguntas que hacemos son muchas más, pero en aras de la brevedad nos limitamos a plantear como ejemplos las siguientes:

¿La misión de la empresa hace consideraciones sobre su responsabilidad social ante el delito del LA/FT?

¿En la visión, valores organizacionales y principios organizacionales se hace referencia al LA/FT?

¿Cuáles son los productos o servicios que exponen a la empresa al riesgo de LA/FT?

¿A qué mercados y segmentos objetivo están dirigidos?

¿Cuál es la cobertura geográfica de las operaciones de la empresa?

¿Cuál es el nivel de exposición de esas áreas geográficas al riesgo de LA/FT?

¿Posee la empresa operaciones en esas áreas? (Obviamente son más vulnerables las empresas que operan servicios financieros en áreas geográficas de mercado impactadas por los delitos de LA/FT).

¿Las operaciones comerciales de la organización se realizan solamente en el mercado nacional o también con el exterior? (exportaciones-importaciones).

¿La organización está gerenciada mediante procesos? (Es más fácil identificar eventos de riesgo de LA/FT en empresas que tienen procesos adecuadamente documentados).

¿Existe dentro de la organización la cultura de gestión por riesgos? (Si existe, sería más fácil diseñar e implementar el SARLA/FT o el SIPLA/FT).

¿Cuáles son las formas que utilizan los clientes para cancelarle a la empresa sus facturas?

¿Cuáles son las políticas que se tienen sobre conocimiento de clientes?

¿Cuáles son los objetivos estratégicos que se verán afectados en caso de que se materialice un evento de riesgo de LA/FT?

¿Posee la empresa manuales que identifican y documentan los procesos direccionales, los misionales y los de apoyo? (Si no, es recomendable abordar este dispendioso trabajo).

¿Tiene la organización política sus procesos correspondientes consistentes para evitar el fraude en sus operaciones? ¿En ellas existen consideraciones con respecto al LA/FT?

¿Cuál es el nivel de desarrollo actual de los sistemas de control en la empresa? ¿Existe una estructura organizacional que se pueda utilizar como base para la estructura organizacional y de sistemas que requiere el SARLA/FT o el SIPLA/FT?

¿Cómo es la estructura organizacional de control interno de la empresa?

¿Posee la organización un recurso tecnológico que permita manejar técnica y eficientemente la información que produce el SARLA/FT o el SIPLA/FT?

3. POLÍTICAS PARA LA PREVENCIÓN Y CONTROL DEL LA/FT

Las organizaciones, bien en cumplimiento del SIPLA/FT o del SARLA/FT, deben trazar políticas relacionadas con:

La naturaleza, objeto social y cobertura de las actividades que realiza.

El cumplimiento de los reglamentos internos y de todas las disposiciones relacionadas con el SIPLA/FT.

Los clientes y operaciones con personas que no estén plenamente identificadas.

La vinculación de clientes que por su perfil o por las funciones que desempeñan podrían exponer en mayor grado a la entidad al riesgo de LA/FT.

La colaboración con la administración de justicia.

La reserva de la información recaudada y reportada.

La prevención y resolución de conflictos de interés que puedan presentarse en la aplicación del SIPLA/FT.

Las sanciones por incumplimiento a las normas relacionadas con el SIPLA/FT.

A la concordancia con los estándares internacionales sobre la materia, particularmente los pronunciados por GAFI y GAFISUD.

La cultura organizacional en materia de prevención y control del LA/FT.

La determinación del riesgo implícito en las operaciones que realicen con personas naturales o jurídicas de países que no aplican las recomendaciones formuladas por el GAFI y GAFISUD o los aplican en forma insuficiente y, así mismo, establecer el procedimiento a seguir para controlar y/o minimizar el riesgo potencial identificado.

El control y canales de comunicación entre la oficina principal y sus sucursales y subsidiarias o relacionadas, e instancias de reporte y consul-

ta entre el oficial de cumplimiento y todas las dependencias de la institución.

La conservación de documentos.

Las empresas, para implementar el SARLA/FT, deben diseñar e implementar cuatro tipos de políticas: 1. Políticas generales para la gestión del SARLA/FT, 2. Políticas específicas para impulsar la cultura de prevención y control del riesgo LA/FT en la empresa, 3. Políticas específicas para cada etapa del SARLA/FT. 4. Políticas para los mecanismos e instrumentos de la etapa de control.

A manera de ejemplo, en los puntos 3.1. a 3.6. se clasifican algunas políticas.

3.1. **Políticas generales para la gestión del SARLA/FT**

Con el fin de asegurar el adecuado funcionamiento del SARLA/FT, se proponen las siguientes políticas generales que son reglas de conducta y procedimientos para orientar la actuación en cuanto a la gestión del riesgo:

En la empresa se reconoce que la materialización de un evento de riesgo relacionado con el LA/FT atenta contra la empresa al generar pérdidas que afectan el logro de sus objetivos corporativos.

En la empresa el SARLA/FT tiene como objetivos la prevención de que no sea utilizada para realizar cualquier tipo de operación de lavado de dinero y detectar y el reporte oportuno de esas operaciones cuando acontezcan. La prevención y el control se refieren a las dos fases consideradas por las normas de la Superintendencia Financiera de Colombia.

En la empresa se reconoce que el lavado de activos y la financiación del terrorismo representan una gran amenaza para la estabilidad del sistema financiero y la integridad de los mercados por su carácter global, y, consciente de ello, debe implementar el SARLA/FT con el fin de prevenir y controlar que sea utilizada para dar apariencia de legalidad a activos provenientes de actividades delictivas o para la canalización de recursos

hacia la realización de actividades terroristas; por tal motivo, la junta directiva y la alta gerencia de la entidad consagrará en el manual la necesidad y exigirán a todos los funcionarios que antepongan el cumplimiento de las normas en materia de administración de riesgo de LA/FT al logro de las metas comerciales.

Para el logro de los objetivos de prevención y control, la empresa posee políticas, procedimientos, mecanismos e instrumentos para identificar, evaluar, controlar y monitorear eventos de riesgo.

El sistema de administración del riesgo de lavado de activos y de la financiación del terrorismo debe realizarse bajo el esquema de gestión por procesos conforme al ciclo PHVA.

Para la empresa, los objetivos de la implementación del SARLA/FT son:

Proteger a la empresa de las pérdidas e impacto que puedan generar los eventos del riesgo de lavado de activos y de la financiación del terrorismo.

Contribuir a la efectividad y eficacia de la empresa para el logro de su misión y objetivos corporativos.

Cumplir con los requerimientos legales establecidos por la Superintendencia Financiera de Colombia en el capítulo XIII de la Circular Externa 100 de 1995.

La junta directiva, directivos, funcionarios y empleados están comprometidos con la gestión de riesgos, y por tanto deben impulsar la cultura de la gestión del SARLA/FT.

La junta directiva es el único organismo que tiene facultad para designar el responsable de la implementación del SARLA/FT.

La junta directiva, directivos, funcionarios y empleados deben asegurar el cumplimiento de las normas internas y externas relacionadas con la gestión del SARLA/FT.

La junta directiva debe permitir la prevención y resolución de conflictos de interés en la recolección de información en las diferentes etapas del SARLA/FT, especialmente para el registro de evento de riesgo de LA/FT.

La junta directiva debe permitir la identificación de cambios en los controles y perfiles de los eventos de riesgo de LA/FT.

Los controles aplicados a los eventos de riesgo de LA/FT deben ser aprobados por la gerencia y por la junta directiva.

La junta directiva es el órgano que tiene la decisión final para tomar medidas a fin de prevenir y controlar el evento de riesgo de LA/FT.

La gestión del SARLA/FT siempre deberá estar integrada a la planeación estratégica de la empresa.

Todos los eventos de riesgo de LA/FT identificados en la empresa y seleccionados como de mayor prioridad deberán estar controlados mediante un plan de tratamiento.

El comité de riesgos estará adscrito a la junta directiva de la empresa y en ningún caso podrá pertenecer a áreas operativas u otras que generen conflictos de interés.

Todos los funcionarios y empleados de la empresa deben recibir inducción y capacitación sobre riesgo de LA/FT.

Todas las personas vinculadas a la empresa deben estar comprometidas con la adecuada administración del SARLA/FT, según su nivel jerárquico.

En la ejecución (hacer) del proceso SARLA/FT también se deben desarrollar y aplicar los conceptos y secuencias del ciclo PHVA, para establecer el riesgo inherente y su consecuente riesgo residual; es decir, el ciclo PHVA debe servir para determinar e implementar el tratamiento de evento de riesgo de LA/FT que permita minimizar el riesgo inherente - riesgo residual.

Para una efectiva administración del riesgo de LA/FT, el SARLA/FT debe ser gestionado, entre otros, mediante procesos interrelacionados (sistema) que deben contribuir al logro de la prevención y control de los eventos de riesgo de LA/FT de la empresa.

Todo proceso involucrado en la gestión del SARLA/FT debe tener una autoridad, uno o varios responsables y uno o varios ejecutores.

Una misma persona podrá ejercer la autoridad, la responsabilidad y/o la ejecución de un proceso.

Una misma persona podrá ejercer autoridad, responsabilidad y/o ejecución compartida en varios procesos.

A quien se le asigne la autoridad de un proceso se debe denominar gerente del proceso y a quien se le asigne la responsabilidad se le debe denominar administrador del proceso.

La alta dirección de la empresa debe demostrar su compromiso con la cultura de la prevención y control del LA/FT y con la implementación del SARLA/FT, favoreciendo decisiones orientadas a asegurar la disponibilidad de recursos esenciales (recurso humano, habilidades especializadas, infraestructura organizacional, recursos tecnológicos y financieros), para establecer, implementar, mantener y mejorar el SARLA/FT.

Todos los directivos, funcionarios y empleados que ingresen a la empresa mediante contrato laboral y de cualquier otro tipo, antes de comenzar a desempeñar las funciones de su cargo y dentro del proceso de inducción, deben recibir obligatoriamente y sin excepción capacitación en los propósitos y contenido del SARLA/FT.

Todas las capacitaciones realizadas deberán ser evaluadas.

El oficial de cumplimiento y el gerente de riesgos, en el proceso de gestión del SARLA/FT, siempre buscarán un común acuerdo en cuanto a posiciones conceptuales, metodológicas, instrumentales y éticas, para beneficio de la empresa.

La empresa no tendrá o dará por terminadas las relaciones comerciales y/o laborales con personas naturales o jurídicas vinculadas por las autoridades policivas en actividades delictivas, LA/FT y/o aquellas que se encuentren reportadas en las listas ONU, OFAC o Clinton y demás listas vinculantes para Colombia o en listas que tengan razones objetivas para no prestar los servicios a clientes y usuarios descritas en el manual y se procederá según lo descrito en los procedimientos de conocimiento de usuarios, clientes y agentes económicos.

Las diferencias conceptuales, metodológicas, instrumentales y éticas que resultaren de la intervención del oficial de cumplimiento y del gerente de riesgos en el proceso de gestión del SARLA/FT, en búsqueda de un común acuerdo, serán sometidas en primera instancia a consideración y decisión de la gerencia general y en última instancia ante la junta directiva.

Todos las diferencias generadas en el ejercicio de la autoridad, responsabilidad y de ejecución que surjan entre funcionarios a partir de la implementación del SARLA/FT se deberán resolver utilizando preferencialmente los conceptos y metodologías expuestas en el manual y en última instancia recurriendo a expertos externos a la empresa.

3.2. Políticas específicas para impulsar la cultura de prevención y control del riesgo LA/FT en la empresa

La cultura organizacional en prevención y control de LA/FT es el conjunto de políticas, hábitos y valores que deben practicar todos los directivos, funcionarios y empleados en la empresa, para evitar que esta sea utilizada activa o pasivamente en operaciones de lavado de activos y de financiación del terrorismo.

La cultura antilavado y antifinanciación del terrorismo debe ser expresada por los directivos, funcionarios y empleados vinculados a la empresa, mediante sus actitudes.

Las actitudes ante el delito de LA/FT y ante las medidas de prevención y control de esos delitos tienen tres componentes:

Tabla 3
Componentes de una actitud

Componentes actitudinales	Pasos de la cultura	Delito LA/FT	Antidelito LA/FT
Cognoscitivo	Conocer	Lo que sé	Lo que sé
Afectivo	Sentir Preferir	Lo que siento	Lo que siento
Comportamental	Actuar	Lo que hago	Lo que hago

Una actitud describe las evaluaciones cognoscitivas permanentes, favorables o desfavorables de una persona, los sentimientos y las tendencias de acción hacia los sistemas de prevención y control de LA/FT.

Una política, aplicada a los temas de gestión de riesgo de LA/FT, es todo lo que está escrito y aprobado, que rige a la empresa y que debe ser respetado por todos sus integrantes. Las políticas anti LA/FT deben estar escritas detalladamente en el manual del SARLA/FT y en los manuales de procesos y procedimientos y manuales de funciones, planes de capacitación y planes estratégicos, entre otros.

El fortalecimiento de la cultura se debe realizar mediante el diseño e implementación de políticas y actividades para la prevención y control del riesgo de LA/FT.

La empresa no vinculará a ningún tipo de funcionario que haya sido relacionado de manera cierta o no con actividades de lavado de activos o financiación del terrorismo.

Los valores de la organización siempre deberán estar direccionados a la prevención y control del lavado de activos y la financiación del terrorismo.

La actividad de prevención y control de LA/FT siempre deberá primar sobre cualquier otro tipo de medidas de prevención y control.

Los intereses económicos de la organización nunca podrán primar sobre los intereses relacionados con la prevención y control del lavado de activos y la financiación de terrorismo.

Ninguna persona vinculada a la empresa, cualquiera que sea su rango jerárquico, podrá ser eximida de actividades de capacitación en prevención y control de LA/FT.

Cualquier persona vinculada a la empresa, quien manifieste, de manera comprobada por el oficial de cumplimiento o la alta gerencia, un sentimiento afectivo a favor del delito de LA/FT será retirada de manera inmediata de la empresa.

Toda actividad propuesta para el fortalecimiento de la cultura de prevención y control del riesgo de LA/FT deberá recibir el total apoyo político y económico de las directivas de la empresa, previa su evaluación. Por tanto, la alta gerencia de la empresa debe demostrar su compromiso con la cultura de la prevención y control del LA/FT y con la implementación del SARLA/FT, tomando y favoreciendo decisiones orientadas a asegurar la disponibilidad de recursos esenciales (recursos humanos, habilidades especializadas, infraestructura organizacional, recursos tecnológicos y financieros), para establecer, implementar, mantener y mejorar el SARLA/FT.

3.3. Políticas específicas para cada etapa del SARLA/FT

La empresa debe cumplir con las siguientes políticas al implementar cada una de las etapas del SARLA/FT.

3.3.1. *Para la identificación de eventos de riesgo de LA/FT*

La identificación de evento de riesgo de LA/FT siempre debe efectuarse teniendo en cuenta los siguientes factores de riesgo (agentes generadores del riesgo de LA/FT):

- a) Clientes/usuarios;
- b) Productos;
- c) Canales de distribución, y
- d) Jurisdicciones

Para la segmentación de los factores de riesgo, siempre se debe utilizar la metodología definida por la empresa y consignada en los instrumentos del manual.

En todo tipo de análisis sobre riesgo de LA/FT se considera que un evento de riesgo de LA/FT impacta a una UE.

La detección de un evento de riesgo de LA/FT se realizará siempre en los procesos de dirección estratégica, realización y apoyo definidos en el mapa de procesos de la empresa, contenidos en el manual.

El gerente de riesgos y los administradores de los procesos son los responsables de identificar y gestionar los eventos de riesgo de LA/FT del o los procesos a su cargo descritos en el manual.

Los cambios en la ejecución de los procesos o en la oferta de nuevos servicios deben ser reportados anticipadamente a la gerencia de riesgos.

Todo el personal vinculado a la empresa puede identificar un evento de riesgo de LA/FT, el cual debe ser reportado al comité evaluador de operaciones por los medios que este determine en un plazo no superior a 5 días después de detectados.

Todo evento de riesgo de LA/FT identificado y reportado al comité evaluador de operaciones debe ser descrito a partir de sus causas, factores de riesgo, situaciones de riesgo, riesgos asociados e impactos.

Toda operación calificada como sospechosa, en los términos definidos por la SFC y en el manual, para todos los productos ofrecidos por la empresa, debe ser considerada como evento de riesgo de LA/FT.

3.3.2. *Para la medición de eventos de riesgo de LA/FT*

Para todos los eventos de riesgo de LA/FT identificados se debe aplicar únicamente la metodología de medición definida por la gerencia de riesgos.

La calificación (valoración) de los eventos de riesgo de LA/FT se realiza en forma centralizada por parte de la gerencia de riesgos.

La gerencia de riesgos es la única entidad de la empresa autorizada para establecer metodologías para medición de frecuencias, impactos y calificación de eventos de riesgo de LA/FT. Además es la única entidad responsable de definir los criterios que permitan seleccionar el impacto que más dificulte el logro de los objetivos estratégicos de la empresa. Igualmente es responsable de calcular y justificar la probabilidad de ocurrencia de un evento de riesgo de LA/FT.

El nivel de severidad de un evento de riesgo de LA/FT es el resultado del producto de la frecuencia (probabilidad medida en una escala entre 1 y 5) multiplicado por el impacto considerado como más relevante (medido en una escala entre 1 y 5).

El gerente de riesgos y oficial de cumplimiento son las personas responsables de establecer la frecuencia de un evento de riesgo de LA/FT ocurridos y evento de riesgo de LA/FT posibles, para lo que deben, preferiblemente, recurrir a fuentes internas de información.

Para todo evento de riesgo de LA/FT se debe determinar el perfil de riesgo individual y consolidado.

3.3.3. *Para el control de eventos de riesgo de LA/FT*

Para todo evento de riesgo de LA/FT se debe establecer un nivel de exposición en razón de la calificación dada a los factores de riesgo en la etapa de medición.

Todo evento de riesgo de LA/FT debe tener un perfil de riesgo consolidado frente a todos los factores de riesgo y los riesgos asociados.

El control debe traducirse en una disminución de la posibilidad de ocurrencia y del impacto del riesgo de LA/FT en caso de materializarse.

La gerencia de riesgos y el oficial de cumplimiento, en coordinación con el comité evaluador de operaciones, son la autoridad y los responsa-

bles de tomar las decisiones adecuadas para cada uno de los eventos de riesgo de LA/FT identificados.

Los mecanismos e instrumentos utilizados para el SIPLA se integran a la etapa de control del SARLA/FT y, por tanto, deben ser considerados elementos de prevención y control.

Las medidas de control decididas deben ser actualizadas o reemplazadas si no son eficaces para prevenir y controlar el efecto de un evento de riesgo de LA/FT.

3.3.4. *Para el monitoreo de eventos de riesgo de LA/FT*

Para monitorear se debe:

Desarrollar procesos de seguimiento efectivo que faciliten la rápida detección y corrección de deficiencias en las etapas del SARLA/FT.

Realizar seguimiento del riesgo inherente y residual de cada factor de riesgo y de los riesgos asociados.

Realizar seguimiento del riesgo inherente y residual consolidados. La consolidación debe darse entre los factores de riesgo y los riesgos asociados.

Asegurar que los controles sean comprensivos de todos los eventos de riesgo de LA/FT y que los mismos estén funcionando en forma oportuna y efectiva.

Establecer indicadores descriptivos y/o prospectivos que evidencien potenciales fuentes de riesgo de LA/FT.

Asegurar que los riesgos residuales se encuentren en niveles de aceptación establecidos por la empresa.

Permitir comparar la evolución del riesgo inherente con el riesgo residual de cada factor de riesgo y de los riesgos asociados, tanto en forma desagregada como consolidada.

Desarrollar reportes que permitan establecer evoluciones del riesgo, así como la eficiencia de los controles implementados.

Realizar un monitoreo a los perfiles de riesgo y las exposiciones a pérdidas de cada evento de riesgo de LA/FT por lo menos una vez cada seis meses.

Realizar seguimiento efectivo que permita detectar y corregir las deficiencias en el caso en que aplique.

Realizar seguimiento al comportamiento de los indicadores definidos dentro del SARLA/FT.

En la etapa de monitoreo, se garantizará que los controles estén funcionando de forma oportuna y efectiva y que los riesgos residuales se encuentran en los niveles adecuados de prevención y control establecidos por la organización.

3.4. Políticas específicas para los mecanismos e instrumentos de la etapa de control del SARLA/FT

3.4.1. *Para el conocimiento del usuario*

La empresa capturará información de todos sus usuarios y clientes durante la realización de cualquier operación comercial, solicitando los siguientes datos:

—Para personas naturales

- a) Nombres y apellidos;
- b) Tipo y número de identificación, y
- c) Domicilio y número telefónico.

—Para personas jurídicas

- a) Nombre o razón social;
- b) NIT - RUT;
- c) Domicilio y número telefónico de la empresa, y

- d) Tipo y número de identificación de quien actúa como representante legal.

La empresa podrá solicitar información adicional a los usuarios y clientes de sus servicios. Esta información adicional deberá ser capturada en un formulario único especial.

Todos los usuarios de las operaciones relacionados con los productos ofrecidos por parte de la empresa deberán utilizar el formulario especial. En él se tienen establecido los siguientes formatos:

- a) Formato de vinculación/actualización/entrevista (utilizado en el momento de pago de la operación). Con este formato se entiende vinculado el usuario o cliente, se entiende que se ha efectuado la actualización anual de los datos y se ha hecho entrevista presencial por parte del empleado;
- b) Comprobante de pago;
- c) Declaración en efectivo;
- d) Declaración de cambio (cuando es del caso);
- e) Declaración voluntaria de origen de fondos;
- f) Autorización de consulta y reporte a centrales de riesgo, y
- g) Datos de usuario y datos de apoderados según el caso.

3.4.2. *Para el conocimiento del cliente*

Para la empresa, el conocimiento del cliente no sólo es una obligación sino una de las principales medidas de control para que no sea utilizada como instrumento para el LA/FT. Por esta razón, es importante establecer las siguientes políticas de conocimiento del cliente (que se constituyen en un esfuerzo organizado para recolectar información relevante que permita detectar y analizar operaciones sospechosas):

Conocer a los clientes tiene dos propósitos generales: 1. Servir de medida disuasiva para alejar de la empresa a los lavadores de dinero. 2. Permitir la detección de operaciones inusuales y la determinación de operaciones sospechosas, que se deben reportar a las autoridades.

Las políticas de conocimiento del cliente para efectos de la prevención del lavado de activos son parte integral del negocio.

La información relevante sobre el cliente, para efectos de prevenir y controlar el lavado de activos, es la que sirve para establecer los siguientes aspectos: Identificación completa, actividad económica, procedencia u origen de los fondos, y volumen y características de las transacciones financieras.

En la empresa, se deben distinguir dos grandes categorías de personas: clientes y usuarios. Se entiende como *cliente* la persona natural o jurídica con la cual se tiene una relación contractual de carácter financiero. Esta relación puede ser de manera ocasional o permanente. El *usuario* es la persona natural o jurídica que tiene acceso a un número limitado de servicios de la empresa, pues no existe la relación contractual o, si existe, esta no genera un riesgo significativo.

La diferenciación entre cliente y usuario tiene como propósito establecer controles más estrictos para los clientes, debido a que estos tienen una relación más significativa con la empresa, pero al mismo tiempo mantener controles suficientes para los usuarios.

La empresa tiene criterios clasificadores para analizar sus operaciones y orientar los controles correspondientes. La primera clasificación lógica de los clientes obedece a la distinción entre personas naturales o jurídicas.

La identificación de las personas jurídicas requiere la solicitud de más información; no es suficiente contar con los mismos datos que suministraría la persona natural. Las personas jurídicas están compuestas por socios, pueden tener varios representantes legales y domicilios. Por esta razón, es importante ir más allá de los datos básicos y conocer algo más sobre las personas que dirigen y controlan a la persona jurídica. Adicionalmente, las transacciones comerciales, contables y financieras de las personas jurídicas son más complejas, por lo tanto se requiere mayor soporte documen-

tal para entenderlas.

Jurídicamente existe la posibilidad de nombrar apoderados para realizar operaciones con una empresa, en nombre de otra persona. Este tipo de operaciones requiere una doble identificación, pues es necesario identificar tanto al cliente como a su apoderado. Además, es necesario corroborar la validez y autenticidad del poder o el documento en el cual consta la designación del apoderado.

El conocimiento del cliente no es simplemente una obligación puntual que se cumple con el diligenciamiento de unos formatos. En la empresa, es una política que implica una acción planeada y coordinada entre varias de sus áreas, labor que se desarrolla en cinco instancias: vinculación del cliente, análisis de la información, prestación del servicio y actualización de datos.

Para desarrollar una política de conocimiento del cliente eficaz, la empresa debe realizar una labor continua y organizada que puede ser descrita mediante las siguientes etapas:

Vinculación del cliente. El momento más importante en este proceso es la vinculación del cliente. Se trata de su primera relación con la empresa, en la cual el cliente presenta su documentación y la empresa decide sobre su vinculación. Esta oportunidad es muy valiosa para aplicar la política de conocimiento del cliente y prevención del lavado de activos. Para efectos operativos y de control, se debe solicitar información básica como registros de firmas, fotocopias de documentos de identificación, direcciones de correspondencia, referencias, etc. A su vez, la política de conocimiento del cliente conlleva la solicitud y análisis de información complementaria que tiene como único fin evitar que la empresa sea utilizada para lavar activos o legitimar capitales.

Análisis de operaciones inusuales o sospechosas. La mejor fuente de información para realizar este estudio es aquella suministrada por el cliente al momento de vincularse. En consecuencia, un mecanismo que permita la consulta fácil de esta información es fundamental para el ágil desarrollo de la política de prevención al lavado de activos.

Análisis de la información suministrada. La empresa debe asegurarse de que la información esté completa y debe solicitar información adicional o explicativa, verificar ciertos datos y, finalmente, establecer que toda la información tenga sentido y sea coherente.

Prestación del servicio. La empresa debe identificar a las personas que realizan operaciones con ella, sin necesidad de repetir el proceso que se realizó a la hora de la vinculación del cliente.

Cuando se presta un servicio a un cliente ya vinculado, sobre el cual se ejerció la política de conocimiento del cliente, se pretende simplemente confirmar que la persona que realiza la transacción es efectivamente el cliente de la empresa. Lo anterior con los siguientes propósitos:

- Comparar la operación con el perfil del cliente y el segmento del mercado;
- Consolidar las operaciones periódicas del cliente para efectos de análisis y control;
- Confrontar los listados especiales (listas de clientes que no deben ser vinculados; por ejemplo, personas incluidas en las listas de la OFAC);
- Verificar las señales de alerta correspondientes, y
- Actualizar los datos. Es normal y previsible que los clientes de la empresa cambien algunas de sus características personales y financieras durante la duración de la relación contractual con la empresa. Los individuos y la empresa cambian de actividad económica, de domicilio, etc. Por esta razón, es importante actualizar en forma periódica y sistemática los datos suministrados por los clientes. De lo contrario, la confrontación de las operaciones realizadas con la información no actualizada del cliente puede inducir a creer que existen operaciones sospechosas donde no las hay o lo contrario.

Conocer al cliente implica recolectar y analizar información relevante sobre su identidad y su actividad económica. Esta información proviene de diferentes fuentes, públicas y privadas, y conforman un conjunto de datos que le sirven a la empresa para conocer el riesgo relativo de cada uno de

sus clientes frente a operaciones de lavado. A su vez, todos los documentos y los datos recolectados en desarrollo de esta política servirán de sustento para detectar operaciones sospechosas y encontrarles justificación a operaciones que aparecían como tal a primera vista. Por estas razones de peso, la empresa debe recaudar la información pertinente sobre sus clientes, de acuerdo con ciertas pautas, que se describen a continuación. De esta labor depende el éxito del control que con dicha información se puede ejercer.

Los aspectos o labores que conforman el conocimiento del cliente son:

- a) Identificación del cliente;
- b) Diligenciamiento de formularios;
- c) Solicitud de documentos de soporte;
- d) Verificación de datos;
- e) Consulta de listas especiales;
- f) Asignación del perfil y ubicación en el segmento del mercado;
- g) Selección del cliente;
- h) Anticipación de servicios y movimientos;
- i) Conservación y organización de la información;
- j) Consolidación de operaciones, y
- k) Actualización de datos y documentos.

En términos sencillos, identificar el cliente es asegurarse que la persona que se acerca a la empresa no es otra, es decir no es suplantada o está actuando con una identidad falsa. Esta labor se basa en el cotejo o comparación de la firma, la fotografía y la huella dactilar en documentos que se presumen auténticos, frente a los documentos presentados por el cliente o usuario.

Los documentos que habitualmente se utilizan para identificar per-

sonas naturales (físicas) son: partida de nacimiento, documentos de identidad, cédula electoral, licencia de conducción, pasaporte, tarjeta de seguridad social o registro civil. Para identificar las personas jurídicas se emplean los siguientes documentos: contratos sociales, estatutos, registro mercantil, documentos notariales, documentos de identificación tributaria, licencias o registros especiales.

Como mecanismo adicional se solicitan referencias personales, laborales, bancarias o comerciales que tienen el propósito de determinar la existencia real de la persona, vincularla con otros individuos o empresas, y facilitar la verificación de los datos básicos.

La empresa debe tener establecida una lista de documentos admisibles como identificación, según cada caso y de acuerdo con las normas

No basta con identificar a la persona, es necesario consignar sus datos básicos y su información financiera en formatos especialmente diseñados que permitan obtener un conocimiento adecuado del cliente.

Si bien la empresa podría practicar el principio de buena fe, la información suministrada por los clientes debe ser verificada y soportada en ciertos casos. Por esta razón, debe solicitar documentos originales (de soporte) para comprobar la veracidad de la información suministrada. La empresa debe conservar copias u originales de algunos de estos documentos como formatos, declaraciones, contratos, etc.

La obligación de verificar la información suministrada, de la cual se hizo referencia en el punto anterior, puede cumplirse de varias formas, según el riesgo que implique la transacción, la experiencia de la empresa y las posibilidades prácticas. En algunos casos, basta con consultar información pública y fácilmente disponible, como la guía telefónica, por ejemplo, para corroborar los datos suministrados por el cliente. En otros casos, la empresa considera necesario tomar medidas adicionales y visita al cliente en sus instalaciones para confirmar que la información suministrada es veraz. No es operativo ni pertinente visitar a todos los clientes como tampoco es prudente creer en toda la información suministrada por los clientes. La empresa debe ejercer su buen juicio, conforme a la legislación aplicable, para determinar el alcance de su política de verificación de información.

Para apoyar la labor de verificación de la información presentada por el cliente es de gran utilidad contar con otras fuentes de información que puedan ampliar estos datos, como por ejemplo las centrales de riego e información financiera, y las autoridades que certifican antecedentes judiciales, cuando esta información está disponible.

La empresa debe utilizar las listas especiales que diferentes autoridades expedir con el propósito de alertar sobre los antecedentes de ciertas personas o empresas. Estas listas deben ser utilizadas con sumo cuidado, pues la existencia de homónimos puede generar inconvenientes en su aplicación. Para efectos del narcotráfico, debemos utilizar las listas de la OFAC, dependencia del Departamento del Tesoro.

En algunos casos, el oficial de cumplimiento o el gerente de riesgos pueden determinar que no es conveniente vincular a un cliente, pues dentro de sus controles tienen un sistema de evaluación de factores de riesgo que les permite detectar desde el comienzo los clientes no deseados.

Una de las herramientas más eficaces para la detección de operaciones inusuales y sospechosas es la anticipación de las operaciones que el cliente tiene posibilidad de realizar según su actividad económica. Se trata de analizar la información financiera suministrada para determinar las características y el monto dentro de los cuales se deben enmarcar las operaciones del cliente en el futuro cercano.

La información que se recopila en desarrollo de la política de conocimiento del cliente tiene como propósito servir de sustento para el análisis de operaciones sospechosas. Por esta razón, debe prestarse especial atención a la conservación tanto de los documentos físicos como de los datos que se tengan en medio magnético sobre los clientes.

En algunos casos es suficiente una operación de un cliente para poder determinar que se trata de una operación sospechosa. No obstante, en la mayoría de los casos, es necesario apreciar la actividad del cliente en su conjunto para poder compararla con su perfil, el segmento del mercado al cual pertenece, las señales de alerta y los demás mecanismos de control establecidos para determinar que la operación es sospechosa.

Por esta razón, se debe consolidar el conjunto de operaciones de un cliente en un período fijo que normalmente corresponde a un mes calendario, para obtener una visión más completa de los movimientos del cliente y así poder analizarlos.

Algunos de los datos que el cliente suministra al momento de su vinculación tienen poca probabilidad de cambiar con el tiempo. Por el contrario, la información financiera es por esencia cambiante, y por tanto, es necesario actualizarla constantemente para poder analizar las operaciones del cliente frente a su perfil real. Muchas operaciones que a primera vista aparecen como sospechosas son el resultado de comparar operaciones de los clientes frente a perfiles desactualizados.

La política no debe mirarse como una actividad aislada que no cumple con los objetivos principales del negocio. Por el contrario, una política efectiva de conocimiento del cliente sirve de base para una exitosa gestión comercial y de administración del riesgo en la empresa.

Conocer al cliente nos permite conocer sus características como consumidor de servicios financieros, para ofrecer productos adicionales o no vedados. Los retos del mercado actual exigen que la empresa conozca las preferencias y los hábitos de consumo de sus clientes; toda esta información, debidamente analizada, permite personalizar y mejorar el servicio.

Ejercer la política de conocimiento del cliente no solamente previene y controla la ocurrencia de operaciones de lavado de activos, sino que puede evitar otros delitos como el fraude.

La esencia de la empresa con un negocio financiero es la administración del riesgo. Se debe realizar un seguimiento constante de las operaciones de los clientes, en particular y en su conjunto, para evaluar correctamente el riesgo y tomar acciones frente a otros riesgos como el fraude.

La política de conocimiento del cliente se relaciona con otros controles al lavado de activos. Cada uno de estos controles hace parte del sistema establecido para minimizar su exposición al riesgo de ser utilizada para lavar activos y colaborar con las autoridades en la prevención del delito.

En la empresa, el reporte de transacciones en efectivo, cuando este es exigido por el ente de control, es un control objetivo que consiste en diligenciar un formulario especial, en el cual se consigna información sobre las personas y la operación, cuando se realizan transacciones en efectivo por un monto superior al fijado por la SFC o por la junta directiva de la empresa. Este formulario tiene como propósito dejar constancia de las operaciones en efectivo significativas que los clientes y usuarios realizan.

El formulario en el cual se consignan las operaciones en efectivo no reemplaza la demás información que se debe tener sobre el cliente. A su vez, al conocer al cliente es importante definir si dentro del giro ordinario de los negocios del este está el manejo de grandes sumas de efectivo, para efectos de detectar operaciones inusuales.

Para poder *reportar una operación como sospechosa*, la empresa tiene que comparar el conjunto de operaciones del cliente con su perfil. Operaciones que resultan normales para determinados clientes pueden ser completamente sospechosas para otros.

En términos simples, *segmentar el mercado* es agrupar a los clientes de acuerdo con las características básicas de sus operaciones (volumen, frecuencia, productos, localización, etc.). La racionalidad de los negocios dicta que los clientes de un mismo segmento deben tener características económicas, contables y financieras similares. Es decir, que los datos recolectados al momento de conocer a nuestros clientes nos deben permitir asumir el segmento del mercado en el cual se situarán.

3.4.3. *Para el conocimiento de clientes especiales*

La empresa se debe abstener de iniciar relaciones comerciales con empresas en el exterior que no estén inscritas o registradas ante la entidad oficial del correspondiente país, que no estén facultadas para realizar un determinado tipo de operación y que no tengan procedimientos básicos para la prevención del lavado de activos.

—*Políticas para el análisis del perfil de riesgo del cliente*

La empresa debe diseñar mecanismos efectivos, eficientes y oportunos más exigentes respecto de las operaciones que realizan clientes catalogados como “riesgo alto y medio”.

La aprobación de la permanencia de este tipo de clientes deberá llevarse a cabo por un empleado de jerarquía superior previo estudio del comité o unidad pertinente.

—*Políticas para el monitoreo de clientes especiales*

La empresa determinará cuales operaciones resultan relevantes, teniendo en cuenta el nivel de exposición de riesgo y se basará en los criterios establecidos para este procedimiento.

—*Políticas específicas para las señales de alerta*

La empresa podrá anular o suspender operaciones o relaciones con agentes económicos ante la presencia de una o varias señales de alerta.

3.5. Políticas específicas para la capacitación

Las regulaciones sugieren que todos los directivos, funcionarios y empleados que ingresen a la empresa mediante contrato laboral y de cualquier otro tipo, antes de comenzar a desempeñar las funciones de su cargo y dentro del proceso de inducción, deben recibir obligatoriamente y sin excepción capacitación en los propósitos y contenidos del SARLA/FT.

La empresa debe diseñar, programar y coordinar por lo menos anualmente un plan de capacitación sobre el SARLA/FT dirigido a todas las áreas y funcionarios de la entidad. Adicionalmente, y en el evento de ingresos de personal, deberá darse una inducción y capacitación particular sobre el SARLA/FT.

El programa de capacitación debe constar por escrito y ser revisado y actualizado cuando se requiera por el oficial de cumplimiento en coordinación con el área administrativa de la entidad. Además, debe contar

con los mecanismos de evaluación de los resultados obtenidos con el fin de determinar la eficacia de dichos programas y el alcance de los objetivos propuestos.

Igualmente debe señalar su alcance, los medios que se emplearán para ejecutarlos y los procedimientos que se adelantarán para evaluarlos.

La capacitación y entrenamiento del personal se circumscribe a dar a conocer las normas que sobre prevención y control del riesgo del lavado de activos y de la financiación del terrorismo se tienen establecidas en la empresa y a mantener permanentemente actualizados a los funcionarios sobre las normas que regulan la materia. El no cumplimiento de esta política podría generar riesgos de tipo legal con posibilidad de contraer consecuencias o pérdidas por sanciones, tanto en forma interna, según lo indicado en el código de ética y conducta y lo indicado en el manual del SARLA/FT, como de forma externa, por parte de la Superintendencia Financiera de Colombia. Para evitar el riesgo anterior, la empresa debe establecer los siguientes controles:

De tipo preventivo. Planear los programas de divulgación, capacitación y de reuniones que se deben realizar como mínimo en forma anual. Dejar documentada la planeación de los programas por medios escritos o electrónicos. Establecer indicadores de cumplimiento: número de eventos realizados sobre el número de eventos programados.

De tipo detectivo. Hacer seguimiento a la ejecución de los programas. Dejar documentada, por escrito o en forma electrónica, el seguimiento o revisión a la ejecución de los programas. Documentar por escrito o en forma electrónica por medios tales como cintas magnéticas, grabaciones estereofónicas, videogramaciones, las capacitaciones y reuniones. Todo lo anterior para asegurar que durante el período se esté cumpliendo con lo programado.

De tipo correctivo. Revisar la documentación física o electrónica en forma posterior a la ejecución de las reuniones, capacitaciones, publicaciones, para asegurar que durante el período se haya cumplido con lo programado.

3.6. Políticas específicas de productos y servicios

La empresa debería establecer políticas SARLA/FT para los servicios ofrecidos a clientes/usuarios y agentes económicos.

Por ejemplo, estas políticas tendrían que ver con:

- a) La obligatoriedad de capturar y conservar la información relacionada con el ordenante y con el beneficiario;
- b) La definición de cliente en términos de la cantidad de operaciones realizadas por un mismo beneficiario o remitente en un determinado período de tiempo (el tiempo transcurrido como usuario);
- c) Limitaciones para el valor de la operación a realizar, el tipo de divisa en que se realiza la operación;
- d) La forma de pago de la operación que se realiza;
- e) El lugar de residencia y nacionalidad de quien realiza la operación;
- f) Los formatos que se deben utilizar para realizar la operación;
- g) Los tipos de documentos que deba acreditar el cliente para realizar la operación;
- h) Origen y destino de los fondos de la operación;
- i) Continuidad del cliente como usuario de los servicios;
- j) Realización de operaciones en efectivo;
- k) Al tipo de cliente que realiza la operación: cliente/usuario, y
- l) Valores máximos y mínimos de las operaciones.

3.7. Consideraciones básicas para la implementación de las políticas de prevención y control del LA/FT

3.7.1. *Diseño y aplicación de una metodología para la identificación de operaciones inusuales y diseño de controles que mitiguen el riesgo de LA/FT*

El SIPLA/FT o el SARLA/FT debe permitir efectuar una evaluación y análisis eficaz de las operaciones inusuales de los clientes de modo tal que pueda establecer si una operación escapa de lo simplemente inusual, y proceder a calificarla como sospechosa aplicando para ello las políticas y criterios previamente definidos por la entidad. Para estos efectos, el SIPLA/FT debe establecer el tipo de prueba documental que soporte los resultados del análisis y la evaluación realizada. Las metodologías que proponemos son las denominadas “espina de pescado” y de los “¿cinco por qué?”.

3.7.2. *Diseño de mecanismos e instrumentos para implementar el SIPLA/FT o el SARLA/FT*

—Mecanismos

- a) *Conocimiento del cliente* para la identificación de operaciones inusuales;
- b) *Conocimiento del mercado* para la identificación de operaciones inusuales;
- c) *Segmentación del mercado* para propósitos de prevención y control del LA/FT;
- d) *Segmentación de los factores de riesgo* en relación al mercado;
- e) A través de la segmentación de los factores de riesgo se deben determinar las características usuales de las transacciones comerciales que se desarrollan y compararlas con aquellas que realicen los clientes, a efectos de detectar las operaciones inusuales, y
- f) Determinación y reporte de *operaciones sospechosas*.

—*Instrumentos*

El SIPLA/FT de la empresa debe estar soportado en instrumentos que permitan ejecutar en forma efectiva, eficiente y oportuna los mecanismos de control previstos por la empresa para la prevención y control del LA/FT como los que se señalan a continuación:

Señales de alerta que permitan identificar operaciones inusuales utilizando las técnicas de segmentación de factores de riesgo y operaciones múltiples. Estas señales son los indicadores cualitativos y/o cuantitativos (tales como hechos, situaciones, eventos, cuantías o indicadores financieros, razones financieras) que le permiten a la empresa inferir o identificar comportamientos que se salen de los parámetros definidos previamente como normales. Además, aquellas deben considerar cada uno de los factores de riesgo y las características de sus operaciones, así como cualquier otro criterio que a juicio de la empresa resulte adecuado.

Infraestructura tecnológica para el monitoreo y consolidación de operaciones. La empresa debería contar con una herramienta tecnológica, que le permita implementar adecuadamente el SIPLA/FT, especialmente lo relacionado con los mecanismos e instrumentos del sistema.

Capacitación en temas de prevención y control del LA/FT. La empresa debería diseñar, programar y coordinar planes de capacitación sobre el SIPLA/FT dirigidos a todas las áreas y funcionarios de la entidad, con énfasis en las políticas, los procedimientos y en los mecanismos e instrumentos de control adoptados.

3.7.3. *Definición de mecanismos, procedimientos, instancias responsables de los órganos de funciones de control interno para el riesgo de LA/FT*

El SIPLA/FT y el SARLA/FT deberían:

- a) Prever mecanismos y procedimientos adecuados de control interno que le permitan asegurar el adecuado funcionamiento del sistema;

- b) Designar personas y definir instancias responsables para efectuar la evaluación y supervisión del diseño y funcionamiento del SIPLA/FT, a fin de que se puedan establecer las fallas o debilidades y adoptar las medidas pertinentes para garantizar su adecuado funcionamiento, en especial lo relacionado con los mecanismos e instrumentos definidos anteriormente, y
- c) Definir un organigrama y asignar funciones y responsabilidades para: junta directiva, representante legal, revisoría fiscal, auditoría interna, oficial de cumplimiento.

3.7.4. Diseño de tipos de reportes que debe generar el sistema

El SIPLA/FT que se diseñe debería contemplar la generación de reportes tanto internos como externos, que garanticen el funcionamiento de sus propios procedimientos y el cumplimiento del deber legal de colaborar con las autoridades a cargo de la lucha contra el delito de LA/FT. Los tipos de reportes, tanto internos como externos, fueron mencionados anteriormente.

3.7.5. Diseño de políticas, procesos y procedimientos para la documentación y registros del sistema

Los elementos del SIPLA/FT o del SARLA/FT que implemente la empresa deberían constar en documentos y registros, garantizando la integridad, oportunidad, confiabilidad y disponibilidad de la información allí contenida.

4. PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE POLÍTICAS DEL SARLA/FT

A continuación presentamos una breve descripción de algunos procedimientos relacionados con el SIPLA/FT y con el SARLA/FT. Sólo se trata de ideas que le podrían ayudar a complementar sus procedimientos para prevención y control del LA/FT en la empresa.

4.1. Para identificar (buscar, denominar, describir) operaciones inusuales

Considere que podría estar ante un evento de riesgo de LA/FT inminente. Analice objetivamente los indicios del evento de riesgo de LA/FT, determine la situación de riesgo, el factor de riesgo, la señal de alerta y establezca preliminarmente la o las causas primarias del evento de riesgo de LA/FT y, si le es posible, la causa final. Identifique el tipo de control que se tiene establecido para mitigar el riesgo, si existe, y evalúelo.

Diligencie el formato para reporte de operaciones inusuales y sométalo a consideración de su superior inmediato, quien determinará si su informe efectivamente corresponde a una operación inusual, para luego hacerlo llegar al comité de evaluación de operaciones.

4.2. Para detectar operaciones sospechosas

Con frecuencia, la empresa encontrará dificultades en el cumplimiento de esta obligación legal, bien porque las normas no son claras o porque los procedimientos no son adecuados al fin propuesto, creándose así campos de responsabilidad administrativa e inclusive penal.

En términos generales, el comité evaluador de operaciones inusuales y el oficial de cumplimiento deben considerar como sospechosa una transacción cuyas características, volumen y frecuencia no armonizan con las características del perfil del cliente o del perfil promedio del segmento a que pertenece o con la trayectoria de sus negocios.

Siempre se debe partir de una inusualidad puesta de manifiesto por un funcionario de cuyo análisis y valoración surge la sospecha cuando no es posible desvanecer los elementos que la generan o explicar las circunstancias en que se produce tal inusualidad.

Cuando la confrontación de las operaciones detectadas como inusuales con la información que se tiene del cliente y los mercados no arroja resultados satisfactorios, podemos estar frente a una operación sospechosa.

El deber de la empresa es fundamentalmente: detectar, analizar, evaluar y decidir si la operación es sospechosa y en tal caso comunicarlo a la UIAF.

En este proceso influirán entonces elementos objetivos, cuantificables, verificables y por consiguiente demostrables, pero también se abre un campo a la valoración subjetiva proveniente de la experiencia y el conocimiento de los prototipos de operaciones, circunstancia que deben apreciar las autoridades al tener presente que esta dosis subjetiva implica posibilidad de error, tolerado por la normativa ante la imposibilidad de acierto permanente.

En primer lugar, expresamos como condición para la detección de la percepción de la sospecha, el que los fondos utilizados por el cliente o por el proveedor provienen de una actividad criminal o están relacionados con la financiación del terrorismo.

El reporte de operación sospechosa (ROS) no debe ser confundido con una denuncia y debe ser institucional y no personal.

Según nuestra legislación, una operación sospechosa es todo acto, operación o transacción que, de acuerdo con los usos y costumbres de la actividad de que se trate, resulte inusual o carente de justificación económica o jurídica aparente, sea que se realice en forma aislada o reiterada.

En general, la Comisión Interamericana para el Control del Abuso de Drogas (CICAD) de la Organización de Estados Americanos (OEA) define como operación sospechosa a toda transacción, efectuada o no, compleja, insólita, significativa, con patrones de transacciones no habituales y transacciones no significativas, pero periódicas, que no tengan un fundamento económico o legal aparente.

—Indicios de posibles operaciones sospechosas

A continuación presentamos una relación –no exhaustiva– de posibles indicios para la detección de operaciones sospechosas, sin que constituyan por sí mismos necesariamente pruebas de una operación sospechosa.

- a) Una concentración inusual de operaciones por parte de un cliente o de un proveedor;
- b) Una repetición inusual de operaciones de compra entre un pequeño número de clientes en cierto periodo de tiempo en una jurisdicción de alto riesgo de LA/FT;
- c) La concentración inusual de transacciones y/o órdenes con un único cliente; o con un número limitado de clientes (sobre todo si los clientes están relacionados entre sí);
- d) El cliente solicita específicamente la inmediata ejecución de una compra, sin importarle el precio al que se ejecutará;
- e) Cuando la operación de compra o de venta no guarda relación con la actividad del cliente o proveedor, y
- f) Que la operación o algunas características comerciales del cliente o del proveedor responda a tipologías definidas por la UIAF, adjuntas en anexo a este manual.

Las únicas entidades facultadas para determinar si la operación es “sospechosa” son el oficial de cumplimiento y el comité de evaluación de operaciones. En estos casos no se requiere tener certeza de que se trata de una actividad delictiva, ni identificar el tipo de delito penal o que los recursos involucrados provengan de tales actividades.

Para establecer las razones objetivas de la calificación como *operación sospechosa*, se deberán atender las señales de alerta incluidas en cada operación inusual más los otros elementos que la configuran; el comité de evaluación de operaciones inusuales podrá tener en cuenta señales de alerta relacionadas con: posibles vínculos entre operaciones por variables como nombres de clientes/usuarios/agentes económicos, teléfonos, direcciones, ubicación geográfica; comportamiento de los clientes/usuarios/agentes económicos dentro del mercado, y/o también por inconsistencias entre los valores declarados de ingresos, egresos, activos, patrimonio y su perfil financiero dentro de la empresa, operaciones múltiples. También podrá analizar los datos históricos para el último año, realizar llamadas para

corroborar o verificar la información de las bases de datos del aplicativo operativo y/o de los documentos físicos.

Dependiendo del juicio y criterios del comité, unas operaciones serán consideradas sospechosas y otras, las no consideradas como sospechosas pero que sí son inusuales, podrán ser sometidas a un seguimiento o monitoreo especial, mediante el uso de listas de control o, en su defecto, se dejará constancia de la decisión en el acta del comité.

En todo caso, antes de transmitir a la UIAF el respectivo ROS, se deberá atender a las recomendaciones de la misma, en cuanto a características de calidad de la información, según los documentos expedidos en forma general o según informes de retroalimentación emitidos en forma particular para la empresa.

El asistente del oficial de cumplimiento o quien cumpla sus funciones será el responsable del envío de este reporte a la UIAF.

El comité gerencial del SIPLA/FT, en cabeza del oficial de cumplimiento, será el responsable de mantener en custodia el archivo generado de las operaciones sospechosas por el mismo año calendario al que pertenezcan las respectivas operaciones. Una vez terminado el año, los soportes de las operaciones sospechosas podrán ser enviados al archivo de la empresa; el archivo de la documentación relacionada con estas será organizado en orden cronológico conforme las fechas de reporte de las mismas a la UIAF.

4.3. Para impulsar la cultura organizacional de prevención y control del riesgo de LA/FT

Para impulsar la cultura de prevención y control del lavado de activos y de la financiación del terrorismo, la empresa debería emprender acciones encaminadas a: 1. Fortalecer el conocimiento que deben tener todas las personas pertenecientes a la empresa sobre las actividades delictivas y las medidas de prevención y control del lavado de activos y de la financiación del terrorismo. 2. Fortalecer el componente afectivo y sentimental en contra el delito de LA/FT y a favor de las medidas de prevención y control. 3. Generar un comportamiento positivo y favorable hacia la preven-

ción y control y, negativo y desfavorable hacia el delito.

Las acciones a seguir para el fortalecimiento de la cultura de prevención y control del riesgo de LA/FT podrían ser:

— Capacitación presencial o virtual, de acuerdo a los planes de capacitación programados para el año, los cuales se aplicarían para todos los empleados de la organización.

— Inclusión del tema SARLA/FT en la inducción dada a todos los empleados que ingresen a la empresa.

— Reuniones de junta directiva, cuando se presentan:

a) Justificación y discusión de las propuestas de actualización del manual SARLA/FT;

b) Presentación de los informes de la gerencia general, de la gerencia de riesgos, del oficial de cumplimiento, de la revisoría fiscal y de la auditoría interna, y

c) Publicación de temas sobre el delito de LA/FT y su prevención y control en distintos medios, tanto físicos, como electrónicos, como intranet, internet, carteleras, correos electrónicos, cartillas, instructivos, volantes, entre otros.

— Reuniones realizadas en forma presencial o por medios electrónicos, como la videoconferencia, intranet, internet.

— Establecimiento de la estructura organizacional y definición de sus funciones.

— Asignación de recursos tecnológicos.

4.4. **Para los mecanismos de control**

Las personas interesadas en la empresa se pueden denominar público; estos son: usuarios del servicio, clientes del servicio, proveedores, accionistas, miembros de junta directiva, empleados, asesores, etc. (cualesquiera

de estos podría ser una persona públicamente expuesta).

El mayor nivel de exposición al riesgo de la empresa proviene precisamente de estos públicos, por tanto se constituyen en un importante factor de riesgo de LA/FT.

Para cada tipo de público debería diseñarse un estricto procedimiento que permita determinar sus verdaderas intenciones al utilizar los servicios de la empresa, al establecer relaciones contractuales con ella, la procedencia legítima de sus ingresos, los destinos que tendrán los recursos y los productos que adquiere en ella.

A continuación presentamos algunas ideas que podrían ayudar a documentar técnicamente procesos y procedimientos que aseguren el conocimiento que tenemos de ellos.

4.4.1. *Para el conocimiento del usuario*

El objetivo de este procedimiento es capturar y conservar la información de usuarios de productos y servicios relacionados con las operaciones de la empresa.

Este procedimiento debería aplicar para todos los usuarios de productos y servicios ofrecidos por la empresa.

Antes de realizar la actividad final de una operación, el funcionario del *front office* debe solicitarle al usuario o su apoderado, como mínimo, la información especificada anteriormente, tanto para personas naturales como para personas jurídicas.

Podría establecerse una política que expresa la no vinculación o la terminación de las relaciones comerciales con personas naturales o jurídicas vinculadas por las autoridades policivas en actividades delictivas, lavado de activos y financiación del terrorismo; todas las operaciones realizadas con usuarios debieran ser evaluadas automáticamente por el aplicativo operativo respectivo, tomando como parámetro de búsqueda el número de identificación del usuario contra las listas de control establecidas.

Cuando la lista de control no contenga el número de identificación, el aplicativo operativo debiera utilizar como parámetro de búsqueda el nombre del usuario para que arroje una señal de alerta por posible homonimia e indicar el procedimiento a seguir en cada caso según el tipo de lista y/o aquellas que se encuentren reportadas en las listas ONU, OFAC y demás listas vinculantes para Colombia o en listas que tengan razones objetivas para no prestar los servicios a clientes y usuarios.

4.4.2. *Para el conocimiento del cliente*

El objetivo de este procedimiento es describir los pasos a seguir para diseñar directrices con el fin de determinar perfiles o detectar actividades que desempeñen los clientes, las cuales puedan exponer en mayor grado a la empresa al riesgo de LA/FT.

Este procedimiento aplicaría para todos los clientes y/o usuarios actuales en todo el territorio internacional y nacional, para lo cual se debe:

- a) Catalogar los clientes según clasificación realizada, de acuerdo a documentos informativos, por zonas nacionales y diferentes países de acuerdo a su exposición de riesgo de LA/FT (GAFI);
- b) Verificar la total recepción de los documentos requeridos para la vinculación de clientes y el correcto y total diligenciamiento del formato único de vinculación diseñado para tal fin;
- c) Verificar la información suministrada por el cliente, en cumplimiento de la normatividad nacional e internacional en cuanto a registros, topes, documentación necesaria para su funcionamiento, etc.;
- d) Cotejar la información suministrada por el cliente con respecto a información a la cual se tenga acceso de forma externa e interna;
- e) Evaluar objetividad, efectividad, frecuencia, y nivel de riesgo en señales de alerta detectadas en el cliente, y
- f) Medir exposición al riesgo de LA/FT y ponderar, de acuerdo a resultados analizados, el nivel de riesgo del cliente.

De acuerdo al análisis realizado, el oficial de cumplimiento deberá emitir un concepto positivo o negativo para la junta directiva, con el fin de proporcionar elementos de juicio para tomar las decisiones pertinentes.

— *Vinculación de personas expuestas públicamente (PEP)*

Cuando se esté vinculando una persona que sea considerada como persona expuesta públicamente (en adelante PEP), por estar en una lista de control o porque en el momento de la vinculación se conoce su condición de ser una PEP, dicha vinculación será sometida a aprobación de un funcionario de nivel superior al que normalmente aprueba las vinculaciones. En caso de aprobarse la vinculación de un cliente que tiene la condición de ser un PEP, se le solicitarán documentos escritos para verificar y documentar esa calidad en la cual debe incluir:

- a) Su firma;
- b) Su nombre completo en letra legible;
- c) Empresa para la cual trabaja;
- d) Cargo que ocupa;
- e) Si de acuerdo con sus funciones o por razón de su cargo maneja recursos públicos;
- f) Si detenta algún grado de poder público;
- g) Si goza de reconocimiento público, y
- h) Si los recursos que está recibiendo o depositando, según el servicio, son de su exclusiva propiedad o para su uso personal y que no le pertenecen al Estado, al gobierno o ninguna entidad en las cuales ha desempeñado cargos públicos del orden nacional o internacional.

La comunicación anterior es un anexo y hace parte integral del formulario único de vinculación. El monitoreo de este tipo de clientes se realizará en función de las operaciones que dicha persona realice al interior

de la empresa y se confrontará contra los datos financieros entregados en el formulario único de vinculación/actualización de datos.

En el evento en que un usuario o cliente o beneficiario final pase a ser una persona públicamente expuesta, deberá informarse a la instancia o empleado de jerarquía superior encargado de tales vinculaciones, para efectos de tomar las medidas de control de riesgos.

Si la PEP es representante de una campaña política, se solicitarán los datos del reporte a enviar a la UIAF sobre la campaña política que el PEP representa.

4.4.3. *Para el conocimiento de proveedores*

Las ideas para conocer a proveedores son las siguientes:

La empresa no tendrá o dará por terminadas las relaciones comerciales con personas naturales o jurídicas vinculadas por las autoridades competentes en actividades delictivas de lavado de activos y terrorismo y que se encuentren reportadas en la lista OFAC, ONU o en listas restrictivas de control interno del SARLA/FT en la cual se haya autorizado la no prestación del servicio.

Solamente se realizará conocimiento de proveedores, sobre aquellos que tienen una relación contractual permanente, cuyas compras de mercancía, bienes o servicios que le realice la compañía en forma individual sean iguales o superiores a un valor a establecer por la empresa o que de manera fraccionada o acumulada durante un período de tiempo sea igual o superior a un valor definido por la empresa.

En todos los casos de vinculación de clientes proveedores en la empresa, el área responsable deberá confirmar la información del proveedor, lo mismo que de las personas autorizadas, y de las referencias suministradas, dejando evidencia escrita de tal confirmación, y en aquellos casos en que no pueda verificarse la información antes citada se cancelará la operación.

Con el propósito de establecer controles para prevenir la ocurrencia

de evento de riesgo de LA/FT, todos los empleados que tengan como función contratar, vincular y negociar con proveedores deberán confrontar si el número de identificación del proveedor se encuentra registrado en la lista de la OFAC y ONU.

En ningún caso podrá aprobarse la operación sin la verificación previa de la información presentada por el interesado o si dentro de esta se encuentran diferencias entre lo informado por el solicitante y las confirmaciones realizadas por la agencia, área respectiva o tesorería.

4.4.4. Para el conocimiento de empleados

Cuando exista relación con personas que son tanto empleados como proveedores de bienes o servicios, se tendrá como conocimiento de la persona, solamente el conocimiento como empleado.

Se exceptúan de este proceso las personas que siendo empleados son empresas de servicios públicos.

4.4.5. Para el conocimiento de los accionistas

Cuando exista relación con personas que son tanto empleados como accionistas, se tendrá como conocimiento de la persona, solamente el conocimiento como empleado.

La empresa debería solicitar información personal del accionista, tales como fotocopia del pasado judicial, cedula de ciudadanía, declaración de renta, certificados de origen de fondos, hoja de vida.

4.4.6. Para el conocimiento de la junta directiva

Se debería solicitar a los miembros de junta directiva su hoja de vida y la documentación adjunta a la misma, tales como diplomas, certificados, fotocopia de su cédula de ciudadanía y demás datos consignados en las proformas existentes por las normas legales vigentes para los trámites de posesión de estos ante la Superintendencia Financiera de Colombia.

Una carpeta de miembros de junta directiva deberá permanecer junto con el trámite de posesión ante la Superintendencia Financiera de Colombia para efectos de consulta y archivo. Esta carpeta estará a cargo del secretario o general o, a falta de este, del oficial de cumplimiento.

4.4.7. *Para el conocimiento del mercado*

La empresa debería conocer las características particulares de las actividades económicas de sus clientes, así como de las operaciones que estos realizan en los diferentes mercados, por lo que se hace necesario establecer un procedimiento para conocer el mercado al cual se dirigen los productos que se ofrecen a los clientes.

El procedimiento podría incluir:

— *Administrar los perfiles de los clientes.* Los perfiles de clientes estarán conformados por la asociación de los factores de riesgo (cliente, canal de distribución, jurisdicción, producto).

— *Establecer a cada perfil del cliente sus características usuales,* en términos absolutos y en especial para el tipo de producto al que pertenezca cada cliente, su cantidad de operaciones normales, rango de valor normal en promedio por operación, valor máximo y mínimo por operación.

— *Administrar las variables relevantes* para cada uno de los factores de riesgo:

- a) En *el cliente*: su actividad económica, volumen o frecuencia de sus transacciones y monto de ingresos, egresos y patrimonio;
- b) En *el producto*: cantidad de operaciones, rango de valor de operación normal, valor máximo y mínimo;
- c) La *jurisdicción*: nacional, zona de donde se ofrece el servicio al cliente. Según el tipo de producto o servicio, se tendrá en cuenta la variable internacional, zona país o continente de origen o destino de los recursos, y
- d) El *canal*: medio utilizado para prestar el servicio al cliente, puede ser físico (ventanilla) o electrónico (depósito, internet).

La empresa también podría utilizar los segmentos anteriores para conocer el mercado de los usuarios de los servicios.

No se debería tener en cuenta esta segmentación para efectos de conocer el mercado de los agentes económicos distintos de clientes y usuarios.

Los datos de las características usuales y el valor asignado a las variables relevantes serían calculados conforme lo registrado en el último año calendario en las bases de datos de los aplicativos operativos. Se podrían actualizar los datos en un tiempo menor con el fin de ajustar los mismos durante el mismo año calendario.

Se debe asignar un funcionario responsable de calcular y actualizar, como mínimo en forma anual, durante los primeros tres meses de cada año, los datos de las características usuales y el valor asignado a las variables relevantes indicados en el punto anterior.

Una vez actualizado en forma anual todos los perfiles de los clientes, la misma servirá para conocer el mercado y establecer señales de alerta que ayuden a detectar posibles operaciones inusuales.

A cada perfil de cliente o combinación de los factores de riesgo, con sus respectivas variables, se le podrán establecer calificaciones entre uno (1) y cinco (5), en donde uno (1) es una calificación que indica menor riesgo y cinco (5) es una calificación que indica mayor riesgo, con el fin de clasificar los segmentos de mercado y sus respectivos perfiles.

4.4.8. *Excepciones*

En el desarrollo de los procedimientos de conocimiento del cliente, la empresa no estará obligada a exigir el formulario de solicitud de vinculación ni realizar entrevista al potencial cliente cuando quiera que se trate de alguna de las siguientes operaciones, productos o servicios:

- Operaciones realizadas con organismos multilaterales.
- La constitución de fidencias de administración para el pago de obligaciones pensionales.

— En los títulos de capitalización colocados mediante mercadeo masivo o contratos de red, siempre que el pago de las cuotas se haga mediante descuento directo de cuenta de ahorros, cuenta corriente o tarjeta de crédito, y que el cliente haya autorizado expresamente el traslado.

— Cuentas de ahorro abiertas exclusivamente para el manejo y pago de pasivos pensionales.

— En los créditos que se instrumentan a través de libranza, siempre que estas no excedan de seis (6) salarios mínimos legales mensuales y sean otorgadas a empleados de empresas que se encuentren previamente vinculadas en calidad de cliente con la entidad vigilada otorgante del crédito.

— La vinculación a entidades administradoras del sistema general de pensiones en cuanto a los aportes obligatorios.

— La vinculación a entidades administradoras de cesantías en lo relacionado con los recursos provenientes de dicha prestación.

— Los productos o servicios financieros abiertos a nombre de los beneficiarios del programa “Familias en Acción” y “Familias Guardabosques” que hacen parte del programa “Contra Cultivos Ilícitos” administrados por la Agencia Presidencial para la Acción Social y la Cooperación Internacional (Acción Social), siempre que estén destinadas exclusivamente al manejo de los recursos provenientes de dichos programas.

En los siguientes seguros:

— Los tomados por entidades financieras, aseguradoras o sociedades administradoras de fondos de pensiones por cuenta de sus clientes.

— Los relativos a la seguridad social.

— Aquellos en que el tomador, asegurado, afianzado o beneficiario sea una persona jurídica bajo el régimen de derecho público, salvo los tomados por empresas industriales y comerciales del Estado y/o sociedades de economía mixta que no estén sometidas a inspección y vigilancia de la SFC.

— Los contratos de reaseguro.

— Los tomados mediante mercadeo masivo o banca seguros siempre que el pago de las primas se haga mediante descuento directo de cuenta de ahorros, cuenta corriente o tarjeta de crédito, y que el cliente haya autorizado expresamente el traslado.

— Aquellos tomados por personas naturales o jurídicas por cuenta y a favor de sus empleados, cuyo origen sea un contrato de trabajo o relación laboral, respecto de la información del asegurado y el beneficiario. En lo que hace al tomador, la información debe solicitarse en su totalidad.

— Aquellos que las entidades aseguradoras están obligadas a expedir por disposición legal.

— Aquellos otorgados mediante procesos de licitación pública.

— De cumplimiento cuando se celebren para garantizar el cumplimiento de contratos con entidades de carácter público.

— De accidentes personales en vuelo.

— Los contratos de coaseguro para las compañías distintas a la líder.

— Pólizas judiciales.

— De salud.

— Exequiales.

4.5. Para los instrumentos establecidos para la prevención y control del LA/FT

Son instrumentos de control las señales de alerta, la segmentación de los factores de riesgo, el seguimiento de las operaciones y la consolidación electrónica de operaciones.

Los requerimientos que reciba la empresa, provenientes de las autoridades y entidades competentes, tales como la DIAN, la Policía, la Fiscalía, el DAS, la Superintendencia Financiera de Colombia y el Banco de la República, podrían ser atendidos conforme el siguiente procedimiento:

—Los requerimientos se pueden recibir por medios físicos o escritos y por medios electrónicos o magnéticos.

—Cuando el requerimiento se reciba en forma física, cada responsable deberá radicarlos imponiendo su firma y/o sello de la empresa en señal de haber recibido el mismo, indicando la fecha de su recepción.

—Cuando los requerimientos de información de autoridades competentes se reciban en forma electrónica, será responsabilidad de quien recibió dicho requerimiento coordinar su respuesta por parte del área responsable de atenderlos.

—Una vez recibidos los requerimientos, radicados y circularizados al área responsable, esta última deberá dar respuesta a los mismos conforme los plazos otorgados en cada requerimiento. Cuando el plazo no se mencione, y no exista la urgencia manifiesta en el requerimiento, el área responsable podrá tomar un plazo de tres días hábiles para realizar la debida respuesta. En los casos en los cuales se requiera un plazo superior a los indicados en el requerimiento, el área responsable debe solicitar, mediante una comunicación dirigida a la entidad que realizó el requerimiento, la ampliación del plazo y el resumen de las razones que motivan dicha solicitud.

—El oficial de cumplimiento debería ser el responsable de atender los requerimientos relacionados con entidades competentes, como la Policía, el DAS, la Fiscalía y demás entidades judiciales o policivas. Las fechas de los requerimientos se tomarán a partir de que la comunicación sea recibida por el área responsable, en especial el área de cumplimiento o quien cubra sus funciones.

—Las comunicaciones de entidades como la DIAN y la Superintendencia Financiera de Colombia que se relacionen con temas del área de cumplimiento, áreas de lavado de activos y/u otras actividades delictivas de dichas entidades y demás situaciones afines con la información que administra el área de cumplimiento deben ser remitidas al área de cumplimiento para cumplir con el procedimiento descrito anteriormente.

—Las respuestas a requerimientos pueden ser entregadas por medios escritos o electrónicos y, en todo caso, atendiendo la forma como lo indica el requerimiento.

— La entrega del requerimiento podrá ser realizada por medio de una empresa de correos o en forma directa por empleado directo o temporal con contrato con la empresa.

— Las copias de las respuestas radicadas ante las entidades competentes serán remitidas al área que originó las respuestas, en especial las relacionadas con el área de cumplimiento, con el fin de archivarlas en orden consecutivo conforme la fecha de recepción del requerimiento.

— Por lo menos una vez al año el archivo de la correspondencia deberá ser remitido o entregado, mediante comunicación escrita o por medios electrónicos, al área de archivo de recursos físicos, conforme los procedimientos establecidos para la custodia, almacenamiento y guarda y consulta de la correspondencia de la empresa.

— El área responsable, en especial el área de cumplimiento, deberá guardar copias de las cartas entregadas en una carpeta en donde se archive la correspondencia interna entregada. Esta carpeta deberá estar en el área de cumplimiento por lo menos durante el mismo año calendario al cual pertenecen los requerimientos según sus fechas de recepción.

4.6. Para dar cumplimiento a las obligaciones relacionadas con las listas internacionales

4.6.1. *Listas internacionales vinculantes para Colombia*

El procedimiento que se establezca en la empresa para dar cumplimiento a las obligaciones relacionadas con las listas vinculantes para Colombia podría consistir en consultar al menos mensualmente la última actualización de la página de Internet de la ONU en inglés (<http://www.un.org/sc/committees/1267/consolist.shtml>) o en español (<http://www.un.org/spanish/sc/committees/1267/consolist.shtml>).

Otra fuente para saber si la lista ha sufrido algún cambio es la correspondiente a los archivos que la Superintendencia Financiera de Colombia tiene publicados en su servicio de comunicación entre ella y las entidades vigiladas (RAS, RDSI), en el cual se pueden descargar las comunicaciones que el Ministerio de Relaciones Exteriores ha radicado ante la Superintendencia Financiera de Colombia.

Una vez confirmada la fecha de la última modificación en la página web de la ONU o de la fuente, se deberá ingresar al sistema la respectiva actualización.

Esta actualización podrá realizarse en forma total, es decir, retirando completamente la lista y añadiendo la nueva lista o agregando o retirando (actualizando) los datos que hayan sufrido modificación respecto de los campos incluidos en él o los aplicativos operativos.

Cuando una operación o proceso genere una señal de alerta cuyo procedimiento indique que debe ser autorizada por el comité evaluador de operaciones, este realizará el análisis de la operación, confrontando la información suministrada por el agente económico (usuario, cliente, empleado, proveedor, etc.) contra la información disponible en las bases de datos de cada lista de control y, en caso de encontrar similitudes, dicho comité podría dar instrucción de anulación de la operación o del proceso.

Debe dejarse evidencia documental de la modificación y/o actualización de la lista vinculante para documentar la debida diligencia.

4.6.2. *Otras listas de control de riesgos LA/FT*

Para prevenir y controlar el riesgo LA/FT, la empresa debería implementar, además de la lista del punto anterior, otras las cuales no son vinculantes para Colombia, pero que por razones objetivas resulta importante adoptarlas al interior de la empresa.

Estas listas de prevención y control conviene incluirlas dentro del aplicativo operativo, de tal forma que cada transacción sea validada contra la totalidad de las listas, utilizando como llave principal para el cruce de información el número de identificación y como llave secundaria la cadena de caracteres que conforma su nombre completo, es decir, nombres y apellidos.

No todas las listas son restrictivas para no dejar realizar una operación o para no prestar el servicio al cliente o usuario. Algunas listas pueden ser de seguimiento, es decir, que tan solo generarán una señal de alerta, instruyendo a los empleados que atienden público y/o que administran opciones relacionadas con clientes y/o usuarios dentro del aplicativo operativo, para que sigan un procedimiento específico.

—*Lista de posible suplantación de persona al realizar operaciones*

Esta lista es un ejemplo de las que sólo generarán una señal de alerta y se elaboran teniendo como base los siguientes criterios:

Fuente	Ámbito	Tipo de lista	¿Se presta servicio al cliente/usuario?	Razón objetiva para implementar la lista
Operaciones directas del cliente o usuario y por indicación de fuente cierta	Nacional	Sólo es para generar una señal de alerta, no es restrictiva para prestar el servicio	Sí, según análisis del responsable de la operación	Exposición al riesgo de lavado de activos y de la financiación del terrorismo, causado por clientes/usuarios que quieren utilizar la entidad con documentos falsos, o con documentos originales pero que no corresponden a su identidad. Se exceptúan los apoderados o representantes, quienes tienen el poder de representar a un tercero

Quien en la empresa tenga conocimiento de la existencia de un evento de riesgo de LA/FT causado por posible suplantación debe informar sobre la ocurrencia de esta situación al oficial de cumplimiento, con el fin de que se realice la respectiva actualización en el aplicativo operativo.

Una suplantación o posible suplantación se puede demostrar analizando:

- El documento de identificación del cliente/usuario. Si presenta señales de haber sido adulterado o falsificado, o si los elementos de seguridad documental incorporados por la Registraduría Nacional del Estado Civil o cualquier entidad competente, nacional o internacional, no corresponden con el documento físico presentado, entre otros, y
- Si la forma de la escritura empleada en la firma y/o la huella dactilar tomada sobre el documento de identificación son distintas de la firma o escritura y/o huella que el cliente/usuario realice sobre él o los formatos o formularios utilizados por la empresa.

En cualquier operación de la empresa con un posible cliente o usuario o con algún otro agente económico, el responsable de la operación debe

decidir si continúa con ella, conforme la señal de alerta generada por el sistema.

Estas señales de alerta deben ser ajustadas por el oficial de cumplimiento, conforme los controles establecidos para el evento de riesgo de LA/FT analizado, y podrían ser de tipo restrictivo, es decir, que no se puede efectuar la operación, o de tipo preventivo, es decir, que se debe generar una señal de alerta con una instrucción sobre cómo se debe proceder.

Se pueden crear alertas con base en homónimos, las cuales pueden ser restrictivas o preventivas.

Cuando las operaciones no se puedan ejecutar, conforme el mensaje de señal de alerta que aparezca en la pantalla, el responsable de la operación debe informarlo para anular, devolver, reintegrar la operación, según el tipo de producto o servicio involucrado.

—*Lista por análisis especial de operaciones*

Este es otro tipo de lista no vinculante que podría utilizar la empresa y se puede elaborar con base en clientes o usuarios que fueron incluidos en operaciones sospechosas individuales o múltiples.

Fuente	Ámbito	Tipo de lista	¿Se presta servicio al cliente/usuario?	Razón objetiva
Operaciones sospechosas especiales	Nacional – Interno	Restrictiva por número de Identificación	No	Aumenta, en la empresa, el grado de exposición al riesgo del lavado de activos y de la financiación del terrorismo, causado por la presunción de que la empresa sea utilizada por clientes/usuarios a los cuales se les ha detectado vínculos, conexiones o asociaciones por alguna de las variables tales como el nombre completo del remitente, nombre completo del beneficiario y/o su número de identificación, para un periodo de tiempo razonable y con montos relacionados por fuera de los perfiles

Esta lista de operaciones sospechosas especiales se alimenta de aquellas operaciones analizadas, en formas diferentes a los procesos estándar que tiene la empresa para detectar operaciones sospechosas, conforme el reporte de señales de alerta y/o por el reporte de operaciones inusuales, que al ser calificadas con un puntaje que demuestra un alto nivel de exposición al riesgo nos dan indicios de estar ante un evento de riesgo de LA/FT.

Estas personas podrían ser clasificadas según la severidad de la operación sospechosa.

—*Lista de personas fallecidas*

Otra lista de gran importancia para efectos de prevención y control del LA/FT es la de personas fallecidas.

Fuente	Ámbito	Tipo de lista	¿Se presta servicio al cliente/usuario?	Razón objetiva
Datawin o policía o entidades competentes	Nacional	Restrictiva	No	Si el número de identificación corresponde a una persona que ha sido registrada por el Estado, desde el punto de vista legal, como fallecida y que se conoce de ese hecho mediante consultas en Datawin o mediante información remitida por las entidades competentes, entonces no se debe permitir que ese documento de identificación sea utilizado por delincuentes para utilizar a la entidad en operaciones ilícitas. Estas personas aumentan el riesgo LA/FT en la empresa

Cuando un funcionario del *front office* conozca, mediante algún medio (Datawin) o mediante la información escrita o verbal de parte de alguna entidad competente (Policía, Fiscalía, DAS, Registraduría, etc.), sobre un número de identificación que pertenece a una persona fallecida y que no ha sido otorgada a otra persona, debe remitir comunicación por escrito o en medio electrónico al área de cumplimiento para que la persona responsable en esta área la incorpore en la base de datos de los aplicativos operativos el número de identificación con la señal de alerta restrictiva.

—*Lista de PEP (personas públicamente expuestas)*

Esta lista se puede construir con base en los siguientes criterios:

Fuente	Ámbito	Tipo de lista	¿Se presta servicio al cliente/usuario?	Razón objetiva
Entidades oficiales o del Estado con información de carácter público que informen en internet sus listas de personal que por razón de su cargo manejen recursos públicos, detenten algún grado de poder público o gocen de reconocimiento público	Nacional e internacional	De seguimiento	Sí, según decisión del responsable	Por mandato expreso de la ley se debe prever procedimientos de vinculación y monitoreo de operaciones de persona nacional o extranjera que por su perfil o por las funciones que desempeña pueden exponer en mayor grado a la entidad al riesgo LA/FT

Estas listas podrán ser actualizadas en cualquier momento y como mínimo una vez al año, según la información disponible y conocida.

En el caso que el aplicativo operativo o un funcionario del *front office* detecte que se está tratando de hacer una vinculación o una operación con una persona expuesta públicamente, se deberá avisar al jefe inmediato o al empleado de jerarquía superior al que normalmente aprueba las vinculaciones en la entidad, para que sea este último quien tome la decisión de continuar con la operación o la cancele.

En el evento en que un cliente/usuario pase a ser una persona públicamente expuesta, el empleado responsable deberá informar a la instancia o empleado de jerarquía superior para que se tomen las decisiones respectivas. Estas decisiones pueden dar lugar a incluir a una persona en listas de control y seguimiento de PEP, o cualquier otra lista de un mayor grado de riesgo LA/FT, cancelar la operación, devolver o reintegrar los recursos de la operación inicial, diligenciar formatos especiales, confirmar y/o verificar la información, entre otras.

En caso de estar ante la presencia de personas que representen una campaña política, se podrían verificar los datos de la campaña y su representante y se seguiría lo indicado por las normas legales vigentes para efectos del reporte respectivo. La verificación de los datos debe quedar en

el formulario único o anexo al mismo por parte del empleado que realizó la operación y la verificación.

—*Lista judicial*

La empresa la podría elaborar con base en los siguientes criterios.

Fuente	Ámbito	Tipo de lista	¿Se presta servicio al cliente/usuario?	Razón objetiva
Requerimientos de la Policía, el DAS, la DIJIN, la Fiscalía, la Interpol	Nacional / internacional	Restrictiva	No	Riesgo de realizar transacciones con posibles delincuentes que pueden estar al margen de la ley y que por esto aumente el grado de exposición del riesgo del lavado de activos y demás actividades ilícitas

Esta lista incluiría a las personas por su número de identificación, según los requerimientos que la empresa ha recibido de las entidades policivas competentes, tales como la Policía, la Fiscalía, el DAS, la DIJIN, la Interpol o un juez de la República que esté vinculando a personas relacionadas con investigaciones o actuaciones relacionadas con actividades delictivas que puedan conducir, especialmente, al lavado de activos o financiación del terrorismo.

Como excepción, las personas pueden ser retiradas de esta lista si demuestran, con su pasado judicial, que no tienen situaciones judiciales pendientes o actuales con la justicia colombiana. Su pasado judicial debe ser posterior a la llegada del requerimiento. En caso de autorizarse la operación, la misma debe ser reportada a la entidad que originó el requerimiento.

El comité evaluador de operaciones, o el oficial de cumplimiento, o el gerente de riesgos, o el gerente general, o quien cumpla sus veces, podrá crear tantas listas de control del riesgo del LA/FT como sean necesarias a fin de evitar la ocurrencia de evento de riesgos relacionados con actividades delictivas. Tales listas se entenderán que hacen parte del presente manual y se podrán adicionar al presente manual cuando estén en ejecución, para lo cual se deberá utilizar la hoja de control de cambio y presentar la adición en la próxima reunión de junta directiva en señal de información.

4.7. Para garantizar la reserva de la información reportada conforme lo establece el Estatuto Orgánico del Sistema Financiero

La empresa debería asegurar la reserva de la información que se llega-re a reportar conforme a lo establecido en el artículo 105 del Estatuto Orgánico del Sistema Financiero. Dicho artículo (modificado por la L. 1121 del 29 de diciembre de 2006) dice:

Reserva sobre la información reportada. Sin perjuicio de la obligación de reportar de forma inmediata y suficiente a la Unidad de Información y Análisis Financiero la información a que se refiere la letra d) del numeral 2º del artículo 102, las instituciones financieras sólo estarán obligadas a suministrar información obtenida en desarrollo de los mecanismos previstos en los artículos anteriores cuando así lo solicite la Unidad de Información y Análisis Financiero o la Fiscalía General de la Nación.

Las autoridades, las entidades, sus administradores y sus funcionarios que tengan conocimiento por cualquier motivo de las informaciones y documentos a que se refieren los artículos anteriores, deberán mantener reserva sobre los mismos. Además no podrán dar a conocer, a las personas que hayan efectuado o intenten efectuar operaciones sospechosas, que se ha comunicado a la Unidad de Información y Análisis Financiero, información sobre las mismas, y deberán guardar reserva sobre dicha información.

4.8. Para prevenir y resolver los posibles conflictos de interés e imposición de sanciones

La empresa debe poseer un código de ética y conducta, el cual debe ser aprobado por la junta directiva y en él se deben incluir los mecanismos suficientes para la resolución de conflictos de interés. En ese documento se deben establecer los principios, valores, conductas y mecanismos para la prevención y resolución de conflictos de interés que deben observar los funcionarios que presten sus servicios a la empresa en todas sus actuaciones, así como la imposición de sanciones.

Parte de lo indicado en el código de ética y conducta lo podemos observar en los siguientes dos puntos:

Se considera que existe conflicto de interés cuando cualquier funcionario y/o empleado, administrador y accionista, en razón de su actividad, se enfrenta a distintas alternativas de conductas con relación a intereses, de suerte que la satisfacción de los propios implique la lesión de los intereses de la compañía, las normas de carácter legal, los principios o políticas de la entidad; por ejemplo, generan conflicto de interés situaciones de disyuntiva en la toma de decisiones cuando se trate de escoger entre el beneficio propio con el de la compañía, el beneficio propio con el de un cliente, el beneficio propio con la transparencia del mercado o cualquier situación que implique la omisión de sus deberes legales, contractuales o morales a los que se encuentra sujeto.

La empresa debería tener procedimiento para la prevención de conflictos de interés contenidos en el código de ética y conducta. Este procedimiento incluye los procesos de evaluación, calificación y resolución del conflicto; a continuación se explica cada uno:

—Evaluación

El análisis contiene la identificación de la situación y de las circunstancias que configuran el conflicto de interés o permitieron su ocurrencia. Todo funcionario y/o empleado conocedor de una situación generadora de un potencial conflicto de interés debe dar aviso a su jefe inmediato. Cuando se trate de administradores y accionistas, se deberá dar aviso inmediato al representante legal. El jefe inmediato deberá evaluar la conducta e informar al representante legal sobre la misma, incluyendo la decisión adoptada. En caso de existir duda sobre la situación de conflicto de interés, el representante legal deberá solicitar una opinión legal sobre la conducta y plantear el tema ante el comité de auditoría de la entidad. Este procedimiento aplica en todas aquellas situaciones que involucren a los administradores y accionistas de la compañía.

—Calificación

El comité de auditoría o en su defecto la junta directiva calificarán el conflicto de interés presentado de acuerdo con su impacto y gravedad. Se

tendrá en cuenta si la ocurrencia del conflicto se presentó por información del interesado o por investigación oficiosa de algún funcionario y/o empleado, directivo, accionista o por información de alguna persona o autoridad o simplemente por azar. Cuando se trate de administradores y accionistas, se llevará el tema al comité de auditoría; en caso de que no pueda ser resuelto por este ente, se integrará un comité de tres miembros compuesto por el representante legal, un delegado de la junta directiva y un amigable componedor aceptado por las partes.

—*Resolución*

La resolución al conflicto de interés se dará conforme a la aplicación de la ley e interpretación de políticas y normas internas y debe contar con la aprobación del ente que haya recibido la atribución para hacerlo por parte de la empresa.

En caso de considerarse necesario, los conflictos de interés generados por la legislación vigente pueden ser consultados a la Superintendencia Financiera de Colombia o a la entidad legal pertinente, para resolver dicha situación.

Estos lineamientos para la resolución de conflictos de interés también deberían estar contenidos en el código de ética y conducta de la empresa.

—*Sobre régimen de sanciones*

La empresa debe establecer las consecuencias o sancionar disciplinariamente a los empleados que faciliten o coadyuven en la utilización de sus servicios para el lavado de activos, lo mismo para aquellos que incurran en inhabilidades, incompatibilidades, conflictos de interés y en general por violaciones al código de conducta, manual del SARLA/FT, manuales de procedimiento o funciones, conforme a lo establecido en la legislación laboral, el contrato de trabajo y el reglamento interno de trabajo.

Por lo anterior, la conducta irresponsable, permisiva, negligente u omisiva en el desarrollo comercial y operacional de la empresa que viole el código de conducta y/o el manual SARLA/FT, acarreará las sanciones disciplinarias y de ley para los funcionarios y/o empleados.

En cuanto a los administradores y accionistas, se seguirán las normas estatutarias y legales para revisar el tipo de sanción a aplicar, sin perjuicio de las acciones judiciales a que haya lugar.

4.9. Para asegurar el cumplimiento de los reglamentos internos y demás disposiciones relacionadas con el SARLA/FT

La empresa, sus órganos de administración y de control, así como el oficial de cumplimiento y demás empleados y funcionarios, deberían asegurar el cumplimiento de las normas legales y reglamentos internos y demás disposiciones encaminadas a prevenir y controlar el LA/FT, con el propósito no sólo de contribuir a la realización de los fines del Estado y de cumplir la ley, sino de proteger la imagen y la reputación nacional e internacional de los sistemas cuyo control y vigilancia competen a la Superintendencia Financiera de Colombia.

Cualquier incumplimiento sobre este deber por cualquiera de sus órganos de administración y de control, del oficial de cumplimiento y demás empleados y funcionarios, deberá ser atendido conforme las normas internas o externas que le sean aplicables, según lo indicado en el código de ética y conducta y/o con sujeción al reglamento interno de la empresa y/o según lo indicado en los estatutos.

5. EMPRESAS OBLIGADAS A DISEÑAR E IMPLEMENTAR EL SARLA/FT O EL SIPLA/FT

Las diferentes superintendencias colombianas de vigilancia y control de empresas del sector financiero y del sector real han emitido normatividad específica para cada tipo de empresa, la cual presentamos a continuación indicando el número de circular externa o resolución y una muy breve descripción de su alcance:

Tabla 4
Entidades del sector financiero que deben implementar el SARLA/FT

Sector	Financiero						
SUBSECTOR	Establecimientos de crédito	Aseguradoras e intermediarios de seguros	Remesas, compraventa de divisas	Entidades vigiladas que administran o representan franquicias	Intermediarios de valores y otros agentes	Pensiones, cesantías y fiduciarias	Portafolio de inversión
NORMATIVIDAD	Circular Externa 022 de 2007 (abril 19). Referencia: instrucciones relativas a la administración del riesgo de lavado de activos y de la financiación del terrorismo. Mediante la Circular 026 de 2008 de la Superfinanciera se obliga a las entidades financieras a reportar las transacciones en efectivo que superen los 10 millones de pesos. Capítulo Decimoprimer, Título I de la Circular Básica Jurídica (Circular Ext. 007 de 1996)						
TIPO DE SISTEMA DE PyC LA/FT	SARLA/FT	SARLA/FT	SARLA/FT	SARLA/FT	SARLA/FT	SARLA/FT	SARLA/FT
SUPERVISOR	SFC	SFC	SFC	SFC	SFC	SFC	SFC
SISTEMA DE PREVENCIÓN Y CONTROL DEL LA/FT	SARLA/FT	SARLA/FT	SARLA/FT	SARLA/FT	SARLA/FT	SARLA/FT	SARLA/FT
TIPO DE ENTIDAD	Establecimientos bancarios	Compañías de seguros generales			Almacenes generales de depósito	Sociedades administradoras de fondos de pensiones y de cesantía	Fondos de valores
	Corporaciones financieras	Compañías de seguros de vida			Administradoras de sistemas de pago de bajo valor	Entidades administradoras del régimen solidario de prima media con prestación definida	Fondos de inversión
	Compañías de financiamiento comercial	Cooperativas de seguros			Casas de cambio	Sociedades fiduciarias	Fondos comunes ordinarios
	Entidades cooperativas de carácter financiero	Oficinas de representación en Colombia de reaseguradoras del exterior			Trámite de posesión en línea ante la Superintendencia	Trámite de posesión en línea ante la Superintendencia	Fondos comunes especiales
	Organismos cooperativos de grado superior	Sociedades corredoras de seguros					

Sector	Financiero						
	Institucio-nes oficiales especiales - IOE (banca de segundo piso)	Sociedades de capitalización					
TIPOS DE REPORTES	Reporte de Operaciones Sospechosas (ROS)						
	Reporte de transaccio-nes en efecti-vo (vigilados Superfinan-ciera)						

Tabla 5

Entidades del sector real que deben implementar SIPLA/FT

Sector real						
Subsector	Normatividad	Tipo de sistema de PyC LA/FT	Supervisor	Sistema de prevención y control del LA/FT	Tipos de reportes	
Juegos de suerte y azar localizados	<ul style="list-style-type: none"> - Resolución 141 de 2006, UIAF: impone obligación de reportar de manera directa a la UIAF. - Resolución 022 del 23 de febrero de 2007 - Resolución 078 del 10 de julio de 2007 - Circular Externa 081 del 29 de enero de 1999, Supersalud: loterías y concesionarios de apuestas permanentes, distribuidores de loterías, casinos y juegos de azar 	SIPLA/FT	Supersalud	SIPLA/FT	Reporte de Operaciones Sospechosas (ROS)	Reporte para juegos de azar
Juegos de suerte y azar loterías y juegos nove-dosos	<ul style="list-style-type: none"> - Resolución 142 de 2006, UIAF: se impone a las personas jurídicas que operan el monopolio rentístico de los juegos de suerte y azar localizado y no 	SIPLA/FT	Supersalud	SIPLA/FT	Reporte de Operaciones Sospechosas (ROS)	Reporte para juegos de azar

Sector real						
Subsector	Normatividad	Tipo de sistema de PyC LA/FT	Supervisor	Sistema de prevención y control del LA/FT	Tipos de reportes	
	localizado, la obligación de reportar de manera directa a la UIAF. – Resolución 022 del 23 de febrero de 2007 – Resolución 078 de 10 Julio de 2007					
Notariado y registro.	– Resolución 033 de 2007, UIAF: impone a notarios obligación de reportar de manera directa a la UIAF – Resolución 044 del 15 mayo de 2007 – Instrucción Administrativa 08 14 de agosto de 2007, Supernotariado y Registro: obligación de SIPLA/FT	SIPLA/ft	Supernotariado y Registro	SIPLA/FT	Reporte de Operaciones Sospechosas (ROS)	Reporte de operaciones notariales
Profesionales de compra y venta de divisas	– Resolución 062 de 12 junio de 2007, UIAF – Resolución 111 de 21 agosto 2007 – Carta Circular 001 del 2 de diciembre 2007 – Circular Externa 026 de 27 junio 2008, SFC – Circular 003 de 2009, UIAF	SARLA/FT	Superfinanciera	SIPLA/FT	Reporte de Operaciones Sospechosas (ROS)	
Compra y venta de vehículos automotores	– Resolución 114 de 2007: se impone a compraventa y/o compraventa consignación de vehículos automotores nuevos y/o usados, la obligación de reportar de manera directa a la UIAF.	SIPLA/FT	UIAF	Operaciones sospechosas	Reporte de Operaciones Sospechosas (ROS)	Reporte compra y venta vehículos
Comercio exterior y responsables de la función aduanera	– Resolución 285 del 19 de diciembre de 2007, UIAF: la cual se impone a los depósitos públicos y privados, sociedades portuarias, usuarios de zona franca, empresas transportadoras, agentes de carga internacio-	SIPLA/FT	DIAN	SIPLA/FT	Reporte de Operaciones Sospechosas (ROS)	Reporte de transacciones cambia- rias

Sector real						
Subsector	Normatividad	Tipo de sistema de PyC LA/FT	Supervisor	Sistema de prevención y control del LA/FT	Tipos de reportes	
	<p>nal, usuarios aduaneros permanentes y usuarios altamente exportadores, la obligación de reportar de manera directa a la UIAF.</p> <ul style="list-style-type: none"> – Resoluciones 285 de 2007 y 212 (ausencia de operaciones sospechosas) de 2009 – Circular Externa 0170 de 10 de octubre 2002, DIAN – Circular Externa 100-000004 de 7 de octubre de 2009, de la Superintendencia de Sociedades: (...) sugiere que se adopten medidas y conceptos de PyC del LA/FT 					
Metales: oro	<ul style="list-style-type: none"> – Resolución 363 del 18 de noviembre de 2008: se impone a exportadoras y/o importadoras de oro, las casas fundidoras de oro y a las sociedades de comercialización internacional deber de reportar a la Unidad de Información y Análisis Financiero (UIAF) 	SIPLA/FT	UIAF	Operaciones sospechosas	Reporte de Operaciones Sospechosas (ROS)	Reporte transacciones oro
Transportadoras de valores	<ul style="list-style-type: none"> – Circular Externa 003 de 2009 de la Superintendencia de Vigilancia y Seguridad, para empresas transportadoras de valores, empresas de vigilancia y seguridad privada autorizadas en la modalidad de transporte de valores y empresas blindadoras de vehículos 	SIPLA/FT	UIAF	Operaciones sospechosas	Reporte de Operaciones Sospechosas (ROS)	Reporte para transportadoras de valores y blindadoras

Tabla 6

Entidades del sector solidario que deben implementar el SIPLA/FT

SECTOR	SOLIDARIO
SUBSECTOR	Cooperativas
NORMATIVIDAD	CBJ 07 de 2008 de Supersolidaria
TIPO DE SISTEMA DE PyC LA/FT	SIPLA/FT
SUPERVISOR	Supersolidaria
TIPOS DE REPORTES	Reporte de Operaciones Sospechosas - ROS

5.1. Empresas del sector real y del sector financiero

Para efectos de este libro, las organizaciones las podemos clasificar en dos grupos: aquellas que ejercen su actividad en el sector financiero, vigiladas y controladas por la Superintendencia Financiera de Colombia y, las del sector real de la economía, vigiladas por la DIAN, la Superintendencia de Notariado y Registro, la Superintendencia de Salud, la Superintendencia de la Economía Solidaria, la Superintendencia de Vigilancia y Seguridad Privada, y la Unidad de Información y Análisis Financiero (UIAF).

Las entidades del sector financiero deben diseñar e implementar el SARLA/FT, mientras que las del sector real deben hacerlo con el SIPLA/FT y algunas solamente deben reportar a la UIAF las operaciones sospechosas que detecten.

—*Excepciones*

Las siguientes entidades se encuentran exceptuadas de la aplicación de los artículos 102 a 107 del Estatuto Orgánico del Sistema Financiero:

- El Fondo de Garantías de Instituciones Financieras (Fogafin);
- El Fondo de Garantías de Entidades Cooperativas (Fogacoop);
- El Fondo Nacional de Garantías S.A. (FNG);

- d) Los fondos mutuos de inversión sometidos a vigilancia permanente de la SFC;
- e) Las Sociedades Calificadoras de Valores y/o Riesgo;
- f) Las oficinas de representación de instituciones financieras y de reaseguros del exterior;
- g) Los intermediarios de reaseguros, los organismos de autorregulación;
- h) Los proveedores de infraestructura de conformidad con la definición del artículo 75 del Decreto 4327 de 2005, con excepción de los almacenes generales de depósito y los administradores de sistemas de pago de bajo valor, y
- i) Las entidades administradoras del régimen de prima media con prestación definida, excepto aquellas que se encuentran autorizadas por la ley para recibir nuevos afiliados.

Las entidades sometidas a la inspección y vigilancia de la SFC que deban implementar el SARLA/FT y que en el desarrollo de su actividad pretendan vincular como clientes a entidades vigiladas por esta superintendencia se encuentran facultadas para exceptuarlas del cumplimiento de la norma.

5.2. **Características de las empresas obligadas a diseñar e implementar el SIPLA/FT y el SARLA/FT**

La prevención y control del lavado de activos y financiación del terrorismo debe ser aplicada tanto por las empresas del sector real de la economía como por las del sector financiero.

Las primeras tienen como actividad la prestación de servicios no financieros o la producción de bienes de consumo o industriales; las otras se dedican únicamente a la prestación de servicios financieros.

La actividad de prestación de servicios financieros y no financieros, por ejemplo los juegos de suerte y azar, el transporte de valores, la vigi-

lancia y seguridad, los servicios notariales, los de comercio exterior, los de captación y colocación de dineros, etc., se denomina “servucción”, mientras que la de generación de bienes de consumo o industriales se denomina “producción”.

Esta diferenciación la debemos hacer por sus implicaciones en el diseño de los sistemas de prevención y control del LA/FT en empresas de servicios, especialmente las dedicadas a servicios financieros y las empresas de producción.

5.2.1. *Concepto de servucción*

No existe en español una palabra que permita designar el proceso creativo de un servicio, por lo que sus autores han optado el neologismo “servucción”.

El gran aporte de este enfoque es poner el énfasis en la calidad de los servicios como resultado del sistema de servucción, característica diferencial cada vez más importante para la supervivencia de las empresas. Agregaría que otro aporte es individualizar la participación del cliente y del personal en contacto con la generación del servicio, lo cual es muy valioso para efectos de la prevención y control del LA/FT.

De una manera sencilla, la “servucción” puede definirse como el proceso de elaboración de un servicio, es decir, toda la organización de los elementos físicos y humanos en la relación cliente-empresa, necesaria para la realización de la prestación de un servicio y cuyas características han sido determinadas desde la idea concebida, hasta la obtención del resultado como tal (el servicio).

— *Características de los servicios*

Los servicios tienen ciertas características que los diferencian claramente de los productos:

- a) Son intangibles;
- b) Requieren participación activa del cliente;

- c) Son perecederos, y
- d) Son inseparables.

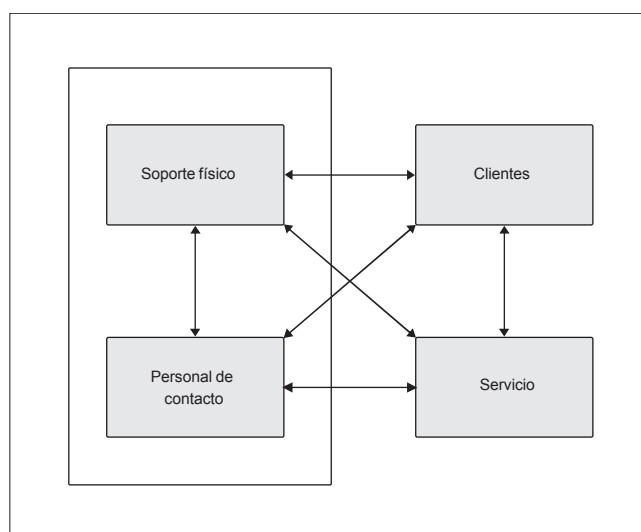
—Elementos del sistema de servucción

Los elementos que integran el sistema de servucción son fundamentalmente diferentes a los de la producción:

- a) Cliente;
- b) Un soporte físico;
- c) Personal de contacto;
- d) El servicio;
- e) Un sistema de organización interna, y
- f) Demás clientes.

La forma como interactúan los elementos en un sistema básico de servucción se expresan en el siguiente diagrama:

Gráfico 9
Sistema de servucción



Es importante recordar aquí que el cliente-comprador de un servicio participa de manera activa en la generación del mismo; sin él el mercado en su totalidad no existiría.

La total satisfacción de las necesidades del cliente es el primer elemento en el sistema de servucción; el cliente, en este sentido, debe sentirse estimulado y motivado para solicitar el servicio que se vaya a prestar.

Seguidamente se encuentra el tener un soporte físico apto para la prestación del servicio, para lo cual se debe disponer de un soporte material excelente para la prestación de un buen servicio.

La servucción es todo el engranaje detrás de la prestación de un buen servicio. Así mismo, siempre estaremos en contacto con alguna persona que será la responsable de la atención en determinado lugar. En el sector financiero nos referimos al personal del *front office*. Este tercer punto es de vital importancia (el personal de contacto). La atención personalizada al cliente es un punto de suma importancia en la servucción; el personal encargado debe ser idóneo y estar preparado para satisfacer a cabalidad las necesidades de los consumidores.

Es bueno recordar que el cliente no ve la servucción, sino su resultado. Él es el protagonista principal.

Como un cuarto punto se encuentra el servicio ya prestado y el servicio interno en la empresa. Es indispensable que se realice una estrategia interna en la cual se identifiquen todos los puntos a mejorar y se deleguen funciones en departamentos y en personal calificado. Es necesario comunicar todo lo que se va a hacer para que todos “halen” hacia el mismo lado, hacia la consecución del objetivo final. En el sector financiero nos referimos al *middle office* y al *back office*.

De otro lado, se encuentran los competidores cuyo comportamiento debe evaluarse también para determinar sus fortalezas y debilidades y poder aprender de las posibles ventajas que tengan en comparación con la propia empresa. Cabe recordar que sin competidores simplemente no existirían estrategias para la servucción. Vale la pena destacar este punto, ya que si se está sólo en el mercado, no se tendría una referencia directa en cuanto al servicio prestado.

Por último, desarrollado y estudiado todo lo anterior, se procede al diseño e innovación del servicio como tal.

La innovación también debe existir siempre en la prestación de un servicio. Así mismo tenemos la opción de quejarnos por medio de sugerencias o por intermedio de defensores del consumidor quienes son los encargados de estar al tanto de todo lo que deseamos al ser atendidos.

Ahora que conocemos todo lo que se maneja detrás de la consecución de un servicio, con total seguridad valoraremos mucho más el esfuerzo que se hace por atender todos nuestros deseos y aquellos caprichos que siempre tendremos y su importancia para el diseño e implementación de un sistema de prevención y control del LA/FT en la empresa.

En pocas palabras, podría decirse que para un servicio se necesita mano de obra, un soporte físico y un beneficiario, es decir, un cliente.

Haciendo una representación simplificada de un sistema de servucción, describimos a continuación los elementos ya mencionados que componen dicho sistema:

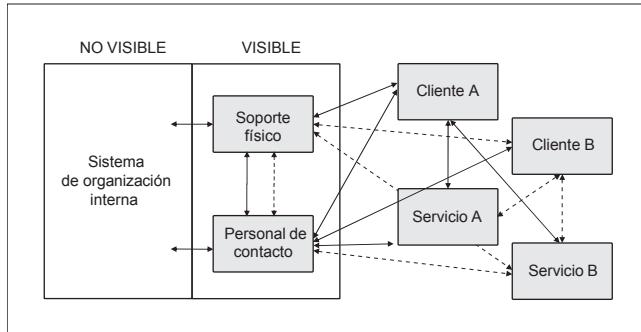
El *cliente*. El consumidor está implicado en la fabricación del servicio. Es un elemento primordial y su presencia es indispensable;

El *soporte físico*. Se trata del soporte material necesario para la producción del servicio. Contempla dos categorías: los instrumentos necesarios para el servicio (muebles, maquinarias) y el entorno material en el que se desarrolla el servicio (locación, edificio, decorado);

El *personal de contacto (PCC)*. Son las personas empleadas por la empresa que están en contacto directo con los clientes, y

El *servicio*. Es el resultado de la interacción de los tres elementos de base: el cliente, el soporte físico y el personal de contacto. Este resultado constituye un beneficio que debe satisfacer la necesidad del cliente.

Gráfico 10
Sistema de servucción complejo



La gran diferencia entre la prestación de un servicio y la fabricación de un producto es que el cliente es un integrante fundamental del sistema de servucción: es a la vez productor y consumidor. Por lo tanto, es clave entender la secuencia de los actos de participación en la servucción que el cliente lleva a cabo para beneficiarse del servicio ofrecido. Tales actos de participación son:

- Actos intelectuales de comprensión, de investigación o de evaluación que preceden a una toma de decisión;
- Actos verbales para finalizar la toma de decisión o para hacer progresar el desarrollo del servicio;
- Actos físicos indispensables para la realización del servicio, y
- Actos de espera entre secuencias.

Pero estos actos de participación podrían tener la intención de la comisión del delito de LA/FT.

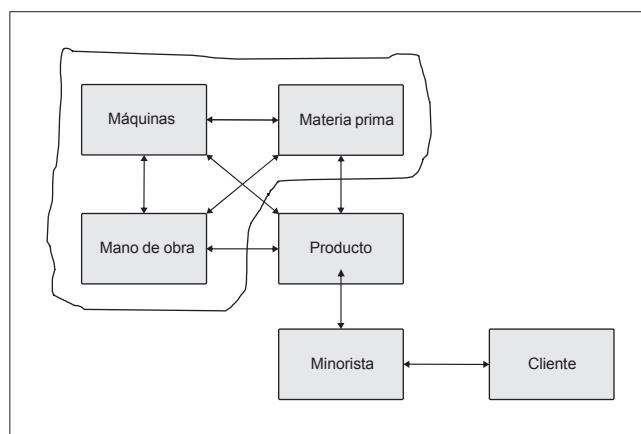
Trabajar sobre los elementos de base y las relaciones entre ellos es lo que permitirá a la empresa brindar servicios de calidad para que logre sobresalir en el mercado. Esto, junto con la definición de procedimientos y políticas de prevención y control, es lo que permitirá que la empresa no sea vulnerable al delito del LA/FT.

5.2.2. *Concepto de producción*

Es un sistema de acciones que se encuentran interrelacionadas de forma dinámica y que se orientan a la transformación de ciertos elementos. De esta manera, los elementos de entrada, conocidos como factores, pasan a ser elementos de salida –productos–, tras un proceso en el que se incrementa su valor.

Los factores son los bienes que se utilizan con fines productivos (las materias primas, la maquinaria, la fuerza laboral, la capacidad gerencial). Los productos están destinados a la venta al mayorista, luego al minorista y finalmente al cliente o consumidor final.

Gráfico 11
Sistema de producción de bienes



Es decir, las máquinas puestas a funcionar gracias a la mano de obra y, las materias primas que generan el producto que se le hace llegar al cliente por intermedio de los minoristas. Este sistema está presente en las empresas del sector real. El anterior diagrama esquematiza lo expuesto.

6. NECESIDADES DE PREVENCIÓN Y CONTROL DEL LA/FT

Las empresas –sea cual sea su naturaleza–, sus directivos, los funcionarios en oficinas de gobierno y las personas en general no quieren ver-

se involucradas activa o pasivamente en operaciones de LA/FT, por tanto, tienen la necesidad de hacer prevención.

6.1. Necesidades de prevención de las empresas

Dentro del contexto organizacional del SARLA/FT o SIPLA/FT, se deben considerar las necesidades de prevención de la empresa. Tanto directivos, empleados como funcionarios son conscientes de los altos niveles de riesgo operativo a los que está expuesta la empresa en virtud del manejo de dineros y del cumplimiento de normas establecidas por los entes de control, lo cual exige manejo de procesos y diseño e implementación de actividades de control que minimicen el impacto y la frecuencia del riesgo operativo.

La empresa a través de su SARLA/FT, con adecuadas propuestas de valor, debe garantizar a sus *stakeholders* que sus operaciones están protegidas de ser utilizadas en forma directa –es decir, a través de sus accionistas, administradores y vinculados– como instrumentos para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o del ocultamiento de activos provenientes de dichas actividades.

6.2. Necesidades de prevención del Estado

La Superintendencia Financiera de Colombia obliga a las entidades vigiladas a cumplir con el SIPLA/FT o el SARLA/FT. A este tema nos hemos referido ampliamente en la primera parte del libro.

6.3. Necesidades de *stakeholders* o partes interesadas

Todos los públicos desean sostener relaciones comerciales con una empresa que prevenga y controle el impacto del riesgo de LA/FT a través de un sistema de administración de ese riesgo.

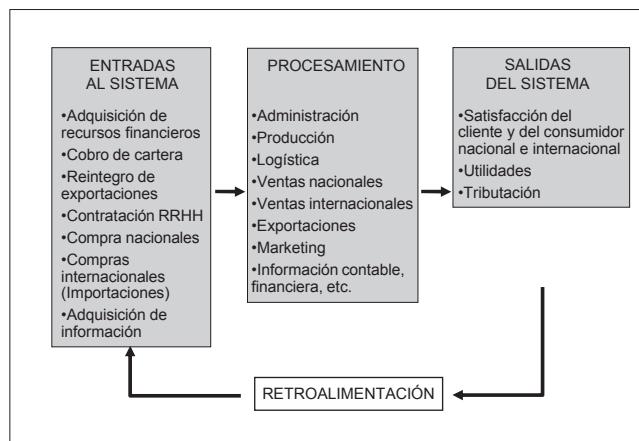
7. SISTEMA EMPRESARIAL DE PRODUCCIÓN: MACROPROCESOS Y PROCESOS DEL SISTEMA

Con el fin de lograr una mejor comprensión de las características de los factores que exponen a la organización al riesgo de LA/FT, debemos recurrir a la aplicación del enfoque sistémico de procesos.

Es decir, podemos considerar la organización como un sistema en el que se realizan procesos de contratación, compras, reintegro y cobros (entradas): capital, recursos humanos, materias primas, equipos de producción e información que son coordinados y utilizados mediante procesos de administración, producción, logística, comercialización nacional e internacional –*marketing*– y de generación de información contable, financiera, para la producción (salida) de bienes y servicios a fin de satisfacer necesidades y deseos de clientes y consumidores nacionales e internacionales y la generación de utilidades para los socios y tributación para el Estado.

El siguiente gráfico ilustra lo expresado:

Gráfico 12
El sistema de producción como un proceso



7.1. Enfoque sistémico de la organización y factores que la exponen al riesgo de LA/FT

En una empresa, en consideración al análisis anterior, por las razones que exponemos a continuación y por su naturaleza, los factores que la exponen al riesgo de lavado de activos y financiación del terrorismo son los siguientes:

Clientes. Este factor está relacionado con los propietarios de canales de distribución mayoristas y minoristas, nacionales e internacionales, especialmente los mayoristas que adquieren los productos de la empresa y quienes los utilicen con fines industriales.

Proveedores. Se deben considerar los proveedores de insumos y materias primas, porque algunos podrían utilizar dineros de procedencia ilegal para su producción. Una de las formas que usan los “lavadores de dinero” es ofrecer insumos con precios muy bajos con respecto al mercado.

Jurisdicciones geográficas. Son las áreas geográficas nacionales donde se comercializan los productos donde están las ciudades y poblaciones con algún nivel de exposición al LA/FT por la presencia del narcotráfico y guerrilla.

Logística de las ventas nacionales y exportaciones. Porque en los procesos y recursos utilizados para el empaque, despacho y transporte, los prestadores de estos servicios podrían estar incluyendo dineros o artículos ilícitos. Un alto nivel de riesgo se presenta cuando se trabaja con transportadores o distribuidores externos a la empresa.

Operaciones de comercio exterior. Para la logística de la importación y exportación se debe tener claro quién recibe la mercancía, en dónde es almacenada y quiénes son los operadores de efectivo de divisas, porque se podría dar la suplantación de la empresa para importar o exportar y lavar el dinero.

Recurso humano. Utilizado en las áreas administrativas y de producción. El mayor riesgo se presenta cuando se trabaja con empleados temporales. Hay que identificar los empleados con nivel de vida elevado con relación a sus ingresos, y el pago en efectivo de grandes sumas de dinero por parte de los clientes.

CAPÍTULO 3

Propuesta metodológica

En una propuesta metodológica que conduzca a la implementación de cualquiera de los sistemas de prevención de lavado de activos, se deben considerar los mecanismos que establecen las regulaciones administrativas internas expedidas por las autoridades de supervisión, control y vigilancia. En el caso colombiano, la Superintendencia Financiera por medio de su Circular 022 de 2007, ha señalado dos mecanismos relevantes: (i) la identificación y análisis de operaciones inusuales, y (ii) la determinación y reporte de operaciones sospechosas.

Por tanto, en el SIPLA/FT como en el SARLA/FT, las operaciones inusuales (OI) y las operaciones sospechosas (OS) constituyen conceptos y herramientas determinantes, como se explicará, en el entendido que resulta necesario establecer: quiénes son los responsables de su identificación y detección y cuál es el procedimiento que se debe seguir para el efecto; describir la asociación de una operación sospechosa con un evento de riesgo de LA/FT; establecer los componentes de una operación sospechosa; describir el proceso general que se debe seguir para identificar operaciones inusuales y detectar operaciones sospechosas; exponer la forma como se deben realizar los reportes de operaciones sospechosa (ROS); explicar y caracterizar la gestión del SIPLA/FT y del SARLA/FT mediante riesgos en procesos; definir las metodologías y procesos de las etapas de administración del SARLA/FT, entre ellas la que denominamos “espina de pescado” y definir qué es un evento de riesgo de LA/FT, entre otros aspectos.

Relación entre operaciones totales, normales, inusuales y sospechosas

En el contexto de la normatividad internacional y colombiana sobre prevención y control del riesgo de LA/FT y, en el proceso de servucción

de empresas del sector financiero, podemos identificar las siguientes variables:

- a) Cantidad de operaciones inusuales (OI) identificadas con respecto a la cantidad de operaciones realizadas en el mes;
- b) Cantidad de operaciones sospechosas (OS) detectadas con respecto a la cantidad de operaciones realizadas en el mes;
- c) Cantidad de operaciones normales (ON) realizadas;
- d) Cantidad de operaciones totales (OT) realizadas;
- e) Cantidad de operaciones individuales, o sea las realizadas por un solo cliente, a quien corresponde, por ejemplo un solo número de documento de identidad, una sola dirección y un solo teléfono, y
- f) Cantidad de operaciones múltiples (OM), es decir, las realizadas por un grupo de clientes quienes se identifican con números de documento de identidad diferentes pero que reportan, por ejemplo, igual número telefónico, igual número de cuenta corriente o de ahorros en la misma entidad financiera, igual número telefónico e incluso igual dirección residencial.

Entre estas variables existen las siguientes relaciones:

El conjunto de la OT se puede desagregar en el subconjunto de las ON, el subconjunto de la OI y el subconjunto de las OS.

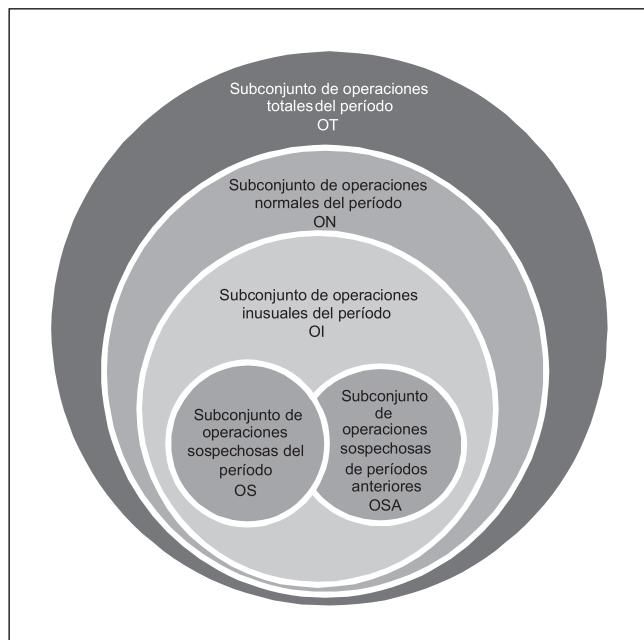
Las ON son aquellas que no pertenecen al subconjunto de las OI ni de las OS.

El subconjunto de las OS pertenecen al subconjunto de las OI.

La cantidad de OS podrá ser igual o mayor que la de OI. La desigualdad se presenta debido a que para detectar las OS correspondientes al mes es necesario realizar un rastreo de las operaciones realizadas por los mismos clientes en meses anteriores a fin de poder remitir a la UIAF operaciones que razonablemente hagan presumir la comisión del delito de LA/FT.

La detección y la cuantificación de las operaciones sospechosas (OS) es uno de los propósitos del SIPLA/FT y del SARLA/FT; por tanto, estas son una expresión del riesgo de LA/FT a que está expuesta la empresa.

Gráfico 13
Relación entre operaciones totales, normales, inusuales y sospechosas



1. OPERACIONES SOSPECHOSAS Y OPERACIONES INUSUALES

En los términos más generales, debemos decir que quienes participan en el proceso de identificación de operaciones inusuales son aquellas personas vinculadas a la empresa con la responsabilidad de participar o ejecutar directamente las actividades de cada uno de los macroprocesos de la compañía.

Los procesos de identificación de operaciones inusuales y de detección de operaciones sospechosas pueden ser considerados como un siste-

ma, en el cual las “entradas al sistema” son todos los tipos de operaciones que realiza la empresa; la aplicación de normas externas y políticas internas de todo tipo, metodologías y conceptos corresponden a la “caja negra” del sistema; y las “salidas” son los informes para uso tanto interno como externo que se deben producir, especialmente el de operaciones sospechosas.

1.1. Identificación de operaciones inusuales

Para que los empleados, funcionarios o directivos de la empresa identifiquen una operación inusual primero deben *percibir* uno o varios de los diferentes tipos de señales de alerta que expondremos posteriormente. Es decir, *percibir*, lo cual quiere decir *recibir*, a través de los sentidos, imágenes, impresiones o sensaciones externas; también se refiere a *comprender* o *conocer* algo.

Por lo anterior, las señales de alerta se deben buscar (en este caso, “percibir”) en los factores de riesgo y sus correspondientes situaciones de riesgo. Hay que tener en cuenta que aquellas siempre están asociadas a operaciones inusuales (OI). A continuación exponemos algunos ejemplos:

- Indicadores que muestran el incumplimiento de políticas sobre límites y topes establecidas por la empresa.
- La presencia de operaciones múltiples (OM).
- La presencia de operaciones por grandes cantidades de dinero realizadas en efectivo.
- Cuando en el perfil del cliente se exceden los parámetros definidos para su segmento de mercado.
- Las actitudes y comportamientos de quienes intervienen en los procesos de la empresa.

En el procedimiento para identificar operaciones inusuales se hace patente la utilidad de la metodología de la “espina de pescado” y la de los

“cinco por qué”, Dicho procedimiento está en concordancia con la terminología y metodología que hemos expuesto.

Para su documentación debemos partir de las siguientes premisas:

— El subconjunto de operaciones sospechosas (OS) siempre pertenece al subconjunto de operaciones inusuales (OI).

— El subconjunto de operaciones inusuales (OI) está comprendido en el conjunto de operaciones totales (OT) de la empresa.

Una operación sospechosa (OS) siempre será un evento de riesgo de LA/FT.

— La palabra “identificar” es un concepto que puede implicar variadas interpretaciones; por tanto, si esta palabra se utiliza para denotar una acción a emprender dentro de un proceso, se pueden producir resultados no homogéneos, lo cual consideramos funesto para la prevención y control del LA/FT.

— Para subsanar esta dificultad preferimos utilizar la palabra “buscar”; dicho entonces de este modo, se deben buscar operaciones inusuales (OI) o eventos de riesgo de LA/FT.

— Para buscar los eventos de riesgo de LA/FT es necesario proporcionar algunos elementos que faciliten su encuentro.

— Esos elementos son los enunciados en la metodología de la “espiña de pescado” los cuales son: (1) *señales de alerta* que se pueden percibir en (2) *situaciones de riesgo* en las que intervienen (3) *factores de riesgo* cuando se realiza cualquier tipo de (4) *operación* en la empresa.

El procedimiento de búsqueda de operaciones inusuales (OI) conlleva las siguientes actividades:

a) Percibir o darse cuenta de la presencia de una señal de alerta. Darse cuenta de una señal de alerta debería ser consecuencia de la aplicación de un procedimiento sistemático de búsqueda que requiere tener un amplio dominio de las señales de alerta. A manera de orientación, presentamos una lista de los diferentes tipos de señales de alerta expuestas en otra parte del libro:

- Señales de alerta en el proceso de venta.
 - Señales de alerta por operaciones múltiples.
 - Señales de alerta por operaciones individuales.
 - Señales de alerta en operaciones internacionales.
 - Señales de alerta institucionales internas.
 - Señales de alerta generales.
 - Señales de alerta en personas jurídicas.
 - Señales de alerta en personas naturales o jurídicas.
 - Señales de alerta propias que arroja el sistema operativo de la empresa.
 - Señales de alerta generales en clientes o usuarios;
- b) Describir la operación inusual utilizando los elementos que facilitaron su percepción y utilizando un formato especialmente diseñado para ello;
- c) Denominar la operación inusual, es decir, asignarle un nombre breve que facilite posteriormente su referenciación;
- d) Remitir formato a superior inmediato;
- e) El superior inmediato debe evaluar y aprobar el informe en términos de su confiabilidad y calidad como expresión de una operación inusual (OI), y
- f) Remitirlo al comité de evaluación de operaciones para que este determine si se trata de una operación sospechosa (OS).

1.2. Detección de operaciones sospechosas

El procedimiento para detectar operaciones sospechosas (OS) sólo debe ser realizado por el oficial de cumplimiento o por el comité evaluador de operaciones, los cuales deben verificar si:

— La descripción de la operación inusual cumple con los requerimientos de las políticas y metodologías establecidas por la empresa.

— La documentación de, por ejemplo, conocimiento del cliente, pruebas que evidencien las señales de alerta de la operación inusual, certificados de origen de los dineros y demás documentos requeridos por el buen criterio evidencian el cumplimiento de la “debida diligencia”.

— La operación inusual (OI) obedece la normatividad oficial y la normatividad interna, incluido el manual de gestión del SARLA/FT o del SIPLA/FT de la empresa según el caso, para que dicha operación pueda ser calificada como sospechosa.

Los criterios que debe utilizar el comité de evaluación de operaciones para determinar si una operación inusual (OI) corresponde a una operación sospechosa (OS) son: la evaluación objetiva del contenido de la operación inusual (OI) y el buen criterio personal de sus integrantes, y la aplicación de las políticas establecidas por la empresa para determinar operaciones sospechosas (OS).

No se recomienda, para este propósito, la utilización de calificación mediante puntajes (*scoring*), porque se podría caer en el error de perder la objetividad del análisis.

Para la identificación de operaciones inusuales (OI), se recurre a políticas y procedimientos en los cuales se establecen parámetros cuantitativos y cualitativos contra los cuales se comparan las características y elementos de la operación; mientras que para la detección de operaciones sospechosas (OS) se podrían utilizar las mismas políticas y procedimientos, pero con parámetros más exigentes y criterios personales más rigurosos.

1.3. Ejemplos de identificación y detección de OI y OS por OM

A continuación presentamos una operación múltiple (OM) definida con parámetros que, según políticas de la empresa, se podrían calificar como una operación inusual (OI) y como una operación sospechosa (OS).

Tabla 7
Identificación y detección de OI y OS por OM

Parámetros de la OM	OS	OI
Período considerado de tiempo	6	3
Cantidad de operaciones	9	5
Valor acumulado de las operaciones	US\$ 120.000	US\$ 90.000
Cantidad de clientes/teléfonos/direcciones/ diferentes que intervienen en las operaciones múltiples	3	2
Cantidad de oficinas diferentes en las cuales se realizaron las operaciones	2	4

Tabla 8
OI y OS por perfiles de segmentos de clientes

Parámetros de la OM	OI	OS
Valor máximo de la operación realizada por un cliente que pertenezca al perfil	US\$ 1.200	US\$ 1.200
Valor promedio de operación realizada por los clientes que pertenecen al perfil	US\$ 800	US\$ 800
Valor mínimo de la operación realizada por un cliente que pertenezca al perfil	US\$ 350	< US\$ 350
Cantidad promedio de operaciones realizadas en un período de tiempo por los clientes que pertenecen al perfil	7	9
Frecuencia promedio de operaciones de los clientes que pertenecen al perfil	6	4

1.4. Responsables en el proceso de identificación de OI y detección de OS

El proceso inicia con la percepción de señales de alerta que permiten identificar operaciones inusuales. A continuación relacionamos las tareas que deben realizar los responsables que interactúan en el proceso de identificación de operaciones inusuales (OI) y detección de operaciones sospechosas (OS):

- El área de ventas es la responsable de identificar operaciones inusuales entre sus clientes en cada jurisdicción geográfica.
- El área de compras es la responsable de identificar operaciones inu-

suales entre todos sus proveedores, tanto nacionales como internacionales.

— El área de logística debe identificar operaciones inusuales en los procesos de transporte y distribución física.

— El área de recursos humanos es la responsable de identificar operaciones inusuales entre todas las personas vinculadas laboralmente.

Cada una de las áreas debe diligenciar el formato de reporte de operación inusual para que sea evaluado por la gerencia de cada área y se remita al comité evaluador de operaciones inusuales.

El comité evaluador de operaciones inusuales determinará, entre las operaciones inusuales, cuáles son las operaciones sospechosas y producirá un acta de cada una de sus reuniones, la cual se remitirá al oficial de cumplimiento.

El oficial de cumplimiento remitirá trimestralmente a la UIAF el reporte operaciones sospechosas. Si el oficial de cumplimiento o el mencionado comité no detectan operaciones sospechosas, de todas formas el mencionado reporte también debe enviarse.

2. OPERACIÓN SOSPECHOSA Y SU ASOCIACIÓN CON UN EVENTO DE RIESGO DE LA/FT

Según la Superintendencia Financiera de Colombia, en su Circular Externa 022, una operación sospechosa (OS) es toda operación inusual (OI) que, de acuerdo con razones objetivas establecidas por la entidad, es identificada como sospechosa porque está relacionada con el delito del LA/FT, la cual deberá ser reportada a la UIAF.

En términos prácticos, una operación sospechosa (OS) corresponden a toda operación realizada por la organización que, por su número, cantidad o características, no se enmarca dentro de los sistemas y prácticas normales del negocio y que, de acuerdo con los usos y costumbres de la actividad que se trate, no haya podido ser razonablemente justificada. Estas son las operaciones que deben ser reportadas a la UIAF en el reporte de ope-

raciones sospechosas (ROS).

De acuerdo con nuestra metodología, una operación sospechosa (OS) también puede ser denominada como evento de riesgo de LA/FT (ERLA/FT) y sus componentes son los mismos de las operaciones inusuales (OI).

3. REPORTE DE OPERACIONES SOSPECHOSAS (ROS)

Corresponde a la organización reportar a la UIAF en forma inmediata las operaciones que se determinen como sospechosas. Así mismo, se deberán reportar las operaciones intentadas o rechazadas que contengan características que les otorguen el carácter de sospechosas de LA/FT. Estos reportes deben ajustarse a los criterios y objetivos establecidos por la entidad.

Consideramos que los responsables en la empresa para la detección de operaciones sospechosas son el comité evaluador de operaciones inusuales y/o el oficial de cumplimiento, quienes tienen en la empresa la responsabilidad y la participación (actuación) para determinar si una operación inusual puede ser calificada como operación sospechosa y, además, concluir si se trata o no de una operación sospechosa.

Ese reporte y la decisión del comité deben quedar en poder del oficial de cumplimiento para su reporte a la UIAF, pues es el único funcionario con autoridad, responsabilidad y colaboración para informar sobre las operaciones sospechosas determinadas por el comité SIPLA/FT.

—*Procedimiento para reportar a la unidad de información y análisis financiero (UIAF) las operaciones sospechosas*

En Colombia se debe utilizar el sistema de reporte en línea, el cual es un sistema de información en ambiente web, desarrollado por la UIAF como mecanismo principal para recibir los reportes de información en línea. Para acceder a este sistema se requiere de un computador con acceso a Internet y el navegador Internet Explorer 6.0 o superior.

Para registrarse en el sistema se ingresa a la página principal del aplicativo y se hace clic en la opción “solicitud de acceso”. Luego se diligencia el formulario que aparece en pantalla y se presiona el botón enviar. La UIAF verificará la solicitud y por correo electrónico será enviado el usuario y contraseña que le permitirá ingresar a la aplicación, información que debe quedar únicamente en poder del oficial de cumplimiento o de quien sea designado por la empresa para ejecutar dicha tarea.

El instructivo producido por la UIAF para el propósito anterior está disponible en la página web <http://www.uiaf.gov.co/idcategoria=2626&uiaf_2008=35eb0bd30c1df20aae63f82dde1d9e51>.

Resumiendo lo anterior, corresponde al oficial de cumplimiento reportar en forma inmediata a la UIAF, de acuerdo a concepto del comité evaluador de operaciones inusuales, cualquier operación que se determine como sospechosa. El reporte inmediato se tomará a partir de que la operación haya sido calificada como “sospechosa” por parte de la mayoría de los integrantes del comité evaluador de operaciones inusuales.

En estos casos no se requiere que la empresa tenga certeza de que se trata de una actividad delictiva, ni identificar el tipo de delito penal o que los recursos involucrados provengan de tales actividades.

En el evento de que durante un período la empresa no haya determinado la existencia de operaciones sospechosas, se debe informar este hecho a la citada UIAF, dentro de los diez (10) primeros días del mes siguiente.

De acuerdo con lo consagrado en el artículo 42 de la Ley 190 de 1995, el reporte de operaciones sospechosas no dará lugar a ningún tipo de responsabilidad para los funcionarios de la empresa en su calidad de informantes, ni para los directivos o empleados que hayan participado en su detección y/o reporte.

Será el comité evaluador de operaciones inusuales quien establezca las razones objetivas para determinar si una operación o un grupo de operaciones deben ser calificados como sospechosas.

Para establecer las razones objetivas, se deberán atender las señales de alerta incluidas en cada operación inusual más los otros elementos que la configuran; el comité evaluador de operaciones inusuales podrá tener en cuenta señales de alerta relacionadas con: posibles vínculos entre operacio-

nes por variables como nombres de clientes/agentes económicos, teléfonos, direcciones, ubicación geográfica; comportamiento de los clientes/agentes económicos dentro del mercado, y/o también por inconsistencias entre los valores declarados de ingresos, egresos, activos, patrimonio y su perfil financiero dentro de la empresa. También podrá analizar los datos históricos para el último año, realizar llamadas para corroborar o verificar la información de las bases de datos del aplicativo operativo y/o de los documentos físicos.

Dependiendo del juicio y criterios del comité, unas operaciones serán consideradas sospechosas y aunque otras no, sí pueden ser inusuales, por tanto sometidas a un seguimiento o monitoreo especial mediante el uso de listas de control o, en su defecto, se dejará constancia de la decisión en el acta del comité.

En todo caso, antes de transmitir a la UIAF el respectivo reporte de operaciones sospechosas (ROS), se deberá atender a las recomendaciones de esa entidad en cuanto a características de calidad de la información, según los documentos expedidos en forma general o según informes de retroalimentación emitidos en forma particular para la empresa o para el sector real.

El asistente del oficial de cumplimiento, o quien desempeñe sus funciones, será el responsable del envío de este reporte a la UIAF.

El comité evaluador de operaciones inusuales, en cabeza del oficial de cumplimiento, será el responsable de mantener en custodia el archivo generado de las operaciones sospechosas por el mismo año calendario al que pertenezcan las respectivas operaciones. Una vez terminado el año, los soportes de las operaciones sospechosas podrán ser enviados al archivo de la empresa. Tal documentación será organizado en orden cronológico conforme las fechas de reporte de las mismas a la UIAF.

4. GESTIÓN DEL SIPLA/FT Y DEL SARLA/FT MEDIANTE RIESGOS EN PROCESOS

Como ya lo expresamos, la empresa debería ser gestionada mediante procesos, por tanto el SIPLA/FT y el SARLA/FT también deberían serlo al interior de la organización. Además, tales sistemas se encuentran estrechamente interrelacionados con los procesos direccionales, procesos de realización o misionales y procesos de apoyo de la empresa.

Por eso, la metodología aplicada a dichos sistemas de administración de riesgos corresponde a pasos sistemáticos e interrelacionados mediante los cuales se administran todos los riesgos al interior de la organización.

4.1. Gerencia o gestión de riesgos por procesos

Se refiere a garantizar que la empresa está previendo y controlando los riesgos de cualquier tipo contenidos en un proceso. Entre otros, la gestión de riesgos por procesos permite:

- a) Eliminar las causas fundamentales del riesgo;
- b) Garantizar que los procesos de la empresa sean gerenciados donde se ejecutan;
- c) Garantizar que los riesgos a que está expuesta la empresa son identificados, evaluados, controlados y monitoreados en el proceso donde ocurren, y
- d) Mantener los niveles de protección logrados y mejorarlos.

La administración del riesgo de LA/FT en la empresa, al igual que la administración de todos los riesgos (SARO, SARM, SARC, etc.), corresponde a una política de gestión por parte de la alta dirección y cuenta con la participación y compromiso de todos sus empleados.

La gestión de riesgos por procesos se define como una estructura o sistema aplicado al proceso de toma de decisiones y el aseguramiento de que estas decisiones son puestas a funcionar, en relación a la *prevención* y *control* de los efectos adversos que en la organización pudiera tener la materialización de eventos de riesgo de LA/FT a los cuales la organización está expuesta y que, por tanto, pudieran comprometer el cumplimiento de sus objetivos.

4.2. Caracterización del proceso de gestión del SIPLA/FT y del SARLA/FT

La gestión del SIPLA/FT y del SARLA/FT, considerada como un proceso, tiene por objetivo prevenir y controlar el riesgo de lavado de activos

y de la financiación del terrorismo y sus riesgos asociados, velando para que la organización logre el cumplimiento de la misión y objetivos corporativos con el menor impacto posible de riesgo. En la empresa el responsable directo del proceso de gestión del SIPLA/FT y del SARLA/FT debería ser el gerente de riesgos.

A continuación se presentan esquemas que caracterizan el contenido de los dos procesos de gestión:

Gráfico 14
Caracterización del proceso de gestión del SIPLA/FT

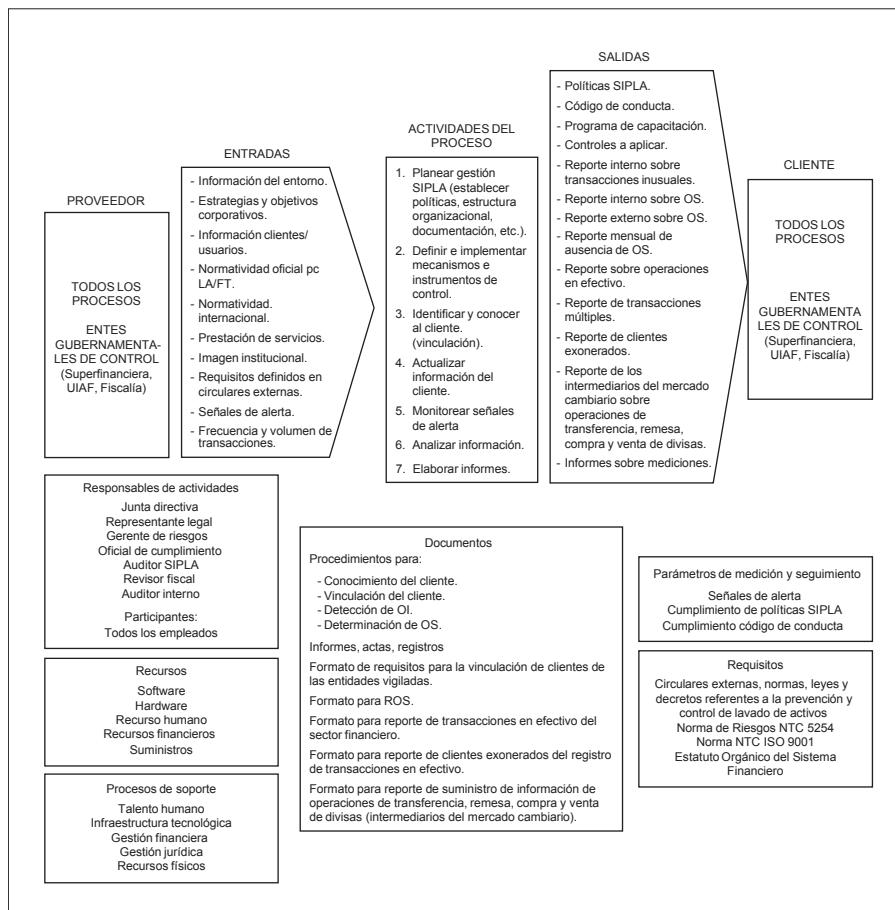
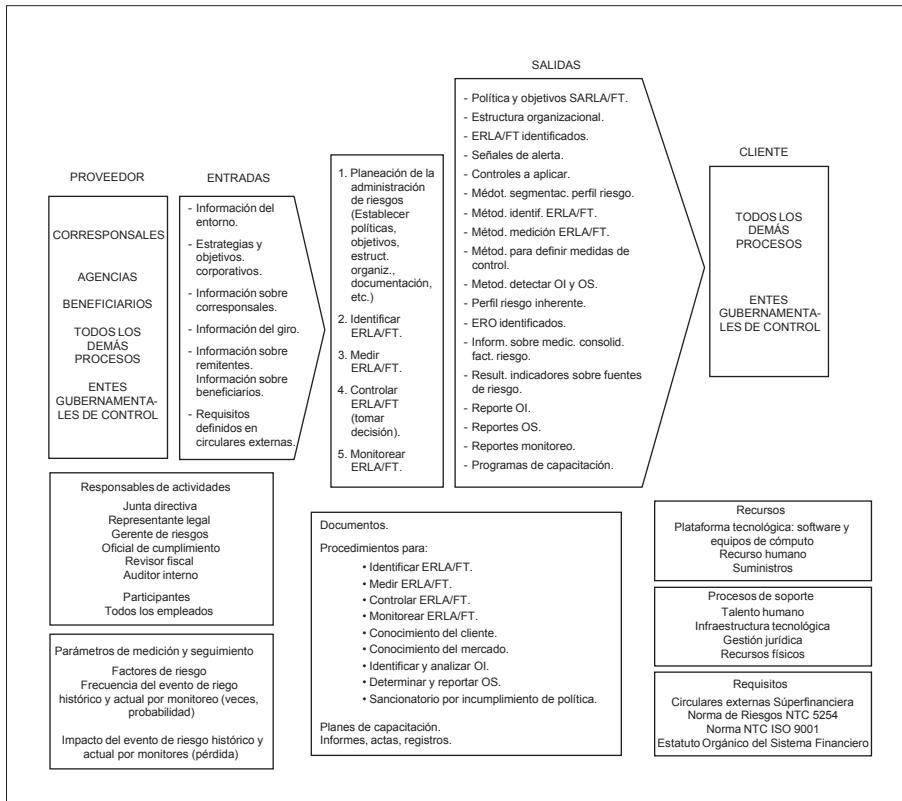


Gráfico 15
Caracterización del proceso de gestión del SARLA/FT



4.3. Lógica del proceso SARLA/FT

Es la que se describe a continuación:

Tabla 9
Lógica del proceso SARLA/FT

Pregunta	Respuesta
¿Necesita encontrar y describir los eventos de riesgo de LA/FT que amenazan a la empresa?	Utilice la técnica de la “espina de pescado” y resuelva la relación causa existente en él; luego elabore una definición de evento de riesgo de LA/FT para la empresa.
¿Por qué debe buscarlos?	Porque entorpecen o impiden el logro de los objetivos de la empresa.
¿Cómo debe buscarlos?	Segmentando todos y cada uno de los factores de riesgo para determinar las UE.
Si debe buscarlos, ¿dónde se buscan?	Búsquelos dentro de la empresa en las UE y también fuera de ella. Búsquelos también en las actividades y actitudes de las partes interesadas.
¿Cómo debo llamarlo?	Debe ponerle un nombre a cada evento de riesgo de LA/FT.
¿Qué hago con él cuando lo encuentre?	Mídalo.
¿Qué es necesario medirles?	La frecuencia, el impacto y su severidad.
¿Para qué lo mide?	Para determinar su severidad (qué tan grave es).
Y luego, ¿qué hago?	Controlarlo.
¿Y después?	Continuar monitoreándolo.

Dado que el Sistema de Administración del Riesgo Operativo (SARO) y el Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo (SARLA/FT) son coincidentes en las etapas definidas para la administración de riesgos: identificación, medición, control y monitoreo, la empresa podría aplicar el mismo modelo metodológico adaptando los términos o elementos según corresponda.

El objetivo de este procedimiento es establecer las directrices para identificar, medir, controlar y monitorear los eventos de riesgo de LA/FT asociados a las unidades estratégicas (UE) definidas por la empresa para el desarrollo de su negocio.

El proceso de gestión de un evento de riesgo de LA/FT, para su aplicación: comprende las etapas de identificación, medición, control, registro y monitoreo; e implica observar y cumplir con:

- Las políticas internas de gestión del SARLA/FT.
- Las recomendaciones y/o requerimientos de la SFC.
- Las actividades propias de la empresa, especificadas para cada etapa.
- Las especificaciones de la norma NTC 5254 (gestión de ingresos).
- Las especificaciones de las mejores prácticas en gestión de riesgos.

4.4. Breve presentación de metodologías y procesos de las etapas de administración del SARLA/FT

En general, para quien se aproxima por primera vez a esta temática, consideramos que la lectura de la Circular Externa 026 DE 2008 emanada de la Superintendencia Financiera de Colombia o del ente de vigilancia y control en cualquier país siempre le causará la inquietante pregunta sobre ¿qué debe hacer para comenzar a implementar el SARLA/FT?

Para efectos de diseño e implantación del SARLA/FT en una empresa, proponemos lo siguiente: este sistema se debe diseñar e implementar teniendo en consideración las características del contexto de la empresa, el cual, de una u otra forma, determina la manera como se resolverán las etapas de identificación, evaluación o medición, control y monitoreo de eventos de riesgo de LA/FT. Esto requiere que se realice un diagnóstico de la empresa, teniendo la perspectiva de los riesgos, para determinar sus fortalezas y debilidades.

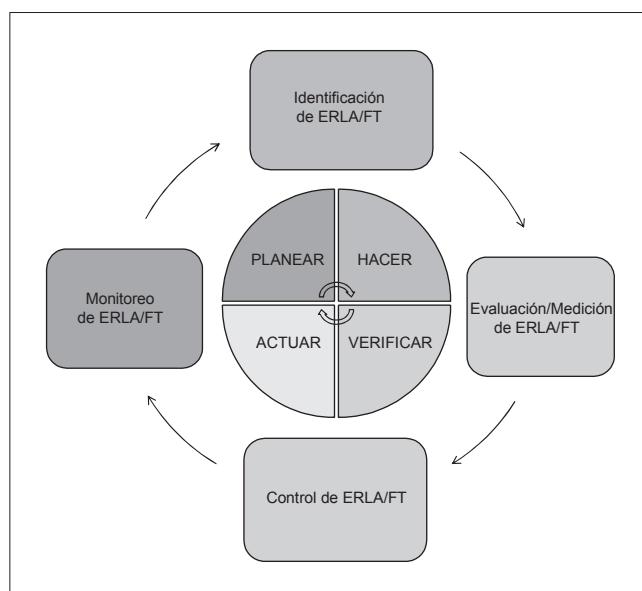
Cada una de las etapas de la gestión del riesgo de LA/FT debe ser planeada, ejecutada (diseñada), verificada y actuada (implementada), de conformidad con lo explicado en la parte del libro referente al ciclo PHVA.

La gestión de riesgos y en particular el riesgo de LA/FT por su naturaleza conlleva un conjunto de conceptos, algunos articulados en el tema de las etapas de la gestión del riesgo, otros en el de las fases de prevención y control y muchos que podríamos llamar “sueltos” (la Circular Ext. 061 de 2007 de la SFC sobre SARLA/FT no está exenta de nuestra observación).

Los modelos esquemáticos que a continuación presentamos tratan de articular visualmente la mayor cantidad de conceptos y metodologías expresadas por la SFC y por el autor de esta parte del libro con referencia a la gestión del riesgo de LA/FT.

Las etapas para la administración del riesgo corresponden a las establecidas por la SFC: identificación, medición, control y monitoreo.

Gráfico 16
Relación entre el ciclo PHVA y las etapas del SARLA/FT



5. METODOLOGÍA DE LA ESPINA DE PESCADO Y DEFINICIÓN

DE EVENTOS DE RIESGO DE LA/FT

La identificación de eventos de riesgo de LA/FT, que según nuestra metodología, es el primer proceso que corresponde a la primera etapa del SARLA/FT o del SIPLA/FT, debe ser aclarada y analizada más profundamente:

La simple identificación de eventos de riesgo de LA/FT solo permite el señalamiento de estos. Pero para poder señalarlos es necesario primero hallarlos y luego sí describirlos. Es casi imposible que se hallen eventos de riesgo de LA/FT, si no se dice *qué son* los eventos de riesgo de LA/FT, en dónde buscarlos, igual que si se describen y no se dice en qué consiste.

Por ahora diremos que:

1. Un *evento de riesgo de LA/FT* es la ocurrencia de una *situación de riesgo* que se percibe mediante *señales de alerta*, observadas en los *factores de riesgo* que integran una *unidad estratégica de negocio (UEN)*, y que responde a ciertas *causas* que hacen prever la posibilidad de *impactos negativos* para la empresa cuando alguien pretende utilizarla o la utiliza como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando pretende el ocultamiento de activos provenientes de dichas actividades. (Los resaltados son *los elementos que conforman un evento de riesgo de LA/FT*).
2. Para hallar eventos de riesgo de LA/FT preferencialmente se deben buscar en los *procesos* de la empresa.
3. Para describir un evento de riesgo de LA/FT se debe hacer a partir de *los elementos que lo conforman*.

De esta forma y ya en el contexto total del SIPLA/FT o del SARLA/FT lo que vamos a identificar (buscar-hallar-describir), medir, controlar y monitorear son eventos de riesgo de LA/FT.

Por tanto, la identificación es la primera etapa, quizás la más importante, por lo que ya especificamos del SIPLA/FT o del SARLA/FT; y para lograr su ejecución, hemos elaborado una metodología que permite identificarlos, describirlos y hallarlos de manera confiable.

Entonces, si vamos a identificar un evento de riesgo de LA/FT, debemos saber en dónde buscarlos, qué método se debe utilizar para buscarlos, cuáles son los elementos que los conforman y qué permiten su descripción; para lo cual, las otras preguntas que surgen inmediatamente son:

Tabla 10

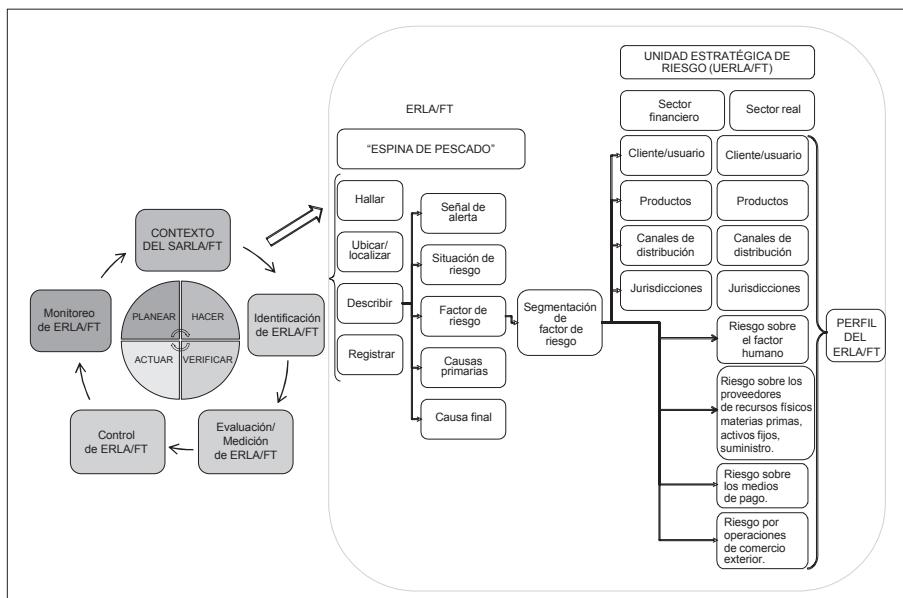
Preguntas claves para las etapas del SERLA/FT y del SIPLA/FT

Pregunta	Respuesta
¿Qué es lo que se debe identificar, medir, monitorear y controlar?	Los eventos de riesgo de LA/FT
¿En dónde puedo localizarlos?	En las Unidades Estratégicas (UE)
¿Cómo puedo hallar los eventos de riesgo de LA/FT y qué método puedo utilizar para buscarlos?	Utilizando el método de solución de la resolución causa-efecto, como por ejemplo el diagrama de “espina de pescado”
¿Cuáles son sus componentes?	Los componentes se deducen de la “espina de pescado” Un evento de riesgo de LA/FT está integrado por situaciones de riesgo, señales de alerta, causas primarias y causas finales
¿Cómo puedo medirlos?	Mediante la frecuencia, el impacto y su severidad
¿Cómo puedo describirlos?	Mediante el perfil de la UE y el perfil del evento de riesgo de LA/FT

El siguiente diagrama esquematiza lo anterior:

Gráfico 17

Fundamentos de la metodología de la espina de pescado para hallar, identificar y describir eventos de riesgo de LA/FT



5.1. Aplicación general de la metodología de la espina de pescado

Para detectar (hallar, encontrar o descubrir), describir y ubicar eventos de riesgo de LA/FT en una unidad estratégica debemos solucionar la relación causa-efecto existente en todo tipo de riesgos apoyándonos en el diagrama causa-efecto, llamado usualmente diagrama de *Ishikawa* porque fue creado por Kaoru Ishikawa, experto en dirección de empresas interesado en mejorar el control de la calidad; conocido también como diagrama “espina de pescado” porque la forma del diagrama es similar al esqueleto de un pez.

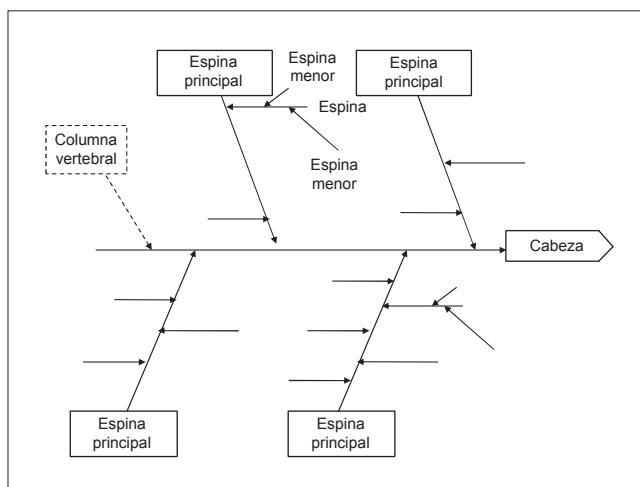
Está compuesto por un recuadro (cabeza), una línea principal (columna vertebral) conformada por cada una de las unidades estratégicas y cuatro o más líneas que apuntan a la línea principal formando un ángulo aproximado de 70° (espinas principales). Estas últimas poseen a su vez dos o tres líneas inclinadas (espinas) y así sucesivamente (espinas menores), según sea necesario.

Consiste en una representación gráfica de las posibles causas en un

sistema, proceso, actividad o situación que pueden contribuir a resolver un problema específico, como por ejemplo el riesgo de lavado de activos.

Utilizando el método de espina de pescado, podemos ilustrar gráficamente la manera en que interactúan los elementos presentes en el riesgo. En el siguiente esquema y ejemplo se presenta la forma general de resolver la relación causa-efecto:

Gráfico 18
Solución general de la relación causa-efecto



Ejemplo de solución de una relación causa-efecto

Con fines solamente didácticos, incluimos una aplicación del uso de este diagrama para encontrar las causas del bajo rendimiento en matemáticas por parte de un grupo de estudiantes. Los factores que podrían determinar ese rendimiento académico en dicha materia y que se diagrama mediante las espinas principales serían*:

(*) La información del ejemplo y los gráficos 18 y 19 fueron tomados de Eduteka-Fundación Gabriel Piedrahita Uribe, según sus políticas de uso. Disponible en web: <www.eduteka.org/modulos/4/123/>.

- a) Los recursos físicos utilizados en el proceso docente;
- b) Los recursos humanos utilizados en el proceso docente, como por ejemplo el profesor de matemáticas;
- c) Las condiciones del estudiante;
- d) Los contenidos curriculares del curso de matemáticas;
- e) Las características de la institución educativa;
- f) El bajo rendimiento en matemáticas, entendido como un *efecto* o consecuencia podría tener como *causas* las características de los *factores* utilizados en el proceso docente en matemáticas, y
- g) La lógica o el concepto de expertos en educación en matemáticas explica el bajo rendimiento académico del grupo en matemáticas desde el punto de vista de:

Los recursos físicos (por la poca cantidad de libros de texto existentes en la institución y/o por la facilidad o dificultad que tienen los estudiantes para disponer de ellos).

El docente en matemáticas (por la adopción de estrategias de clase inadecuadas debido a que estaría realizando actividades poco interesantes para el grupo o estaría asignando tareas inadecuadas, o porque estaría haciendo un uso inadecuado de los recursos, o porque el proceso de evaluación sería inadecuado).

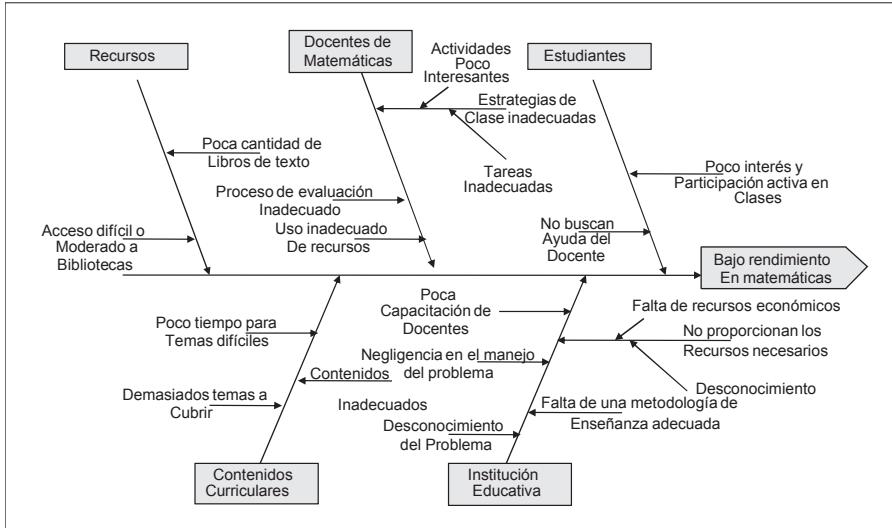
El estudiante (porque ha demostrado poco interés y baja participación en las clases y, además, por no buscar la ayuda del profesor).

El contenido curricular (porque tal vez incluye demasiados temas, o porque son inadecuados y se contempla poco tiempo para temas difíciles).

La institución (por ofrecer poca capacitación a los profesores, porque habría negligencia en el manejo del problema e inclusive desconocimiento del mismo, por no proporcionar los recursos necesarios porque tendría falta de recursos económicos e inclusive desconocería la existencia de esos recursos en el mercado y su metodología de enseñanza sería inadecuada).

En este caso, la espina de pescado ilustraría el asunto de la siguiente manera:

Gráfico 19
Ejemplo de solución de una relación causa-efecto



5.2. Aplicación de la metodología de la espina de pescado en un evento de riesgo de LA/FT

Cada vez que se determine una nueva unidad estratégica (UE) deben analizarse, sus características, la incursión en un nuevo mercado, la apertura de operaciones en nuevas jurisdicciones y el lanzamiento o modificación de los canales de distribución.

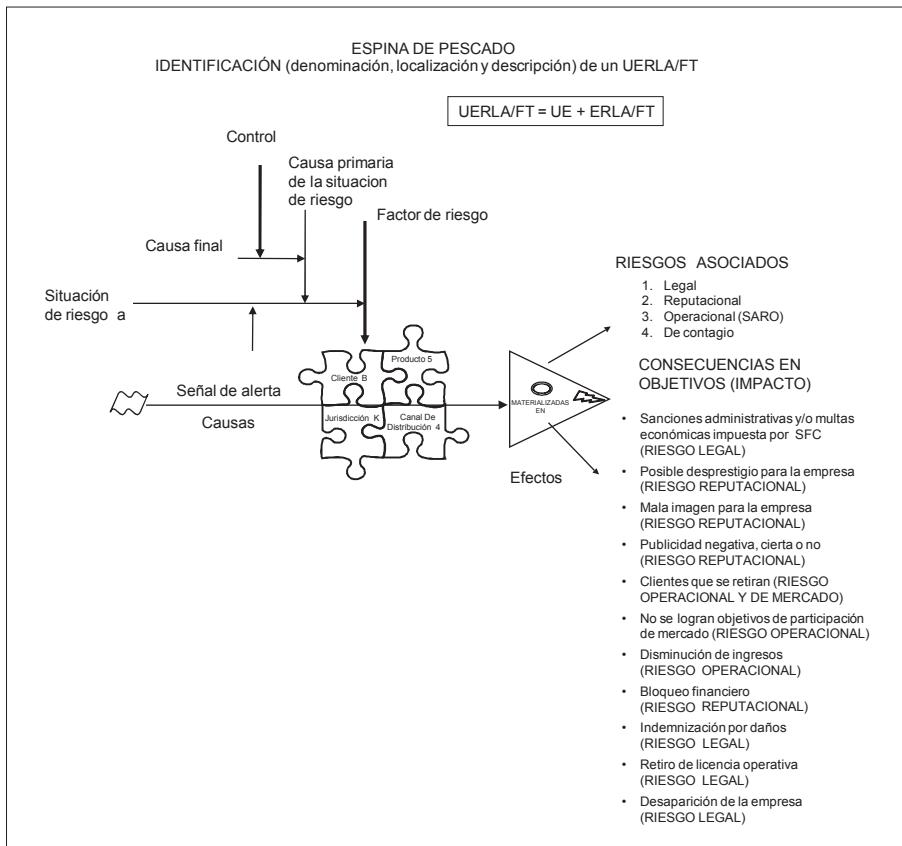
Para cada UE definida se deben identificar los eventos de riesgo de LA/FT inherentes al desarrollo de su actividad, para lo cual se deben diseñar y aplicar metodologías que ayuden a identificar las diferentes UE de la empresa (para ello se recomienda utilizar la metodología de segmentación de los factores de riesgo, utilizando los criterios aplicados anteriormente) y el evento de riesgo de LA/FT y sus riesgos asociados presentes en cada una de las UE.

Como resultado de esta etapa, la empresa debe estar en capacidad de identificar los factores de riesgo y los riesgos asociados a los cuales se ven expuestos en relación al riesgo de LA/FT.

Hay que aclarar que los eventos de riesgo de LA/FT impactan a cada una de las unidades estratégicas de la empresa. Estos eventos contienen se-

ñales de alerta presentes en situaciones de riesgo cuando los clientes realizan operaciones y, están conformados por los siguientes elementos: a) Situación de riesgo; b) Señales de alerta; c) Causas primarias; d) Causa final, y (e) impactos o consecuencias por riesgos asociados.

Gráfico 20
Componentes de un evento de riesgo de LA/FT
y la metodología de la espina de pescado



Un evento de riesgo de LA/FT por lo general está presente en una unidad estratégica (UE) de la empresa, mas no necesariamente todas las UE podrían estar contaminadas por eventos de riesgo de LA/FT. De esta forma debemos decir que al momento del diagnóstico podemos encontrar UE en riesgo y otras que no lo están.

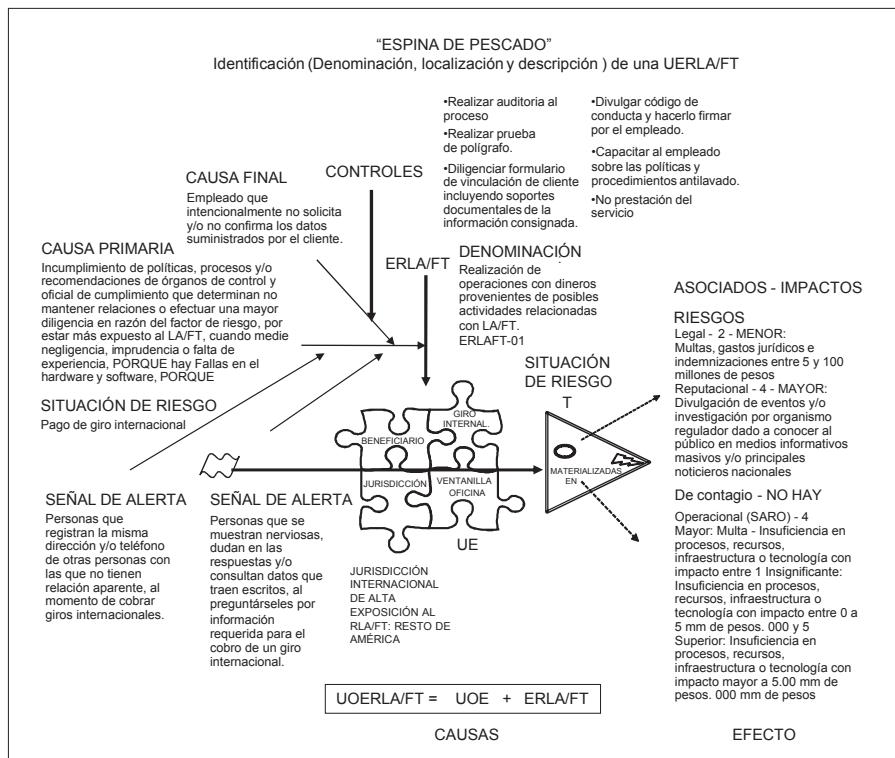
—Unidad estratégica en riesgo de LA/FT (UERLA/FT)

Una unidad estratégica en riesgo de LA/FT (UERLA/FT) está conformada por un evento de riesgo de LA/FT que impacta una UE (UERLA/FT=UE + ERLA/FT).

El evento de riesgo de LA/FT en una UE se puede identificar, es decir, denominar, localizar y describir mediante la solución de la relación causa-efecto presente en él para lo cual proponemos utilizar el “método de la espina de pescado”, como se ilustra con la siguiente aplicación práctica:

Gráfico 21

Una aplicación práctica de la metodología de la espina de pescado



—Perfil de una UE

Se elabora mediante una descripción que contenga el tipo de cliente, los productos, el canal de distribución y la jurisdicción, el valor máximo,

el valor mínimo, la frecuencia y el valor promedio de las operaciones realizadas para cada producto/servicio demandado por un tipo promedio de cliente de un segmento de mercado.

— *Perfil de un evento de riesgo de LA/FT*

Se hace elaborando una tabla en la que se registran: los datos nominales de *identificación* de cada evento de riesgo de LA/FT (denominación, código, macroproceso y proceso, fecha de identificación inicial, autoridad y responsabilidad), la *evaluación* (calificación y clasificación del impacto, la probabilidad y la severidad), la *descripción* que incluye: quién reportó, la fecha de reporte, los *factores de riesgo* involucrados (*cliente, productos, canales de distribución, jurisdicciones*), la *contingencia*, la *causa final* y los *riesgos asociados* para cada evento de riesgo de LA/FT.

Una forma práctica de manejar la información relacionada con eventos de riesgo de LA/FT en una UE es la utilización de formatos donde se consigan perfiles, razón por la cual, a manera de ejemplo, presentamos algunos.

Tabla 11
Formato de perfil de una UERLA/FT (según factores de riesgo)

Evento de riesgo de LA/FT
Este evento de riesgo de LA/FT ha sido asociado con los siguientes <i>segmentos de factores de riesgo de LA/FT</i>
El <i>cliente</i> que actuó como factor de riesgo de este evento de riesgo de LA/FT es:
El evento de riesgo de LA/FT se presentó en la <i>jurisdicción</i> :
El <i>canal de distribución</i> utilizado por el cliente para realizar la operación fue:
El <i>producto</i> de la empresa utilizado por el cliente fue:
Identificación del evento de riesgo de LA/FT (denominación / localización / descripción)
La información utilizada para este evento de riesgo de LA/FT corresponde al período DD/MM/AA
La <i>denominación o nombre</i> de este evento de riesgo de LA/FT es:
Se identifica con el <i>código</i> :
La <i>situación de riesgo</i> de este evento de riesgo de LA/FT se presentó cuando el cliente realizó o recibió:
La <i>causa primaria</i> (¿por qué !?) de este evento de riesgo de LA/FT es que:
Su <i>causa última</i> (¿por qué N?) es que:

OTROS DESCRIPTORES DEL EVENTO DE RIESGO DE LA/FT	
El <i>factor de riesgo</i> que hemos considerado como <i>determinante</i> para este evento de riesgo de LA/FT es:	
Su <i>fecha de identificación</i> inicial es el:	
Este evento de riesgo de LA/FT está bajo la <i>autoridad</i> del:	
Y la <i>responsabilidad</i> del:	
Y la <i>colaboración</i> de:	
El evento de riesgo de LA/FT fue <i>reportado</i> por:	
Su <i>fecha de reporte</i> fue el:	
Evento de riesgo de LA/FT Inherente	Evento de riesgo de LA/FT Residual
La cantidad de <i>eventos ocurridos</i> para este evento de riesgo de LA/FT, desde DD/MM/AA hasta DD/MM/AA, es:	La cantidad de <i>eventos ocurridos</i> para este evento de riesgo de LA/FT, desde DD/MM/AA hasta DD/MM/AA, es:
Probabilidad	Probabilidad
La cantidad de <i>eventos posibles</i> desde DD/MM/AA hasta DD/MM/AA es XXXX (cantidad de operaciones realizadas con el producto), por tanto su <i>probabilidad</i> de ocurrencia es de (%).	La cantidad de <i>eventos posibles</i> desde DD/MM/AA hasta DD/MM/AA, después de las medidas de control y tratamiento (<i>riesgo residual</i>), es (cantidad de operaciones realizadas con el producto), por tanto su <i>probabilidad</i> de ocurrencia es de (%).
Por lo cual la <i>probabilidad inherente</i> recibe un <i>valor descriptivo</i> como:	Por lo cual la <i>probabilidad residual</i> recibe un <i>valor descriptivo</i> como:
Que lo <i>define</i> como un:	Que lo <i>define</i> como un:
Impacto inherente por riesgos asociados	Impacto residual por riesgos asociados
El <i>impacto del riesgo legal inherente asociado</i> (%) para este evento de riesgo de LA/FT se califica y se podrían materializar en pérdidas por concepto de:	El <i>impacto del riesgo legal residual asociado</i> (xx%) para este evento de riesgo de LA/FT se califica y se podrían materializar en pérdidas por concepto de:
El <i>impacto del riesgo reputacional inherente asociado</i> (%) para este evento de riesgo de LA/FT se califica y se podrían materializar en:	El <i>impacto del riesgo reputacional residual asociado</i> (%) para este evento de riesgo de LA/FT se califica y se podrían materializar en:
El <i>impacto del riesgo de contagio inherente asociado</i> (%) para este evento de riesgo de LA/FT se califica y se podría materializar en:	El <i>impacto del riesgo de contagio residual asociado</i> (%) para este evento de riesgo de LA/FT se califica y se podría materializar en:
El <i>impacto del riesgo operacional inherente asociado</i> (%) para este evento de riesgo de LA/FT se califica y se podría materializar en:	El <i>impacto del riesgo operacional residual asociado</i> (%) para este evento de riesgo de LA/FT se califica y se podría materializar en:
El impacto total de los riesgos inherentes asociados es de:	El impacto total de los riesgos residuales asociados es de:
XX puntos	XX puntos

Probabilidad	Probabilidad
Para <i>minimizar o disminuir la severidad</i> que implica este evento de riesgo de LA/FT, se debe:	
La cantidad de <i>eventos ocurridos estimados</i> para este evento de riesgo de LA/FT, desde DD/MM/AA hasta DD/MM/AA, después de las medidas de control y tratamiento (<i>riesgo residual</i>), es:	
Severidad inherente del evento de riesgo de LA/FT	Severidad residual del evento de riesgo de LA/FT
La <i>severidad</i> de este ERAL/FT es calificada con:	La <i>severidad residual</i> de este ERAL/FT es calificada con:
por lo tanto, es <i>considerado</i> como un:	por lo tanto, es <i>considerado</i> como un:

—*Perfil de una Unidad Estratégica (según factores de riesgo)*

Tabla 12
Perfil de una Unidad Estratégica (según factores de riesgo)

Cliente	Jurisdicción y nivel de exposición al RLA/FT	Canal de distribución	Producto	Situación de riesgo
El cliente que actuó como factor de riesgo de este evento de riesgo de LA/FT es un:	El evento de riesgo de LA/FT se presentó en una jurisdicción (por ejemplo):	El canal de distribución utilizado por el cliente para realizar la operación fue (por ejemplo) una:	El producto de la empresa utilizado por el cliente fue un(a):	La situación de riesgo de este evento de riesgo de LA/FT se presentó cuando el cliente realizó (recibió), por ejemplo, un(a):
Rol 1	Nacional de alta exposición al RLA/FT:	Ventanilla oficina	Producto 1	Compra
Rol 2	Nacional de media exposición al RLA/FT:	Transferencia electrónica	Producto 2	Venta
Rol 3	Nacional de baja exposición al RLA/FT:		Producto 3	Apertura
	Internacional de alta exposición al RLA/FT:			Pago
	Jurisdicción internacional de alta exposición al RLA/FT:			Apertura
	Internacional de alta exposición al RLA/FT:			Administración de novedades
	Internacional alta de exposición al RLA/FT:			Cancelación
	Internacional de alta exposición al RLA/FT:			

Cliente	Jurisdicción y nivel de exposición al RLA/FT			Canal de distribución		Producto			Situación de riesgo	
	Riesgo inherente					Riesgo residual				
	Eventos Ocurridos	Eventos Posibles	% Probabilidad	Calificación	Cualificación	Eventos Ocurridos	Eventos Posibles	% Probabilidad	Calificación	Cualificación
Frecuencia										
Impacto										
Severidad										

6. METODOLOGÍA PARA LA IDENTIFICACIÓN DE EVENTOS DE RIESGO DE LA/FT

El riesgo de LA/FT, tal como lo expresa la SFC y a nuestro entender, es un concepto genérico. Difícilmente se puede identificar algo para lo cual no se han proporcionado datos específicos que permitan reconocerlo. La pregunta que surge es: ¿qué es lo que se debe identificar, medir, monitorear y controlar? De nuestra parte, respondemos que lo que se identifica, mide, controla y monitorea son eventos de riesgo de LA/FT.

El mayor problema para la implementación del SIPLA/FT o del SARLA/FT en una empresa es la identificación de operaciones sospechosas a las que también hemos denominado evento de riesgo de LA/FT.

De manera preliminar –porque más adelante analizaremos con profundidad la metodología de identificación de eventos de riesgo de LA/FT–, diremos que:

- Antes de identificar una operación sospechosa o evento de riesgo de LA/FT, debemos saber dónde buscarlo, cómo hallarlo, establecer cuáles son sus componentes y, una vez lo encontramos, cómo denominarlo;
- Un evento de riesgo de LA/FT siempre conlleva de manera implícita la relación causa-efecto, la cual se debe resolver adecuadamente;

- c) Al resolver esa relación conoceremos sus componentes, por ejemplo los factores de riesgo mencionados en la norma, las situaciones de riesgo, las señales de alerta, las causas y por tanto la causa final, y
- d) Si detectamos la causa final, podremos proponer controles.

6.1. Factores de riesgo en empresas del sector real

En la empresa, por las razones que exponemos a continuación y por su naturaleza, consideramos que los factores de riesgo de lavado de activos y financiación del terrorismo que se deben tener en cuenta son los siguientes.

Riesgo sobre el factor humano. Este riesgo inicialmente se identifica con el factor humano. Implica conocer a los empleados y saber cómo están y dónde viven. El mayor riesgo se presenta cuando se trabaja con empleados temporales, así como con transportadores o distribuidores externos. Hay que identificar las “banderas rojas”: nivel de vida elevado con respecto a los ingresos del empleado, el pago en efectivo de grandes sumas de dinero por parte de los clientes, etc.

Riesgo sobre el producto. Si los productos de la empresa pueden ser insumo para la elaboración de sustancias ilícitas, para ser usados para operaciones de contrabando o si tienen productos de difícil cuantificación.

Riesgo sobre los clientes. Si sus productos son utilizados por los clientes nacionales y del exterior. Es importante saber a qué se dedican y si el producto o servicio que ofrece la empresa pueden ser útiles a los delincuentes.

Riesgo sobre los proveedores de recursos físicos, materias primas, activos fijos, suministro. Es importante tener en cuenta que no necesariamente los precios bajos corresponden a las mejores mercancías o a insumos ilícitos. Una de las formas que usan los “lavadores” es ofrecer insumos con precios muy bajos con respecto al mercado. Por eso, si el proveedor es nuevo, es necesario conocer la trayectoria, los socios de la empresa y los suministros ofrecidos a precios por debajo del mercado.

Riesgo sobre canales de distribución. Conocer quiénes ofertan los productos y cómo los adquirieron.

Riesgo sobre los medios de pago. Se refiere al medio de pago que utiliza la empresa para recibir o hacer pagos de cualquier tipo. Generalmente hay sospecha cuando son grandes cantidades de dinero en efectivo.

Riesgo por operaciones de comercio exterior. Suplantación de la empresa para importar o exportar y lavar el dinero. Logística de la importación y exportación, teniendo claro quién recibe la mercancía, en dónde es almacenada y quiénes son los operadores de efectivo de divisas.

6.2. Señales de alerta

Las *señales de alerta*, como su nombre lo indica, se refieren a los *comportamientos particulares de los clientes y a las situaciones atípicas que presentan las operaciones* y que pueden encubrir operaciones de lavado de activos.

Hay que tener en cuenta que no todas las operaciones que presentan comportamientos atípicos e inusuales son operaciones ilegales, por tal razón, el hecho de identificar señales de alerta no significa que la operación deba ser reportada como sospechosa de manera inmediata y automática a las autoridades.

La señal de alerta facilita el reconocimiento de una operación de lavado que corresponde a los procesos característicos de los diferentes métodos adoptados por la delincuencia para el lavado de activos. Ellas son las que permiten identificar operaciones que presentan situaciones inusuales y que en algunos casos son operaciones de lavado de activos, y se identifican gracias al conocimiento que se tiene de los métodos de lavado.

A su vez, el *método de lavado* es la operación completa desarrollada por el delincuente, desde que empieza su actividad ilegal, hasta que concluye dicha operación, con el propósito de dar apariencia de legalidad a los bienes o fondos obtenidos ilícitamente.

Para la empresa del sector real, las “señales de alerta” o “banderas rojas”, también denominadas como “alertas tempranas”, no son lo mismo que “operaciones inusuales u operaciones sospechosas”; esta equivocación genera confusiones.

Las “señales de alerta” o “banderas rojas” ayudan a identificar o detectar comportamientos, conductas, actividades, métodos o situaciones atípicas que pueden encubrir operaciones de lavado. Pero la presencia de ellas no significa estar frente a una operación sospechosa que debe ser objeto de reporte inmediato. Simplemente deben llamar nuestra atención para proceder al análisis detallado de la situación.

Para efectos del SIPLA/FT y del SARLA/FT, tal como lo expresa la SFC, *las señales de alerta* son los hechos, situaciones, eventos, cuantías, indicadores cuantitativos y cualitativos, razones financieras y demás información que la empresa del sector real ha determinado como relevante, a partir de los cuales se pueden inferir oportuna y/o prospectivamente la posible existencia de un hecho o situación que escapa a lo determinado como normal.

Estas alertas sirven como instrumento de prevención y control del riesgo de LA/FT y deben tenerse en cuenta por parte de todos los empleados, según su cargo, función y ubicación, al momento de realizar cualquiera de las operaciones autorizadas por la empresa, sea con clientes o con agentes económicos.

Otro de los componentes de un evento de riesgo de LA/FT son estas señales las cuales se determinan por el conjunto de circunstancias de tiempo, modo y lugar que se presentan en una actividad (situación de riesgo) realizada para ejecutar un proceso misional, operacional o de apoyo que hacen presumir un evento de riesgo de LA/FT en un determinado momento.

Es decir, pueden ser generadas por actuaciones del cliente o de la empresa. Además, se presentan en un determinado momento de la prestación del servicio al ejecutarse algún proceso misional u operativo, generalmente cuando se dan interacciones entre clientes y empleados de la empresa. Y se evidencia mediante manifestaciones a las cuales nos referiremos posteriormente.

6.3. Grupos de señales de alerta

Las señales de alerta se pueden clasificar en los siguientes grupos a saber: 1. Las que se pueden percibir en la operación comercial o financiera de una empresa del *sector financiero*. 2. Las que se pueden percibir en la operación comercial o financiera de una empresa del *sector real*. 3. Las que se perciben según el momento de ejecución de un proceso. 4. Las que se perciben por fuera de la operación. 5. Según la forma como se producen. Discriminaremos más precisamente las señales de alerta de cada uno de estos cinco grupos.

Las siguientes señales de alerta están contempladas en el documento de la *United Nations Office of Drugs and Crime* (UNODC).

GRUPO 1. Señales de alerta que se pueden percibir en la operación comercial o financiera de una empresa del sector financiero por tipo de producto del portafolio financiero.

Los tipos de productos son: cuenta corriente, cuenta de ahorros, certificado de depósito a término, giros internacionales, seguros, encargo fiduciario o fiducia mercantil, transacciones de usuarios, empleados de la institución financiera.

— *Cuenta corriente*

Señales de alerta para la apertura y manejo de la cuenta corriente;

Señales de alerta para el registro de firmas autorizadas de la cuenta corriente;

Señales de alerta para el estado mensual de la cuenta corriente;

Señales de alerta para las consignaciones de la cuenta corriente;

Señales de alerta para los cheques de la cuenta corriente, y

Señales de alerta para las transferencias desde o hacia una cuenta corriente.

— *Cuentas de ahorro*

Señales de alerta para la apertura y el manejo de la cuenta de ahorros;
Señales de alerta para el registro de firmas autorizadas de la cuenta de ahorros;
Señales de alerta para el extracto periódico de la cuenta de ahorros;
Señales de alerta para las consignaciones de la cuenta de ahorros;
Señales de alerta para los comprobantes de retiro de la cuenta de ahorros, y
Señales de alerta para las transferencias locales o internacionales desde o hacia una cuenta de ahorros.

— *Certificados de depósito (CD)*

Señales de alerta para la vinculación y apertura de un CD;
Señales de alerta para los comprobantes de compra o constitución de un CD;
Señales de alerta para la emisión de los títulos de CD, y
Señales de alerta para los comprobantes de cancelación de un CD.

— *Giros internacionales*

Señales de alerta para la vinculación y/o apertura de una “cuenta de giros” o comprobantes de envío de giros internacionales, y
Señales de alerta para los comprobantes de cobro de un giro internacional.

— *Seguros*

Señales de alerta para el formato de vinculación a una *compañía aseguradora*;

Señales de alerta para los comprobantes de pago de la prima del seguro;

Señales de alerta para la emisión o renovación de los certificados de las pólizas de seguro, y

Señales de alerta para los comprobantes de cancelación anticipada de la póliza de seguro.

—*Fiducia mercantil*

Señales de alerta para el formato de vinculación o apertura de un encargo fiduciario o fiducia mercantil;

Señales de alerta para los comprobantes de recepción del dinero o bienes del fideicomitente;

Señales de alerta de los comprobantes de pago a favor o por cuenta del fideicomitente;

Señales de alerta para el formato de vinculación o apertura de un mandato de inversión;

Señales de alerta para los comprobantes de recepción del dinero o títulos;

Señales de alerta de los comprobantes de pago a favor o por cuenta del inversionista;

Señales de alerta en las transferencias de fondos derivadas de negocios de comercio exterior;

Señales de alerta en transacciones de usuarios, y

Señales de alerta para empleados de una institución financiera.

GRUPO 2. *Señales de alerta que se pueden percibir en la operación comercial o financiera de una empresa financiera o de una empresa del sector real.*

Tanto las señales de alerta para empresas del sector financiero como para el sector real se pueden subdividir según los factores de riesgo donde se presentan, por tanto habrá:

— Señales de alerta relacionados con el cliente

Señales en personas naturales o jurídicas;

Señales en personas jurídicas;

Señales por operaciones múltiples, y

Señales por operaciones individuales.

— Señales de alerta relacionadas con el producto

Señales de alerta en el proceso de venta;

Señales de alerta relacionadas con los canales de distribución.

Señales de alerta relacionadas con las jurisdicciones.

Señales en operaciones internacionales.

GRUPO 3. *Señales de alerta que se pueden percibir según el momento de la ejecución de un proceso.*

— Señales de alerta que se pueden percibir antes de iniciar el proceso.

— Señales de alerta que se pueden percibir durante la ejecución del proceso.

— Señales de alerta que se pueden percibir después de ejecutado el proceso.

GRUPO 4. *Señales de alerta que se pueden percibir por fuera de la operación comercial o financiera.*

GRUPO 5. *Señales de alerta según la forma como se producen.*

— Señales de alerta producidas por el sistema previa programación de las mismas.

— Señales de alerta que debe identificar el funcionario mediante su percepción.

La descripción de cada una de estas señales de alerta, las encontrará el lector en el Anexo 7 de este libro.

6.4. Identificación de eventos de riesgo de LA/FT

Una de las etapas indicadas por la SFC para la administración del riesgo de LA/FT corresponde a la identificación; en el libro hemos expresado que lo que se identifica son eventos de riesgo de lavado de activos y de la financiación del terrorismo (evento de riesgo de LA/FT que impactan sobre las UE).

Esta etapa tiene como objetivo identificar los riesgos y un conjunto de eventos, de manera ordenada y sistemática, que puedan dar origen a hechos de lavado de activos y/o financiación del terrorismo. Esta identificación se realiza como un proceso continuo, que abarca todos los procesos para el desarrollo del negocio y teniendo presente los diversos factores de riesgo: cliente/usuario, producto, canal, jurisdicción, empleado, proveedor, entre otros a los cuales puede estar expuesta.

La metodología para la identificación de evento de riesgo de LA/FT consiste, al igual que para el Sistema de Administración de Riesgo Operativo (SARO), en desagregarla en los siguientes pasos:

- a) Detectar el evento de riesgo de LA/FT, teniendo como sinónimos de detectar: hallar, encontrar, descubrir;
- b) Describir cada evento de riesgo de LA/FT, entendiendo como tal la acción de enunciar y consignar por escrito todos los elementos constitutivos (pérdidas que se generan, factores de riesgo, situaciones de riesgo, riesgos y causas) del evento de riesgo de LA/FT, y
- c) Ubicar el evento de riesgo de LA/FT en el contexto de cada unidad estratégica.

Todos los riesgos identificados pueden ser fuentes de eventuales daños que puede sufrir la organización por la propensión a ser utilizada directa-

mente o a través de sus operaciones, materializados a través de los riesgos asociados: reputacional, operacional, legal y/o de contagio.

El proceso de identificación de evento de riesgo de LA/FT debe realizarse permanentemente y estar integrado a la planeación de la gestión de riesgos (ciclo PHVA).

Para una misma UE pueden identificarse varios eventos de riesgo de LA/FT y cada uno de ellos puede originarse por varias causas o factores de riesgo.

El gerente de riesgos y el oficial de cumplimiento, con la colaboración de los responsables de los procesos vinculados a las UE que puedan ser afectados por el riesgo, deben identificar el conjunto inicial de evento de riesgo de LA/FT que se pueden presentar y diligenciar los formatos correspondientes.

6.4.1. *Detección del conjunto inicial de eventos de riesgo de LA/FT*

Para esto, proponemos utilizar una de las dos siguientes metodologías.

—*Metodología I*

Inicialmente, siguiendo los lineamientos para la identificación de evento de riesgo de LA/FT y concentrándonos en un análisis exhaustivo de los cuatro factores de riesgo, se debería recurrir al documento de Naciones Unidas, el cual se anexa a esta obra en el apéndice⁽¹⁾.

De esta manera, se podrían obtener el listado de eventos de riesgo de LA/FT que fueron codificados como se indica en la tabla siguiente:

(1) Naciones Unidas, Embajada Británica (Bogotá), Oficina contra la Droga y el Delito, Programa de Asistencia Legal para América Latina y el Caribe, Riesgo de Lavado de Activos en Instrumentos Financieros, Usuarios y Empleados de Instituciones Financieras, 1^a Versión, Copyright UNODC. Calle 102 # 17A-61 (nivel 4), Telf.: (+571) 6467000 Ext. 337, e-mail: laplac@unodec.org. Disponible en web: <www.unodc.org>.

Tabla 13
Posibles nombres de eventos de riesgo de LA/FT

Possible nombre del evento de riesgo de LA/FT	Possible código del evento de riesgo de LA/FT	Possible factor determinante del riesgo
Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	Clientes
Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	Clientes
Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	Clientes
Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	Clientes
Realización de operaciones con clientes que solicitan transferencias de propiedad a otras personas diferentes del titular o entrega de dinero a un tercero.	Evento de riesgo de LA/FT-05	Clientes
Realización de operaciones con clientes/usuarios incluidos en listas restrictivas.	Evento de riesgo de LA/FT-06	Clientes
Realización de operaciones con clientes/usuarios incluidos en operaciones sospechosas reportadas a la UIAF.	Evento de riesgo de LA/FT-07	Clientes
Realización de operaciones con clientes/usuarios que en corto tiempo se vinculan a la empresa para múltiples productos.	Evento de riesgo de LA/FT-08	Clientes
Realización de operaciones con clientes/usuarios que frecuentemente aparecen incluidos en operaciones inusuales, señales de alerta y/o múltiples con cualquiera de los productos de la empresa.	Evento de riesgo de LA/FT-09	Clientes
Realización de operaciones con clientes/usuarios que no se identifican plenamente.	Evento de riesgo de LA/FT-10	Clientes
Realización de operaciones con clientes/usuarios que suplantan al verdadero cliente o usuario.	Evento de riesgo de LA/FT-11	Clientes
Realización de operaciones con productos que utilizan fondos de dinero provenientes de países bloqueados o catalogados como más expuestos al LA/FT.	Evento de riesgo de LA/FT-12	Producto
Realización de operaciones en jurisdicciones catalogadas como de alto nivel de exposición al riesgo de LA/FT.	Evento de riesgo de LA/FT-13	Jurisdicción
Realización de operaciones en las que se solicita frecuente cambio de titular, apoderado o beneficiario de un producto.	Evento de riesgo de LA/FT-14	Clientes
Realización de operaciones en oficinas que presentan un alto volumen de operaciones sospechosas.	Evento de riesgo de LA/FT-15	Canal

Possible nombre del evento de riesgo de LA/FT	Possible código del evento de riesgo de LA/FT	Possible factor determinante del riesgo
Realización de operaciones por empleados o funcionarios que adoptan comportamientos sospechosos: evaden controles, frecuentemente incurren en errores, impiden que otro compañero atienda a determinado cliente, se ausentan frecuentemente de su trabajo, terminan su jornada después de lo normal, tienen un estilo de vida que no se ajusta a su nivel de ingresos, etc.	Evento de riesgo de LA/FT-17	Empleados y funcionarios
Participación de socios y directivos en aprobación de operaciones posiblemente relacionadas con actividades de LA/FT.	Evento de riesgo de LA/FT-18	Empleados y funcionarios
Realización de operaciones personales o con la empresa por parte de socios, funcionarios y directivos, posiblemente relacionada con actividades de LA/FT.	Evento de riesgo de LA/FT-19	Empleados y funcionarios

Para cada uno de ellos se identificó el factor de riesgo que consideramos como el determinante del riesgo. Obsérvese que cada uno de estos eventos de riesgo de LA/FT se puede asociar con uno o con todos los factores de riesgo, por lo cual fue necesario enunciarlos de la manera más general posible. Es decir, cualquiera de estos eventos de riesgo de LA/FT se puede presentar en cualquiera de las UE de la empresa.

—*Metodología 2. Detección de evento de riesgo de LA/FT mediante la aplicación del diagrama causa-efecto (espina de pescado)*

La solución que se encuentre, utilizando la técnica del diagrama de “espina de pescado”, permitirá identificar, describir y ubicar en la empresa eventos de riesgo de LA/FT; y, generar una definición aplicada del concepto “evento de riesgo de LA/FT” que hemos venido denotando por la si- gla ERLA/FT.

En nuestro concepto, todo ERLA/FT, debe buscarse en una unidad estratégica (UE) y tiende a generar una *pérdida* (o consecuencia o impacto) en la empresa, que se materializa mediante: *riesgos asociados* debido a que en uno o varios *factores de riesgo* se podrían presentar en *situaciones de riesgo* cuando se ejecutan las actividades misionales, operacionales y de apoyo requeridas para generar el portafolio de los servicios o productos de la empresa, las cuales tienen *causas* que se evidencian mediante *señales de alerta*.

Solución específica de la relación causa-efecto en SARLA/FT

Preliminarmente, porque luego profundizaremos en el concepto, tal como ya lo dijimos un ERLA/FT es un sistema conformado por los siguientes factores y elementos.

Factores de un ERLA/FT

Una unidad estratégica está Integrada por los siguientes factores de riesgo de LA/FT, tales como:

- a) Uno o varios *stakeholders* - interesados en la empresa;
- b) Uno o varios clientes;
- c) Uno o varios productos;
- d) Una o varias jurisdicciones, y
- e) Uno o varios canales de distribución.

Elementos de un ERLA/FT

Son los que ayudan a resolver la relación causa-efecto y están presentes en cada factor de riesgo. Son los siguientes:

- a) Una situación de riesgo;
- b) Una o varias señales de alerta;
- c) Una o varias causas primarias;
- d) Una o varias causas principales, y
- e) Uno o varios riesgos asociados.

Los elementos y los factores de riesgo interactuando entre sí y simultáneamente, con propósitos de lavado de activos, son los que pueden generar una pérdida o daño a la empresa.

6.4.2. *Detección de componentes de eventos de riesgo de LA/FT*

Una vez definida la pérdida más relevante que se podría presentar por la ejecución de la actividad del proceso, se deben establecer: a) Todos los *factores de riesgo* que intervienen en caso de materializarse el evento de riesgo de LA/FT y asignar a cada factor una “espina primaria” en el diagrama causa-efecto; b) Para cada uno de los factores de riesgo las probables *situaciones de riesgo* que podrían estar asociadas con cada *tipo de pérdida* y asignarles una “espina secundaria”; c) Para cada *situación de riesgo*, las *señales de alerta* que podrían ocasionar cada una de las pérdidas y asignar a cada riesgo una “espina terciaria”; d) Para cada *riesgo*, todas las *causas posibles* que podrían desencadenar la pérdida y a cada causa asignarle una “espina cuaternaria”, y e) Para cada causa, seleccionar la *causa raíz o causa principal*; para lograrlo, se debe utilizar la metodología de los “cinco por qué”.

Los eventos de riesgo de LA/FT se presentan en las diferentes UE con que opera la empresa en los mercados.

6.4.3. *Descripción de eventos de riesgo de LA/FT mediante la aplicación del diagrama causa-efecto (“espina de pescado”)*

Debe tenerse en cuenta que para una UE pueden darse:

- a) Uno o varios factores de riesgo;
- b) Una o varias *situaciones de riesgo* para cada factor de riesgo;
- c) Uno o varios señales de alerta en una situación de riesgo;
- d) Una o varias causas probables del riesgo para cada riesgo, y
- e) Solo una causa principal o raíz para cada causa probable.

De conformidad con lo anterior, en una UE se pueden identificar tantos eventos de riesgo de LA/FT como combinaciones lógicas de factores

de riesgo con *situaciones* de riesgo, con señales de alerta y con causas raíces que se puedan realizar. Para la descripción de un evento de riesgo de LA/FT, se debe tomar un solo factor de riesgo con una sola situación de riesgo, una sola señal de alerta y una sola causa raíz.

Para la aplicación de esta metodología, se recomienda elaborar un diagrama de “espina de pescado” diferente para cada UE.

La descripción del evento de riesgo de LA/FT se debe realizar mediante el diligenciamiento de todos los campos del formato para la identificación y descripción de evento de riesgo de LA/FT, con la participación de todo el personal involucrado en la UE evaluada, registrando todos aquellos eventos de riesgo que puedan tener un impacto significativo para el desarrollo del negocio, que hayan ocurrido o que podrían presentarse.

Para la descripción de cada evento de riesgo de LA/FT, cada uno se debe codificar, denominar, ubicar, describir, datar, especificar las unidades de medida de la frecuencia y el tipo de impacto. Por lo anterior, hay que tener en cuenta que:

La codificación consiste en asignar códigos que permitan diferenciar fácilmente cada evento de riesgo y su enunciado.

La denominación es asignar un nombre breve que se utilizará para posteriores referencias entre quienes lo gestionan.

La ubicación se refiere a la localización de cada evento de riesgo dentro de un proceso y su correspondiente macroproceso, así como a la identificación del cargo y área que le corresponde.

La descripción se debe hacer mediante un enunciado escrito, extenso y comprensivo, de sus causas, factores, situaciones de riesgo, riesgos asociados y efectos.

La causa: un evento de riesgo de LA/FT se genera por la comisión presunta o comprobada del delito de lavado de activos y financiación del terrorismo.

6.4.4. *Materialización de eventos de riesgo de LA/FT (riesgos asociados al LA/FT)*

Un evento de riesgo de LA/FT puede tener los siguientes riesgos asociados, a través de los cuales se materializa el riesgo de LA/FT; estos son: reputacional, legal, operativo y contagio. Además, pueden tener una o varias de las siguientes causas (presentes en los procesos o inherentes en quienes los ejecutan):

- a) Omisiones;
- b) Carencias;
- c) Inadecuaciones;
- d) Faltas;
- e) Debilidades;
- f) Fallas;
- g) Intención dolosa o culposa;
- h) Diferencias;
- i) Deficiencias.

6.4.5. *Descripción de eventos de riesgo de LA/FT que se podrían utilizar en la empresa*

Detalladamente, un evento de riesgo de LA/FT puede ser generado por uno o varios de los siguientes factores:

- a) Clientes;
- b) Usuarios;
- c) Productos;

- d) Servicios;
- e) Canales de distribución;
- f) Sitios donde se realiza la operación;
- g) Obligaciones contractuales;
- h) Accionistas;
- i) Funcionarios y empleados, y
- j) Proveedores de insumos.

Un evento de riesgo de LA/FT puede generarse, por ejemplo, en una o varias de las siguientes situaciones de riesgo:

Gestión operativa interna con productos de captación y colocación en el sector financiero o productos y servicios en empresas del sector real.

Gestión operativa interna para administración de novedades en operaciones.

Gestión operativa interna en los procesos de comunicación de una operación.

Gestión operativa interna de oficinas.

Gestión pago de operaciones en ventanilla.

Gestión pago de realización de operaciones mediante pago por consignación.

Gestión captación CDT: vinculación y/o apertura.

Gestión captación CDT: verificación de documentación, origen de fondos, capacidad económica y registro oficial del emisor del CDT.

Gestión captación CDT: constitución (emisión, expedición) del CDT.

Gestión captación CDT: renovación, endosos, múltiples endosos, fraccionamiento, adiciones, cambios, garantías, vencimiento.

Gestión captación CDT: registro oficial del emisor del CD.

Gestión captación CDT: monitoreo comercial clientes.

Gestión captación CDT: cancelación.

Gestión colocación crédito vehículos: negociación y renegociación crédito vehículos.

Gestión colocación crédito vehículos: solicitud.

Gestión colocación crédito vehículos: verificación de documentación, origen de fondos, capacidad económica (análisis).

Gestión colocación crédito vehículos: aprobación.

Gestión colocación crédito vehículos: contrato y garantías crédito vehículos.

Gestión colocación crédito vehículos: registro.

Gestión colocación crédito vehículos: desembolso crédito vehículos.

Gestión colocación crédito vehículos: seguimiento crédito vehículos.

Gestión colocación crédito vehículos: recuperación cartera crédito vehículos.

Gestión colocación crédito vehículos: cancelación.

Gestión negociación de divisas: compra de divisas.

Gestión negociación de divisas: venta de divisas.

Gestión de manejo de excedentes: inversiones portafolio.

Gestión de manejo de excedentes: compra de divisas (monetización).

Tabla 14
Sintaxis de la definición de eventos de riesgo de LA/FT

		Lavado de activos y financiación del terrorismo	Reputacional	Legal	Operativo	Contagio	
CONSECUENCIAS	Es el (la, los)	Desprestigio	Desprestigio	Indemnización por daños	Desprestigio	Desprestigio	
		Mala imagen	Mala imagen	Sanción	Mala imagen	Mala imagen	
		Publicidad negativa, cierta o no	Publicidad negativa, cierta o no		Publicidad negativa, cierta o no	Publicidad negativa, cierta o no	
		Pérdida de clientes	Pérdida de clientes		Pérdida de clientes	Pérdida de clientes	
		Disminución de ingresos	Disminución de ingresos		Disminución de ingresos	Disminución de ingresos	
		Procesos judiciales	Procesos judiciales		Procesos judiciales	Procesos judiciales	
		Bloqueo financiero	Bloqueo financiero			Bloqueo financiero	
CAUSA 1	Que se puede generar por	La propensión a ser utilizada directamente como instrumento del LA/FT y/o canalización de recursos hacia la realización de actividades terroristas o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades		Fallas en transacciones			
				Fallas en contratos			
CAUSA 2	Debidos (as) a (la, un, una)	Compromiso activo y consciente en evento de riesgo de LA/FT		Incumplimiento de normas o regulaciones	Deficiencia	Acción	
				Incumplimiento de obligaciones contractuales	Falla	Experiencia	
				Actos malintencionados	Inadecuación		
				Negligencia			
				Actos involuntarios			

		Lavado de activos y financiación del terrorismo	Reputacional	Legal	Operativo	Contagio
CAUSA 3	Que afectan			La formalización o ejecución de contratos o transacciones		
FACTORES DE RIESGO	En (el, la, de, un)				Recurso humano Procesos Tecnología Infraestructura Acontecimientos externos	Vinculado
	Respecto de:	La institución (la entidad)	La institución (la entidad)	La entidad	La institución (la entidad)	La institución (la entidad)
		Prácticas de negocio	Prácticas de negocio		Prácticas de negocio	Prácticas de negocio

7. METODOLOGÍA PARA MEDICIÓN O EVALUACIÓN DE EVENTOS DE RIESGO DE LA/FT

Para medir o evaluar los eventos de riesgo de LA/FT, debemos:

- Medir el riesgo inherente mediante la obtención de valores de probabilidad e impacto de los eventos de riesgo de LA/FT;
- Generar los valores de severidad de los eventos de riesgo de LA/FT que conforman el riesgo inherente;
- Elaborar el mapa de eventos de riesgo inherente de LA/FT;
- Establecer controles y aplicarlos a las causas de los eventos de riesgo de LA/FT;
- Medir y analizar la efectividad de los controles;
- Establecer los eventos de riesgo de LA/FT con los controles menos efectivos, y
- Consolidar en un solo mapa los valores de severidad de los eventos de riesgo de LA/FT del riesgo inherente y luego los valores de severidad de los eventos de riesgo de LA/FT que quedan conformando el riesgo residual.

7.1. Medición del riesgo inherente

Concluida la etapa de identificación, se debe medir la posibilidad o probabilidad de ocurrencia y el impacto de cada evento de riesgo de LA/FT en cada unidad estratégica. Estas mediciones podrán ser de carácter cualitativo o cuantitativo.

Para medir el riesgo de LA/FT se deben diseñar *metodologías* para calcular la *posibilidad o probabilidad* (P), para estimar el valor del *impacto* (I) en los riesgos asociados y para determinar la *severidad* (S) del evento de riesgo de LA/FT en cada unidad estratégica.

La *probabilidad de ocurrencia* (P) de un evento de riesgo de LA/FT es el resultado de dividir la *cantidad de eventos de riesgo de LA/FT ocurridos* (CEO) entre la *cantidad de eventos de riesgo de LA/FT posibles* (CEP). La probabilidad se debe expresar en términos cuantitativos porcentuales y luego en términos descriptivos.

$$P = CEO/CEP$$

Diseñar y aplicar metodologías para hacer una medición o evaluación estimada del *impacto* (I) en cada riesgo asociado, las cuales se expondrán más adelante. El impacto también se debe expresar en valores tomados de una escala de valuación y en términos descriptivos.

La *severidad* (S) del evento de riesgo de LA/FT es el resultado de multiplicar la *probabilidad* (P) por el *impacto* (I) y se debe expresar en términos cuantitativos y descriptivos.

$$S = P \times I$$

Como resultado de esta etapa, la empresa estará en capacidad de establecer el “mapa de riesgo inherente de LA/FT”, que contiene las mediciones de la severidad de cada evento de riesgo de LA/FT en cada unidad estratégica. Más adelante nos referiremos a las escalas de medición cuantitativa y cualitativa.

7.2. Medición del riesgo residual

Una vez se ha realizado la medición de la probabilidad e impacto para cada evento de riesgo de LA/FT identificado como riesgo inherente en los

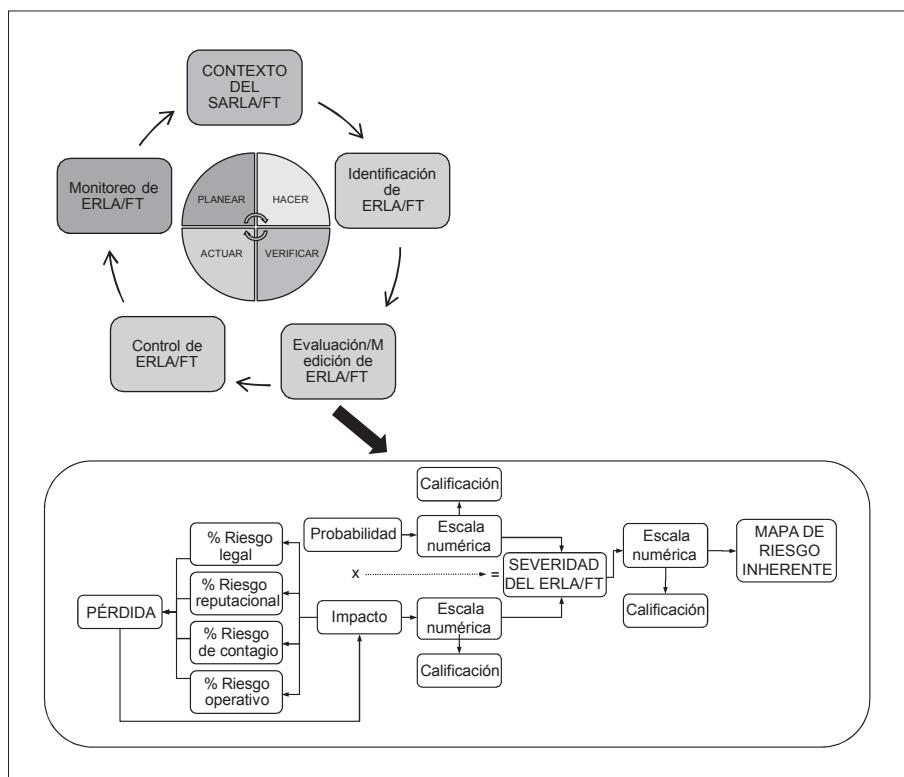
diferentes procesos y procedimientos que se realizan, es necesario evaluar y aplicar los controles que reducen las causas del evento de riesgo inherente, esperar un tiempo mientras los controles surten efecto y luego medir la efectividad de los mismos en términos de la nueva probabilidad de ocurrencia y nuevo impacto del evento de riesgo de LA/FT, con el fin de determinar el nivel de severidad del riesgo residual.

A partir de los eventos de riesgo de LA/FT identificados, controlados y evaluados, posteriormente se debe producir un mapa que contenga la severidad de los eventos de riesgo de LA/FT inherentes y de los residuales.

7.3. Medición o evaluación de un evento de riesgo de LA/FT

Gráfico 22

Metodología para medición o evaluación de un evento de riesgo de LA/FT



Todo evento de riesgo de LA/FT debe ser medido en su frecuencia e impacto y evaluado para determinar su severidad. Por eso es importante aclarar que *medición* es el proceso de cuantificación, explicación y registro detallado de la *frecuencia* con que se repite o se podría repetir el evento o la causa de riesgo expresada en términos de *probabilidad* y del *impacto* que causa en la empresa, medido en términos de una *pérdida* de: a) Imagen y reputación; b) Dinero por sanciones y multas, y e) Bloqueo financiero.

Aun cuando la empresa por autocontrol y por los controles ordenados por entes gubernamentales posea controles aplicados en los diferentes procesos, la evaluación preliminar, mediante el cálculo de probabilidad de ocurrencia e impacto del evento de riesgo de LA/FT, dará como resultado el riesgo inherente.

Los controles existentes y la aplicación de propuestas de nuevos controles o mejoras de los existentes generan el riesgo residual, que será sometido a consideración de la junta directiva para su aceptación o rechazo.

El gerente de riesgos y el oficial de cumplimiento serán los responsables de realizar la evaluación de cada evento de riesgo de LA/FT identificado.

Para facilitar la comprensión de este tema utilizaremos un ejemplo numérico en el cual se asignan escalas cualitativas y cuantitativas tanto para la probabilidad como para el impacto.

7.3.1. ***Medición de la probabilidad de ocurrencia de un evento de riesgo de LA/FT***

Para medir la *frecuencia* (probabilidad de ocurrencia) de un evento de riesgo de LA/FT se debe:

- a) Definir qué tipo de medición cuantitativa (elaborada con valores numéricos o porcentuales de datos estadísticos) y cualitativa (elaborada con escalas descriptivas) se debe utilizar;
- b) Definir tipo de fuente de información para la frecuencia;
- c) Definir horizonte de tiempo para establecer la probabilidad de ocurrencia;

- d) Determinar la cantidad de eventos ocurridos o probables;
- e) Determinar cantidad de eventos posibles;
- f) Definir frecuencia absoluta;
- g) Definir frecuencia relativa (probabilidad);
- h) Calificar la probabilidad de ocurrencia en términos de la escala de probabilidades, y
- i) Documentar medición de la frecuencia.

El horizonte de tiempo para establecer la probabilidad de ocurrencia de un evento de riesgo de LA/FT podría ser de un año y la unidad de medida será:

- Frecuente;
- Probable;
- Escaso;
- Remoto, y
- Improbable.

Para establecer la probabilidad de ocurrencia, se debería tener en cuenta si se han presentado eventos de riesgo de manera permanente, esporádica o recurrente.

La frecuencia podría ser medida y expresada, por ejemplo, en la siguiente escala de probabilidades:

Tabla 15

Ejemplo de probabilidad de ocurrencia y escala para medir un evento de riesgo de LA/FT

Frecuencia (Probabilidad)		
	Probabilidad de ocurrencia	Escala
Evento de riesgo de LA/FT Casi seguro	Mayor = $0 > al 2,0\%$	5
Evento de riesgo de LA/FT Probable	Entre 1,5% y < 2,0%	4
Evento de riesgo de LA/FT Posible	Entre 0,05% y < 1,5%	3
Evento de riesgo de LA/FT Raro	Entre 0,005% y < 0,05%	2
Evento de riesgo de LA/FT Improbable	Entre 0 % y < 0,005%	1

Obsérvese en la tabla anterior que la probabilidad total fluctúa entre, por ejemplo, 0% y 2%. Esto quiere decir que la probabilidad de un evento de riesgo de LA/FT no debería ser superior al 2%, debido a los controles que la empresa tiene establecidos; el techo de la escala podría ser superior a 2%.

Posteriormente, se debe calificar numéricamente la probabilidad de ocurrencia para cada uno de los eventos de riesgo de LA/FT identificados en una escala de 1 a 5.

7.3.2. *Escalas de medición de impacto para cada uno de los riesgos asociados*

Puesto que el impacto se podría materializar en los diferentes riesgos asociados, este debería ser medido en escalas diferentes para cada uno.

Se debe ponderar la relevancia o importancia de cada riesgo asociado. Se podría pensar que en una empresa el riesgo más relevante por su probabilidad de ocurrencia e impacto es el riesgo legal, razón por la cual se podría ponderar con el 40%, mientras que el siguiente es el riesgo reputacional, al cual se le asignaría el 30% de relevancia.

Se construye, entonces, una escala general de medición capaz de tener las escalas de valores y descripciones graduales de cada riesgo asociado; y otras escalas de medición cualitativa y cuantitativa de los diferentes niveles de impacto para cada riesgo asociado.

Para el evento de riesgo de LA/FT que se está evaluando, se selecciona un valor dentro de la escala de los diferentes niveles de impacto. Se define el tipo de fuente de información para el impacto más relevante y se verifica que el horizonte de tiempo para establecer la probabilidad de ocurrencia sea igual al horizonte de tiempo tomado para el impacto. Y se califica teniendo en cuenta sus efectos económicos, reputacionales y legales.

Los impactos para cada riesgo asociado pueden ser medidos y expresados según la siguiente escala de valores:

Tabla 16
Escala de medición de impacto por riesgos asociados

		Riesgo legal	Riesgo reputacional	Riesgo de contagio	Riesgo operacional
1	Insignificante	1 - Multas, gastos jurídicos e indemnizaciones entre 0 y 5 millones de pesos.	1 - Situaciones que no trascienden a los medios informativos.	1 - Efectos legales y reputacionales de un usuario o proveedor involucrado en alguna actividad de LA/FT.	1 - Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 0 a 5 millones de pesos.
2	Leve	2 - Multas, gastos jurídicos e indemnizaciones entre 5 y 100 millones de pesos.	2 - Aviso sorpresivo de prensa u otro medio masivo.	2 - Efectos legales y reputacionales de un cliente involucrado en alguna actividad de LA/FT.	2 - Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 5 y 100 millones de pesos.
3	Moderado	3 - Multas, gastos jurídicos e indemnizaciones entre 100 y 1000 millones de pesos.	3 - Crítica de organismos de control o clientes en medios masivos de comunicación.	3 - Efectos legales y reputacionales de un funcionario involucrado en alguna actividad de LA/FT.	3 - Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 100 millones de pesos y 1.000 millones.
4	Crítico	4 - Multas, gastos jurídicos e indemnizaciones entre 1.000 y 5.000 millones de pesos.	4 - Divulgación de eventos y/o investigación por organismo regulador dando a conocer al público en medios informativos masivos y/o principales noticieros nacionales.	4 - Efectos legales y reputacionales de un <i>directivo</i> (presidente, vicepresidente y miembros de junta directiva y oficial de cumplimiento) involucrado en alguna actividad de LA/FT.	4 - Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 1.000 y 5.000 millones de pesos.
5	Catastrófico	5 - Multas, gastos jurídicos e indemnizaciones más de 5.000 millones de pesos.	5 - Pérdida de confianza por parte del público, intervención de entidades competentes.	5 - Efectos legales y reputacionales significativos de accionistas principales (más del 10%) de la entidad o grupo económico en alguna actividad de LA/FT.	5 - Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto mayor a 5.000 millones de pesos.

—*Consolidación de las escalas de medición de impacto para cada uno de los riesgos asociados*

Mediante el anterior procedimiento, cada evento de riesgo de LA/FT recibiría una calificación por cada tipo de riesgo asociado; es decir, se ob-

tendrían 4 calificaciones. El procedimiento anterior hace necesario que se produzca una única calificación que consolide las 4, para lo cual se procede a utilizar la técnica del promedio ponderado. El valor del impacto que se produciría debería oscilar en una escala de 1 a 5, para que exista correspondencia con la escala de medición de la probabilidad.

Tabla 17
Escala de medición de impacto total por riesgos asociados

Valor cuantitativo del impacto	Valor cualitativo del impacto	Descripción
1	Insignificante	No produce ningún tipo de impacto sobre los objetivos de la organización.
2	Leve	Se producen efectos menores que pueden ser manejados con recursos propios.
3	Moderado	El evento de riesgo de LA/FT afecta algunos objetivos de la organización.
4	Crítico	Algunos objetivos importantes de la organización no se pueden lograr y el impacto no puede ser manejado sólo con recursos propios.
5	Catastrófico	El impacto compromete la supervivencia de la organización.

7.4. Severidad de un evento de riesgo de LA/FT

Una vez se han realizado las mediciones para cada evento de riesgo de LA/FT, se debe establecer el nivel de severidad o castigo que representa cada uno de ellos para la empresa.

El indicador de la severidad del evento de riesgo de LA/FT que determina su nivel de prioridad para el tratamiento de cada evento de riesgo de LA/FT se obtiene multiplicando la calificación del nivel de probabilidad por la calificación dada al nivel de impacto respectivo. De esta forma y para este caso, se obtienen múltiplos que van desde 1 hasta 25, donde 1 es el más bajo nivel de severidad o castigo y por tanto de prioridad, mientras que 25 es el máximo valor, como se indica en la tabla del anexo 1, que permite visualizar los grados de severidad de los eventos de riesgo de LA/FT (obsérvese que los múltiplos se obtienen mediante la permutación de cada una de las ordenaciones posibles de los elementos de los conjuntos finitos

de calificación de la probabilidad y calificación del impacto). Las diferentes permutaciones de las calificaciones de probabilidad e impacto, el múltiplo entre 1 y 25 como calificador de la severidad y una descripción de su nivel para un determinado evento de riesgo de LA/FT se indican igualmente en la tabla mencionada.

Los datos de la tabla también se pueden disponer gráficamente en un plano de coordenadas cartesianas, donde al eje “Y” se le asignan las diferentes calificaciones numéricas y descriptivas de la frecuencia, mientras que al eje “X” le corresponden las calificaciones de impacto.

Esta disposición gráfica ayuda a la elaboración del mapa de eventos de riesgo de LA/FT. También permite ubicar en ella los datos de frecuencia e impacto para cada evento de riesgo de LA/FT y, además, establecer visualmente el nivel de severidad o castigo que impone cada evento de riesgo de LA/FT. Igualmente facilita la construcción del mapa de eventos de riesgo inherente de LA/FT, o sea de los eventos de riesgo de LA/FT sin medidas de control; y del mapa de eventos de riesgo residual de LA/FT, o sea del valor de la frecuencia y el impacto después de establecidos los controles. De la misma forma, posibilita una buena visualización de los resultados de la gestión del riesgo.

En el gráfico mencionado, la calificación del nivel de severidad del evento de riesgo de LA/FT está indicada mediante variaciones del color gris, tal como se indica en la siguiente tabla de convenciones:

Tabla 18
Escala de severidad

Rangos del valor de severidad (calificación de la probabilidad por calificación del impacto)	Calificación de severidad del evento de riesgo de LA/FT	Escala de severidad
1-5	Evento de riesgo de LA/FT <i>aceptable</i>	1
6-9	Evento de riesgo de LA/FT <i>significativo</i>	2
10-12	Evento de riesgo de LA/FT <i>moderado</i>	3
13-25	Evento de riesgo de LA/FT <i>catastrófico</i>	4

—Severidad y tolerancia de un evento de riesgo de LA/FT

La calificación del *nivel de severidad o castigo* que impone el evento de riesgo de LA/FT a una UE es un criterio que se utiliza para determinar la *actitud* que tiene la empresa por el riesgo.

Recuerde que la calificación del nivel de severidad también está indicada por el color según las convenciones utilizadas; a esa actitud se le ha denominado “tolerancia al riesgo de LA/FT” en la compañía.

El nivel de tolerancia ante el riesgo de LA/FT es único y propio de cada organización y tiene un carácter totalmente dinámico, pues varía en función de factores externos y/o internos. En el SARLA/FT, el nivel de tolerancia al *riesgo de LA/FT* está determinado por los niveles de frecuencia e impacto y por tanto también determina el grado de severidad que la empresa le quiere atribuir a cada evento de riesgo de LA/FT.

El objetivo de la gerencia de riesgos, del oficial de cumplimiento y de todos los implicados en la gestión de este riesgo es mantener el nivel de severidad que se conceda a los eventos de riesgo de LA/FT en el nivel más bajo posible, es decir, *no permitir altos niveles de tolerancia*.

La tolerancia del riesgo, su metodología de cálculo, los valores de ponderación asignados a los riesgos asociados, los valores máximos que se le asignen a la frecuencia, al impacto y por tanto a su severidad, así como el nivel de tolerancia al riesgo, deben ser consignados en políticas. Las respuestas a las siguientes preguntas podrían ayudar a definir el nivel de tolerancia:

¿Cuál es la máxima probabilidad de ocurrencia de un evento de riesgo de LA/FT que estamos dispuestos a aceptar para que este sea calificado como de severidad aceptable?

¿Cuál es el mayor valor de impacto de un evento de riesgo de LA/FT en una UE que estamos dispuestos a aceptar para que este sea calificado como de severidad aceptable?

Una medida de la tolerancia al riesgo de LA/FT se obtiene calculando la probabilidad de que un evento de riesgo de LA/FT sea calificado como

aceptable, significativo, moderado o catastrófico. Por eso, es muy útil responder a la siguiente pregunta: ¿cuál es la probabilidad de que un evento de riesgo de LA/FT sea calificado como aceptable, significativo, moderado o catastrófico?

En el ejemplo que venimos utilizando, el nivel de tolerancia del riesgo está expresado por la cantidad de superficie que se le asigne a cada tonalidad de gris en un plano cartesiano. En una matriz como la de abajo, en la cual hemos sustituido los colores por diferentes tonalidades de gris (de 5 filas por 5 columnas):

Si al área en color blanco (*riesgo aceptable*) le hemos asignado 10 porciones entre 25 posible, entonces la probabilidad que hemos otorgado para que un evento de riesgo de LA/FT sea calificado como *aceptable* es de 40% (al área en blanco se le ha asignado el 40% de la superficie del plano cartesiano).

Si al área en gris tono más claro (*riesgo significativo*) le hemos asignado 5 porciones entre 25 posible, entonces la probabilidad que hemos otorgado para que un evento de riesgo de LA/FT sea calificado como *significativo* es del 20% (al área en gris tono más claro se le ha asignado el 20% de la superficie del plano cartesiano).

Si al área en gris más oscuro (*riesgo catastrófico*) le hemos asignado 6 porciones entre 25 posible, entonces la probabilidad que hemos otorgado para que un evento de riesgo de LA/FT sea calificado como *catastrófico* es del 24% (al área en gris más oscuro se le ha asignado el 24% de la superficie del plano cartesiano).

Y así para las demás tonalidades de gris.

Tabla 19
Mapa de tolerancia al riesgo de LA/FT

PROBABILIDAD	Casi seguro	5	Severidad 5 evento de riesgo de LA/FT aceptable	Severidad 10 evento de riesgo de LA/FT moderado	Severidad 15 evento de riesgo de LA/FT catastrófico	Severidad 20 evento de riesgo de LA/FT catastrófico	Severidad 25 evento de riesgo de LA/FT catastrófico
	Probable	4	Severidad 4 evento de riesgo de LA/FT aceptable	Severidad 8 evento de riesgo de LA/FT significativo	Severidad 12 evento de riesgo de LA/FT moderado	Severidad 16 evento de riesgo de LA/FT catastrófico	Severidad 20 evento de riesgo de LA/FT catastrófico
	Possible	3	Severidad 3 evento de riesgo de LA/FT aceptable	Severidad 6 evento de riesgo de LA/FT significativo	Severidad 9 evento de riesgo de LA/FT significativo	Severidad 12 evento de riesgo de LA/FT moderado	Severidad 15 evento de riesgo de LA/FT catastrófico
	Raro	2	Severidad 2 evento de riesgo de LA/FT aceptable	Severidad 4 evento de riesgo de LA/FT aceptable	Severidad 6 evento de riesgo de LA/FT significativo	Severidad 8 evento de riesgo de LA/FT significativo	Severidad 10 evento de riesgo de LA/FT moderado
	Improbable	1	Severidad 1 evento de riesgo de LA/FT aceptable	Severidad 2 evento de riesgo de LA/FT aceptable	Severidad 3 evento de riesgo de LA/FT aceptable	Severidad 4 evento de riesgo de LA/FT aceptable	Severidad 5 evento de riesgo de LA/FT aceptable
			1	2	3	4	5
			Insignificante	Leve	Moderado	Crítico	Catastrófico
			Impacto				

En la tabla anterior:

- El área en blanco corresponde a un ERLA/FT aceptable;
- El área en color gris de tono más claro se refiere a un ERLA/FT significativo;

- c) El área en color gris de tono medio oscuro se refiere a un ERLA/FT moderado, y
- d) El área en color gris oscuro se refiere a un ERLA/FT catastrófico.

7.5. Disposición gráfica del mapa de un evento de riesgo de LA/FT

Cuanto más grandes sean las áreas en blanco y en gris de tono más claro, mayor debería ser el nivel de tolerancia al riesgo, porque esas áreas corresponden a las severidades más bajas de los eventos de riesgo de LA/FT (determinadas por las menores probabilidades de ocurrencia y menores impactos). Ahora, cuanto más grandes sean las áreas de color gris de tono medio oscuro y gris oscuro, menor debería ser el nivel de tolerancia por el riesgo porque esas áreas corresponden a las severidades más altas de los eventos de riesgo de LA/FT (determinadas por la mayor probabilidad de ocurrencia y mayores impactos).

Una vez se realice la medición de la probabilidad y el impacto para los eventos de riesgo de LA/FT identificados en cada proceso, se debe realizar la medición consolidada para la entidad, determinando el perfil corporativo del riesgo inherente (para lo cual es necesario tener en cuenta la definición que proporcionamos de *riesgo inherente*).

7.5.1. *Medición de probabilidad e impacto del riesgo inherente*

- *Obtención de valores de probabilidad de evento de riesgo de LA/FT que conforman el riesgo inherente*

A manera de ejemplo, presentamos la matriz que se podría elaborar con los cuatro primeros eventos de riesgo de LA/FT identificados anteriormente.

Tabla 20
Ejemplo de medición de frecuencia para el riesgo inherente

Cantidad total de operaciones realizadas en el período				497.820		
Nombre	Código	Factor determinante del RLA/FT	Probabilidad inherente			
Nombre del evento de riesgo de LA/FT	Cód.	Factor determinante del riesgo	Número eventos riesgo inherente	Valor de la probabilidad riesgo inherente	Escala de la probabilidad riesgo inherente	Calificación de la probabilidad riesgo inherente
Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	Clientes	8.163	1,63975%	4	Evento de riesgo de LA/FT <i>probable</i> : entre 1,5% y < 2,0%
Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	Clientes	6.100	1,22534%	3	Evento de riesgo de LA/FT <i> posible</i> : Entre 0,05% y < 1,5%
Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	Clientes	20.000	4,01752%	5	Evento de riesgo de LA/FT <i>CASI seguro</i> : > = 2,0%
Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	Clientes	36	0,00723%	2	Evento de riesgo de LA/FT <i>raro</i> : entre 0,0050% y < 0,05%

—*Obtención de valores de impacto por riesgos asociados de los eventos de riesgo de LA/FT que conforman el riesgo inherente*

Tabla 21

Ejemplo de medición del impacto para el riesgo inherente

Identificación		Valores de impacto por riesgos asociados para el riesgo inherente				
Nombre	Código	Riesgo legal inherente	Riesgo reputacional inherente	Riesgo de contagio inherente	Riesgo operacional inherente	Impacto total riesgos inherentes asociados
Nombre del evento de riesgo de LA/FT	Cód.	30%	40%	10%	20%	Impacto total riesgos inherentes asociados
Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	2 - Menor: multas, gastos jurídicos e indemnizaciones entre 5 y 100 millones de pesos.	4 - Mayor: divulgación de eventos y/o investigación por organismo regulador dado a conocer al público en medios informativos masivos y/o principales noticieros nacionales.	0	4- Mayor: Multa - Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 1 Insignificante: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 0 a 5 mm de pesos .000 y 5 Superior: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto mayor a 5.00 mm de pesos .000 mm de pesos	3,0
Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	2 - Menor: Multas, gastos jurídicos e indemnizaciones entre 5 y 100 millones de pesos	0	0	0	0,6

Identificación		Valores de impacto por riesgos asociados para el riesgo inherente				
Nombre	Código	Riesgo legal inherente	Riesgo reputacional inherente	Riesgo de contagio inherente	Riesgo operacional inherente	Impacto total riesgos inherentes asociados
Nombre del evento de riesgo de LA/FT	Cód.	30%	40%	10%	20%	Impacto total riesgos inherentes asociados
Realización de operaciones con clientes/usuarios que cambian frecuentemente datos para su localización.	Evento de riesgo de LA/FT-03	3 - IMPORTANTE: Multas, gastos jurídicos e indemnizaciones entre 100 y 1.000 millones de pesos	0	0	0	0,9
Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	2 - Menor: Multas, gastos jurídicos e indemnizaciones entre 5 y 100 millones de pesos	2 - Menor: aviso sorpresivo de prensa u otro medio masivo.	0	2 Menor: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 5 y 50 mm de pesos y 1. Insuficiente: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 0 a 5 mm de pesos 00 mm de pesos	1,8

— *Severidad de evento de riesgo de LA/FT que conforma el riesgo inherente*

Tabla 22

Ejemplo de medición de la severidad para el riesgo inherente

Nombre	Código	Severidad inherente del ERLA/FT	
Nombre del evento de riesgo de LA/FT	Cód.	Valor de la severidad del evento de riesgo de LA/FT riesgo inherente	Clasificación severidad riesgo inherente
Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	12	12 - 4 X 3- evento de riesgo de LA/FT <i>con severidad significativa.</i>
Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	3	3 - 3 X 1 -evento de riesgo de LA/FT <i>con severidad aceptable.</i>
Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	10	10 - 5 X 2- evento de riesgo de LA/FT <i>con severidad significativa.</i>
Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	2	2- 1 X 2- evento de riesgo de LA/FT <i>con severidad aceptable.</i>

— *Mapa de eventos de riesgo inherente de LA/FT*

Los valores de probabilidad, impacto y severidad de los eventos de riesgo de LA/FT se pueden visualizar como se expresa en la tabla del anexo 2. Dicha tabla, a su vez, se puede representar en un plano cartesiano como el siguiente, que corresponde a un evento de riesgo de LA/FT de riesgo inherente:

Tabla 23

Otra presentación del mapa de eventos de riesgo de LA/FT inherentes

Probabilidad	Casi seguro	5	9-10-11	6	2		
	Probable	4	18	8	3	1	
	Possible	3			7	4-5	
	Raro	2		16			
	Improbable	1	19			17	12-13-14-15
		1		2	3	4	5
		Insignificante	Leve	Moderado	Crítico	Catastrófico	
Impacto							

7.5.2. *Medición de probabilidad, impacto y severidad de un evento de riesgo de LA/FT del riesgo residual*

Para obtener estos valores se requieren datos históricos de la operación de la empresa que sirvan como fuente de información para hacer los cálculos respectivos.

A continuación exponemos un ejemplo que corresponde a cinco eventos de riesgo de LA/FT que ya recibieron el tratamiento de control y que por tanto su probabilidad e impacto pudieron haber variado. Para los eventos de riesgo de LA/FT, identificados los datos de la nueva probabilidad después de establecido el control, podrían ser los siguientes:

Tabla 24
Ejemplo de medición de frecuencia para el riesgo residual

Nombre del evento de riesgo de LA/FT	Cód.	Probabilidad residual			
		Número de eventos ocurridos riesgo residual	Valor probabilidad riesgo residual	Valor descriptivo de la probabilidad riesgo residual	Descripción de la probabilidad riesgo residual
Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	3	0,6026%	3	Evento de riesgo de LA/FT <i>medianamente probable</i> : entre 0,05% y 1,5%
Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	2	0,4018%	3	Evento de riesgo de LA/FT <i>medianamente probable</i> : entre 0,05% y 1,5%
Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización	Evento de riesgo de LA/FT-03	7	1,4061%	3	Evento de riesgo de LA/FT <i>medianamente probable</i> : entre 0,05% y 1,5%
Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	18	0,0036%	1	Evento de riesgo de LA/FT RARO: Entre 0 % y 0,005%
Realización de operaciones con clientes que solicitan transferencias de propiedad, a otras personas diferentes del titular o entrega de dinero a un tercero.	Evento de riesgo de LA/FT-05	2	0,0004%	3	Evento de riesgo de LA/FT RARO: Entre 0 % y 0,005%

— *Obtención de valores de impacto de cada uno de los riesgos asociados y el impacto total de cinco eventos de riesgo de LA/FT que conforman el riesgo residual*

Las ponderaciones indicadas para cada riesgo son definidas mediante la política de la empresa. Un ejemplo de mediación del impacto para el riesgo residual se presenta en la tabla del anexo 3.

—*Obtención de valores de severidad de cinco eventos de riesgo de LA/FT que conforman el riesgo residual*

Tabla 25

Ejemplo de medición de la severidad para el riesgo residual

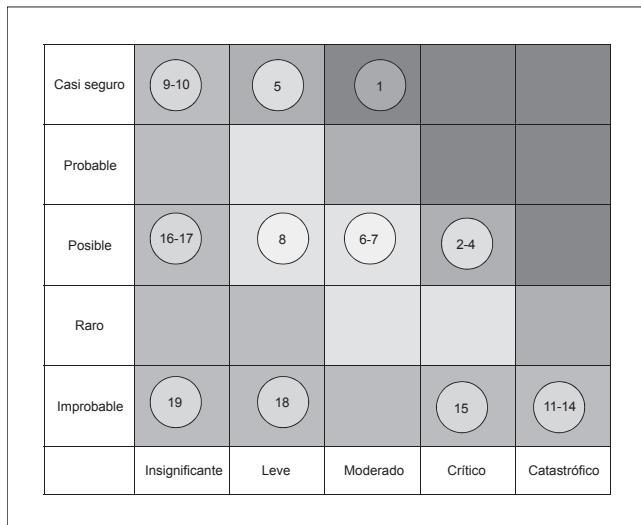
Identificación		Severidad residual del evento de riesgo de LA/FT	
Nombre	Código	Valor de la severidad del evento de riesgo de LA/FT riesgo residual	Clasificación severidad riesgo residual
Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	12	9 - 3 X 3 - evento de riesgo de LA/FT con severidad <i>significativa</i>
Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	3	3 - 3 X 1 - evento de riesgo de LA/FT con severidad <i>aceptable</i>
Realización de operaciones con clientes usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	10	3 - 3 X 1 - evento de riesgo de LA/FT con severidad <i>aceptable</i>
Realización de operaciones con clientes usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	2	1 - 1 X 1 - evento de riesgo de LA/FT con severidad <i>aceptable</i>
Realización de operaciones con clientes que solicitan transferencias de propiedad, a otras personas diferentes del titular o entrega de dinero a un tercero.	Evento de riesgo de LA/FT-05	9	9 - 3 X 3 - evento de riesgo de LA/FT con severidad <i>significativa</i>

—*Mapa de eventos de riesgo residual de LA/FT*

Los valores de probabilidad, impacto y severidad de los eventos de riesgo de LA/FT se pueden visualizar como se expresa en la tabla del anexo 6 sobre medición del riesgo residual. Para ilustrar esto hemos ampliado la cantidad de eventos de riesgo de LA/FT considerados de 5 a 19 (ver anexo 4).

En este gráfico se representan los mismos valores de la tabla del anexo 4, pero en el plano cartesiano.

Gráfico 23
Otra presentación del mapa de eventos de riesgo de LA/FT residual

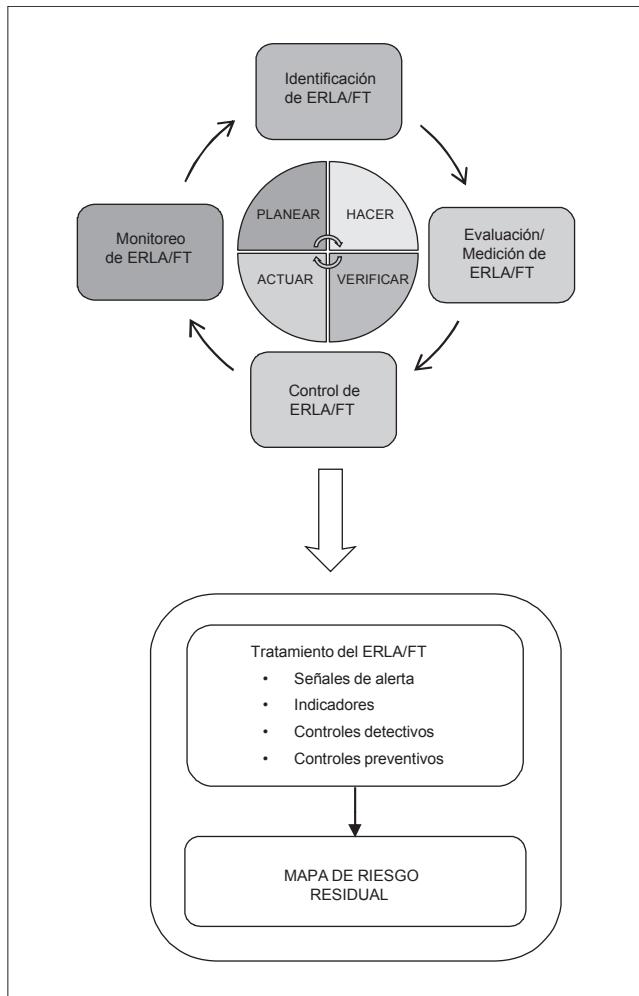


La figura anterior se construyó a partir de un plano cartesiano para el cual, en el eje horizontal (el eje “X”), se incluyó la escala de medición del impacto total por los riesgos asociados, y en el eje vertical (el eje “Y”), la escala que mide la probabilidad de ocurrencia de los diferentes eventos de riesgo de LA/FT. El punto indicativo del cruce de los valores X y asignados a cada eje corresponde a la severidad: las 4 áreas en tonalidades de gris son los sitios donde se puede ubicar cada evento de riesgo de LA/FT y, como se puede apreciar, según su tonalidad de gris el indicador de severidad varía.

Cuando un evento de riesgo de LA/FT es sometido a tratamiento, mediante controles, probablemente variarán la probabilidad de ocurrencia y su impacto y por tanto su nivel de severidad; los cambios en severidad del evento de riesgo de LA/FT implican desplazamiento dentro del mapa.

8. METODOLOGÍA DE CONTROL DE EVENTOS DE RIESGO DE LA/FT

Gráfico 24
Control de eventos de riesgo de LA y FT



En esta etapa la empresa debe tomar las medidas conducentes a controlar el riesgo inherente al que se ve expuesta, en razón de los factores de riesgo y de los riesgos asociados. Para controlar el riesgo de LA/FT, la

empresa debería establecer las metodologías para definir las medidas de control del riesgo de LA/FT y aplicarlas para cada uno de los factores de riesgo y de los riesgos asociados. Además de determinar los niveles de exposición al riesgo en razón de la calificación dada a los factores de riesgo en la etapa de medición, deberá realizar los reportes de operaciones sospechosas a la Unidad Administrativa Especial de Información y Análisis Financiero (UIAF). Como resultado de esta etapa la empresa debe fijar el perfil de riesgo residual de LA/FT. El control debe traducirse en una disminución de la posibilidad de ocurrencia y/o del impacto del riesgo de LA/FT en caso de materializarse.

8.1. Metodología de los “cinco por qué”

La implementación de la metodología de identificación de evento de riesgo de LA/FT, mediante la aplicación del diagrama causa-efecto (“espira de pescado”), podría dar como resultado varias posibles causas de pérdida; por tanto, es necesario identificar la causa raíz o causa principal, para lo cual se debe utilizar la metodología de los “cinco por qué”.

Para implementar esta metodología, es necesario conformar grupos de trabajo que den respuestas sustentadas a cada una de las causas asociadas a una pérdida, para finalmente determinar exactamente la causa raíz o causa principal.

La metodología citada consiste en que una vez identificadas las causas probables de la pérdida se debe iniciar un cuestionamiento de ¿por qué es así? o ¿por qué puede pasar esto?

Con relación al tipo de pérdida que está en consideración y al factor de riesgo bajo análisis y sus situaciones de riesgo asociadas, una manera más directa de formular la misma pregunta es la siguiente: ,¿qué tipo de causa o causas encuentra que pueden explicar esa pérdida? o ¿por qué ese tipo de causa genera una pérdida?

Luego, se continuará preguntando el “por qué” o se formulará la misma pregunta al menos cinco (5) veces, para buscar a fondo y no conformarse con causas ya probadas y ciertas. Habrá ocasiones en que se puede

ir más allá de las cinco (5) veces preguntando “por qué” para obtener la causa principal. Durante este tiempo se debe tener cuidado de no empezar a preguntar “quién”, pues se debe recordar que el interés es en el proceso y no en las personas involucradas.

Para iniciar este tema, es necesario recordar dos conceptos expuestos anteriormente:

Riesgo inherente del LA/FT, es decir, el nivel de riesgo medido por la severidad del evento de riesgo de LA/FT sin tener en cuenta el efecto de los controles, y

Riesgo residual o neto de LA/FT, definido como el nivel de severidad resultante después de aplicar las medidas de prevención y/o control del LA/FT; es decir, podemos hablar de severidad del evento de riesgo de LA/FT sin controles y severidad del mismo como consecuencia de los controles.

Conociendo la causa final que genera un evento de riesgo de LA/FT, debemos tomar medidas para eliminarlas o mitigarlas, es decir, la siguiente etapa es *controlar las causas*.

El objetivo de esta etapa es tomar medidas que propendan por la disminución de la frecuencia e impacto de los eventos de riesgo de LA/FT a los que se ve expuesta la empresa; obviamente, esas medidas tienen que ver con: la prevención y control de las causas, con los factores de riesgo, con las situaciones de riesgo, con las señales de alerta y con los riesgos asociados identificados en un evento de riesgo de LA/FT.

Se deberán implementar nuevos controles o reforzar los existentes con el fin de reducir la probabilidad de ocurrencia o el impacto que se pueda generar en caso de materializarse el evento de riesgo de LA/FT.

Para adelantar esta etapa de control de deben ejecutar los siguientes procesos:

- a) Identificar los controles de LA/FT existentes propuestos o recomendados casi siempre por la auditoría interna y/o la revisoría fis-

cal de la empresa, para prevenir el riesgo de LA/FT. Debido a que la cultura de la prevención y control del riesgo de LA/FT es reciente, en las empresas generalmente no existen controles con el propósito específico de prevenir el LA/FT;

- b) En caso de que exista este tipo de controles, el siguiente paso es evaluar su efectividad para reducir el impacto y/o la probabilidad del evento de riesgo de LA/FT, y
- c) Medir la efectividad del control para establecer el riesgo residual.

A continuación se explicará cada paso.

8.2. Identificación de controles existentes

El gerente de riesgos y el oficial de cumplimiento deben identificar y describir solamente los controles existentes para los eventos de riesgo de LA/FT inherentes o puros identificados, si es que existen, para lo cual se requiere revisar los manuales de procesos y procedimientos, las políticas y toda la documentación que permita identificar los controles existentes que se aplican para prevenir y controlar estos eventos, para luego consignar la información referente al mismo en una matriz que, sugerimos, contenga el registro de los siguientes elementos de control para cada evento de riesgo:

- a) Descripción de la actividad o recurso de control existente implementado para minimizar la severidad del evento de riesgo de LA/FT;
- b) Descripción breve del nombre del control existente;
- c) Identificar el objetivo del control existente. Los objetivos podrían ser: disminuir frecuencia, disminuir impacto, disminuir frecuencia e impacto;
- d) Indicar el estado de implementación del control existente; es decir; si está o no funcionando actualmente;

- e) Definir un costo aproximado del control;
- f) Indicar la última fecha de revisión del control;
- j) Describir las debilidades que tiene el control existente;
- h) Indicar la efectividad que ha tenido el control: pobre, adecuado, bueno;
- i) Indicar la frecuencia de aplicación del control: continuo, diario, semanal, mensual, semestral, anual;
- j) Indicar la forma como se aplica el control: manual, automático;
- k) Indicar persona responsable de la revisión del control;
- l) Indicar la persona responsable de la aplicación del control, y
- m) Indicar si se interrumpe un macroproceso, proceso o actividad de la empresa y si la interrupción es menor o mayor a 3 días.

8.3. **Validación y evaluación de controles actuales (para el riesgo inherente)**

Una vez identificados los controles, se debe verificar su implementación en los procesos donde se encuentran involucrados los riesgos. Esta verificación se debe realizar mediante reuniones en las cuales participan los empleados que están directamente relacionados en cada uno de los procesos. Para la evaluación de los controles se deben calificar atributos, como por ejemplo el tipo de control, la frecuencia del mismo, la responsabilidad y la ejecución, entre otros. La calificación consolidada de los atributos arroja evaluaciones sobre el diseño y solidez del control, determinando la fortaleza del mismo. Al igual que las anteriores etapas, es indispensable documentar los resultados con el fin de tener evidencia de la gestión.

8.3.1. *Relación costo-beneficio de controles de eventos de riesgo de LA/FT*

El gerente de riesgos y el oficial de cumplimiento deben evaluar la relación costo-beneficio de los controles existentes aplicados a los eventos de riesgo de LA/FT identificados.

El costo del control (C), medido en pesos, estará conformado por el valor de la pérdida que generó el evento de riesgo de LA/FT más el costo directo del control.

El beneficio del control estará representado por el valor de la pérdida (impacto) que ha recibido la UE debido al evento de riesgo de LA/FT.

C = COSTO: valor de la pérdida + costo del control (medido en \$)

B = BENEFICIO: disminución de la pérdida (medido en \$)

Los datos y conclusiones de esta relación, para cada evento de riesgo de LA/FT, deberían ser presentados a la junta directiva para que ella decida si se acepta o rechaza el control.

— *Criterios de decisión para seleccionar un control de un evento de riesgo de LA/FT*

Estos criterios están basados en la comparación entre el costo y el beneficio. Si el costo es mayor que el beneficio, se rechaza el control; si el costo es igual al beneficio, se podría aceptar el control; si el costo es menor que el beneficio, se acepta definitivamente el control.

Al tratarse de controles para eventos de riesgo de LA/FT que probablemente no existían, una vez se ha establecido la severidad del riesgo inherente o residual y la relación costo-beneficio de cada control, se debe decidir si el control se mantiene o se aplica nuevamente a un proceso de tratamiento o se mejora el existente.

El gerente de riesgos en conjunto con el oficial de cumplimiento propondrán las posibles acciones a emprender o las opciones para el tratamiento de cada evento de riesgo de LA/FT, según su ubicación dentro de la matriz de riesgos inherentes o residuales, teniendo en cuenta cada caso.

Los tratamientos para los eventos de riesgo de LA/FT deben ser factibles y efectivos y pueden consistir en la redefinición de políticas y estándares, el mejoramiento o definición de nuevas señales de alerta, la redefinición de procesos y procedimientos, entre otros.

La selección de las acciones más convenientes debe considerar la viabilidad jurídica, técnica, organizacional, financiera y económica. Además, es muy importante considerar, en las decisiones sobre los tratamientos, el caso particular de un evento de riesgo de LA/FT cuya probabilidad de ocurrencia es rara y su impacto es crítico o catastrófico, ya que podría resultar que estos, a pesar de no tener impactos económicos, sí puedan generar riesgos legales, reputacionales o de sobrevivencia para la organización.

8.3.2. *Decisiones con respecto a los controles de eventos de riesgo de LA/FT*

Las alternativas de decisión son evitar el riesgo, reducir la severidad del riesgo mediante su tratamiento y retener (aceptar-asumir) el evento de riesgo de LA/FT, las cuales pueden ser consideradas independientemente una de la otra, interrelacionadas o en conjunto:

— Evitar el evento de riesgo de LA/FT: siempre es la primera alternativa a considerar. Implica considerar la decisión de no iniciar o continuar con la actividad que genera el evento de riesgo de LA/FT.

— Reducir-tratar el evento de riesgo de LA/FT: en el caso que el evento de riesgo de LA/FT no pueda ser evitado porque crea grandes dificultades operacionales, la siguiente alternativa es reducirlo al más bajo nivel posible. Este es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

Se consigue mediante:

- a) El rediseño del proceso o la actividad;
- b) La optimización de los procedimientos;
- c) La implementación de controles, y
- d) El mejoramiento del control existente a partir de acciones para reducir la frecuencia, para reducir la pérdida y para reducir la pérdida y la frecuencia.

—Retener-aceptar-asumir el evento de riesgo de LA/FT: luego de que el evento de riesgo de LA/FT ha sido reducido puede quedar un riesgo residual que se mantiene, en este caso la junta directiva, el comité de riesgos o la alta gerencia debe aceptar la pérdida residual probable y debe elaborar planes de tratamiento para su manejo.

Después de establecido el nuevo control para determinar el nivel de severidad resultante y producir el nuevo mapa de evento de riesgo de LA/FT residual, periódicamente se debe calificar la probabilidad de ocurrencia y el impacto. Dependiendo de los resultados obtenidos, se continuará proponiendo nuevas medidas o mejoras al control hasta que su nivel de severidad permita a la junta directiva decidir si asume el evento de riesgo de LA/FT residual.

La información sobre los controles existentes y los planes de tratamiento establecidos para cada evento de riesgo de LA/FT deben registrarse en el formato de perfil de riesgo.

—*Ejemplo de causas y controles para cinco eventos de riesgo de LA/FT*

En la tabla del anexo 5 se expone un ejemplo de las causas y controles para los eventos de riesgo de LA/FT indicados anteriormente.

Le recordamos que para el diseño de controles se deben tener en cuenta las causas de los eventos de riesgo de LA/FT obtenidas al aplicar la metodología de “espina de pescado”.

8.4. Medición de la efectividad de los controles

Todo control tiene como objetivo reducir la frecuencia o el impacto o, conjuntamente, la frecuencia y el impacto del evento de riesgo de LA/FT.

La efectividad de un control (EC) se mide mediante un indicador de efectividad del control (IE_C) y se define como la capacidad que tiene el control para reducir la severidad de un evento de riesgo de LA/FT mediante la reducción de su frecuencia o de su impacto o los dos de manera simultánea.

El IEC se calcula mediante la diferencia entre el indicador de la severidad del riesgo residual (S_{RR}), ya incluido el control y el indicador de la severidad del riesgo inherente (S_{RI}):

$$(IE_C) = (S_{RR}) - (S_{RI})$$

De esta forma:

Si $IE_C > 0$ (+) es porque $S_{RR} > S_{RI}$, lo que equivale a decir que el control *no* tiene capacidad para disminuir la severidad y por tanto el control no es efectivo.

Si $IE_C = 0$ es porque $S_{RR} = S_{RI}$, lo que también equivale a decir que el control *no* tiene capacidad para disminuir la severidad y por tanto el control no es efectivo.

Si $IE_C < 0$ (-) es porque $S_{RR} < S_{RI}$, lo que también equivale a decir que el control *sí* tiene capacidad para disminuir la severidad y por tanto el control es efectivo.

Puesto que estamos analizando el evento de riesgo de LA/FT después de haber recibido algún tipo de control, a continuación se presenta una ta-

bla donde se calcula la efectividad del control, en la cual se puede observar que el valor de la efectividad del control es negativo para los eventos de riesgo de LA/FT con códigos (por lo que podemos determinar que sus controles son eficaces):

- Evento de riesgo de LA/FT-01
- Evento de riesgo de LA/FT-03
- Evento de riesgo de LA/FT-04
- Evento de riesgo de LA/FT-07
- Evento de riesgo de LA/FT-14

En la tabla del anexo 6 se compara el mapa de riesgo inherente con el mapa de riesgo residual y se obtiene el indicador de la efectividad de cada control.

8.4.1. Análisis de efectividad de controles

En las tablas y gráficos siguientes se observa que:

Los controles aplicados a los eventos de riesgo de LA/FT marcados en la última columna con gris oscuro han tenido un efecto positivo sobre la severidad, porque el valor de esta para el riesgo residual es menor que la del riesgo inherente, con lo cual se concluye que el control propuesto es eficiente.

Mientras que los controles marcados en gris claro indican que la severidad del riesgo se mantuvo constante debido a que, según el criterio de los expertos, es recomendable que esos eventos de riesgo de LA/FT se mantengan en la zona gris de tono más claro del mapa de riesgos, donde la severidad es significativa, a fin de seguirlos monitoreando con mayor frecuencia.

Los controles marcados en gris de tono más claro indican que con la medida de control propuesta la severidad del evento de riesgo de LA/FT aumentaría, lo cual no tiene ninguna lógica, razón por la cual se debe revisar el control propuesto o los criterios utilizados por los expertos para determinar la probabilidad e impacto en el riesgo residual.

Tabla 26
Análisis de efectividad de controles

Cód.	Valor de la probabilidad riesgo inherente	Valor probabilidad riesgo residual	Impacto total riesgos inherentes asociados	Impacto total riesgos residuales asociados	Valor de la severidad riesgo inherente	Valor de la severidad riesgo residual	Variación favorable (<) desfavorable (>) de la severidad
Evento de riesgo de LA/FT-01	1,64%	0,60%	3	3	12	9	<
Evento de riesgo de LA/FT-02	1,23%	0,40%	0,6	0,6	3	3	=
Evento de riesgo de LA/FT-03	4,02%	1,41%	0,9	0,9	10	3	<
Evento de riesgo de LA/FT-04	0,01%	0,00%	1,8	1,8	2	1	<
Evento de riesgo de LA/FT-05	0,00%	0,00%	3,6	3,6	9	9	=
Evento de riesgo de LA/FT 06	0,00%	0,00%	4,5	4,5	4	4	=
Evento de riesgo de LA/FT-07	1,64%	0,80%	1,5	1,5	4	3	<
Evento de riesgo de LA/FT-08	0,00%	0,00%	0,9	0,9	1	1	=
Evento de riesgo de LA/FT-09	6,06%	3,01%	1,5	1,5	10	10	=
Evento de riesgo de LA/FT-10	0,36%	0,36%	3,3	3,3	9	9	=
Evento de riesgo de LA/FT-11	0,33%	0,16%	3,6	3,6	9	9	=
Evento de riesgo de LA/FT-12	0,00%	0,00%	4,5	4,5	4	4	=
Evento de riesgo de LA/FT-13	30,13%	30,13%	0,9	0,9	10	10	=
Evento de riesgo de LA/FT-14	1,76%	0,80%	3,6	3,6	12	9	<
Evento de riesgo de LA/FT-15	27,69%	27,69%	0,9	0,9	10	10	=
Evento de riesgo de LA/FT-16	27,69%	16,07%	2,7	2,7	10	10	=
Evento de riesgo de LA/FT-17	0,00%	0,00%	4,1	4,1	4	4	=

Cód.	Valor de la probabilidad riesgo inherente	Valor probabilidad riesgo residual	Impacto total riesgos inherentes asociados	Impacto total riesgos residuales asociados	Valor de la severidad riesgo inherente	Valor de la severidad riesgo residual	Variación favorable (<) desfavorable (>) de la severidad
Evento de riesgo de LA/FT-18	0,00%	0,00%	4,7	4,7	4	4	=
Evento de riesgo de LA/FT-19	0,00%	0,00%	4,7	4,7	4	4	=

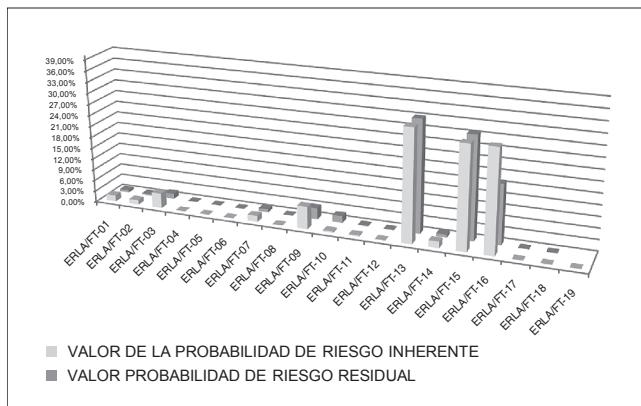
En el gráfico 25 se puede apreciar que los eventos de riesgo de LA/FT con probabilidad significativamente superior a la de los demás, tanto cuando se calculó para el riesgo inherente como para el residual, son los identificados con los códigos 13, 15 y 16, que se definieron brevemente de la siguiente manera:

Realización de operaciones en jurisdicciones catalogadas como de alto nivel de exposición al riesgo de LA/FT-13.

Realización de operaciones en oficinas que presentan un alto volumen de operaciones sospechosas de riesgo de LA/FT-15.

Realización de operaciones en oficinas ubicadas en regiones de alto nivel de exposición al riesgo de LA/FT-16.

Gráfico 25
Probabilidad inherente y residual de evento de riesgo de LA/FT



En el gráfico 26 se puede apreciar que los eventos de riesgo de LA/FT con impacto total por riesgos asociados significativamente superior a la de los demás, tanto para el riesgo inherente como para el residual, son los identificados con los códigos 5, 6, 10, 11, 12, 14, 16, 17, 18 y 19, que se definieron brevemente de la siguiente manera:

Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT (evento de riesgo de LA/FT-01).

Realización de operaciones con clientes que solicitan transferencias de propiedad a otras personas diferentes del titular o entrega de dinero a un tercero (evento de riesgo de LA/FT-05).

Realización de operaciones con clientes/usuarios incluidos en listas restrictivas (evento de riesgo de LA/FT-06).

Realización de operaciones con clientes/usuarios que no se identifican plenamente (evento de riesgo de LA/FT-10).

Realización de operaciones con clientes/usuarios que suplantan al verdadero cliente o usuario (evento de riesgo de LA/FT-11).

Realización de operaciones con productos que utilizan fondos de dinero provenientes de países bloqueados o catalogados como más expuestos a LA/FT (evento de riesgo de LA/FT-12).

Realización de operaciones en las que se solicita frecuente cambio de titular, apoderado o beneficiario de un producto (evento de riesgo de LA/FT-14).

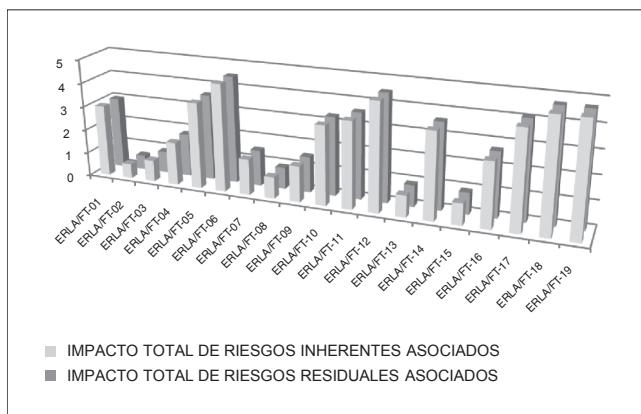
Realización de operaciones en oficinas ubicadas en regiones de alto nivel de exposición al RLA/FT (evento de riesgo de LA/FT-16).

Realización de operaciones por empleados o funcionarios que adoptan comportamientos sospechosos: evaden controles, frecuentemente incurren en errores, impiden que otro compañero atienda a determinado cliente, se ausentan de su trabajo, terminan su jornada después de lo normal, tienen un estilo de vida que no se ajusta a su nivel de ingresos, etc. (evento de riesgo de LA/FT-17).

Participación de socios y directivos en aprobación de operaciones posiblemente relacionadas con actividades de LA/FT (evento de riesgo de LA/FT-18).

Realización de operaciones personales o con la empresa por parte de socios, funcionarios y directivos posiblemente relacionados con actividades de LA/FT (evento de riesgo de LA/FT-19).

Gráfico 26
Impacto total inherente y residual de evento de riesgo de LA/FT



En el gráfico 27 se puede apreciar que los eventos de riesgo de LA/FT con severidad significativamente superior a la de los demás, tanto para el riesgo inherente como para el residual, son los identificados con los códigos 1, 3, 5, 9, 10, 11, 13, 14, 15 y 16, que se definieron brevemente de la siguiente manera:

Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT (evento de riesgo de LA/FT-01).

Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización (evento de riesgo de LA/FT-03).

Realización de operaciones con clientes que solicitan transferencias de propiedad a otras personas diferentes del titular o entrega de dinero a un tercero (evento de riesgo de LA/FT-05).

Realización de operaciones con clientes/usuarios que frecuentemente aparecen incluidos en operaciones inusuales, señales de alerta y/o múltiples con cualquiera de los productos de la empresa (evento de riesgo de LA/FT-09).

Realización de operaciones con clientes/usuarios que no se identifican plenamente (evento de riesgo de LA/FT-10).

Realización de operaciones con clientes/usuarios que suplantan al verdadero cliente o usuario (evento de riesgo de LA/FT-11).

Realización de operaciones en jurisdicciones catalogadas como de alto nivel de exposición al riesgo de LA/FT (evento de riesgo de LA/FT-13).

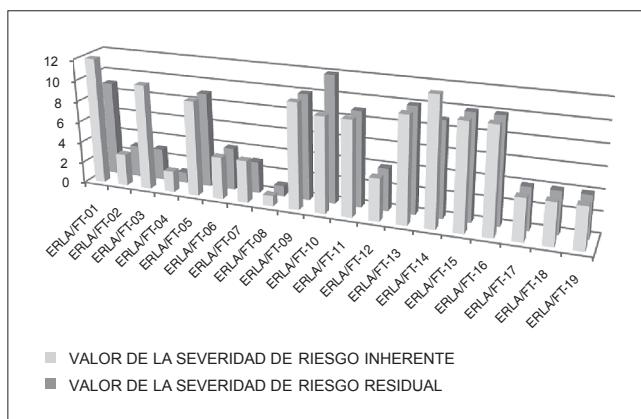
Realización de operaciones en las que se solicita frecuente cambio de titular, apoderado o beneficiario de un producto (evento de riesgo de LA/FT-14).

Realización de operaciones en oficinas que presentan un alto volumen de operaciones sospechosas (evento de riesgo de LA/FT-15).

Realización de operaciones en oficinas ubicadas en regiones de alto nivel de exposición al RLA/FT (evento de riesgo de LA/FT-16).

Gráfico 27

Severidad inherente y residual de evento de riesgo de LA/FT

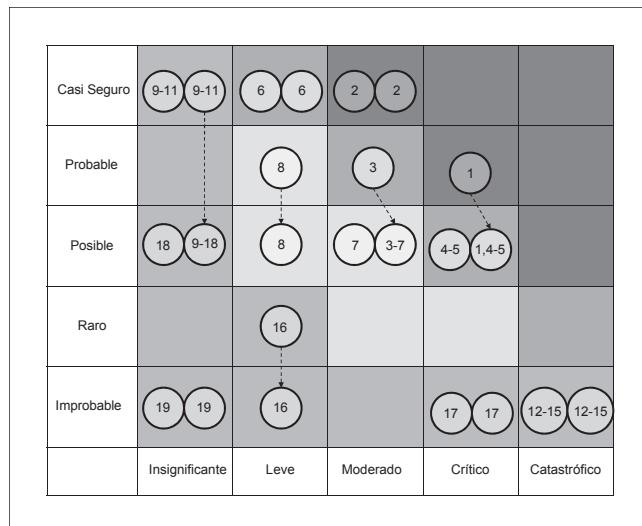


Los eventos de riesgo de LA/FT con los controles menos efectivos. Son los que presentan la más alta probabilidad y el mayor impacto después de establecidos los controles, es decir, los incluidos en las relaciones anteriores.

8.3.2. *Consolidación de mapas de riesgo (residual e inherente)*

En este gráfico se superponen el mapa de riesgo inherente y el de riesgo residual, en el cual se muestran gráficamente los efectos que generaron los controles en la probabilidad y el impacto para cada evento de riesgo de LA/FT, y por tanto permite visualizar la efectividad de los controles.

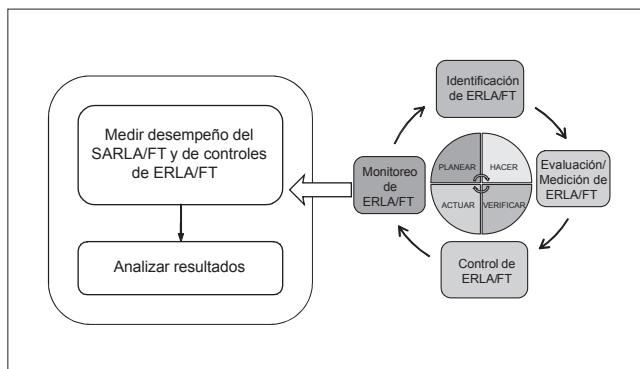
Gráfico 28
Mapa de eventos de riesgo inherente y riesgo residual comparados



9. MONITOREO DE EVENTOS DE RIESGO DE LA/FT

Gráfico 29

Monitoreo de eventos de riesgo de LA/FT



Esta etapa debe permitir a la organización hacer seguimiento del perfil de riesgo y en general del SARLA/FT, así como llevar a cabo la detección de operaciones inusuales y/o sospechosas.

Para monitorear el evento de riesgo de LA/FT se debería:

Desarrollar un proceso de seguimiento efectivo que facilite la rápida detección y corrección de las deficiencias del SARLA/FT. Dicho seguimiento debe tener una periodicidad acorde con el perfil de riesgo residual de LA/FT, pero en todo caso debe realizarse con una periodicidad mínima semestral.

Realizar el seguimiento y comparación del riesgo inherente y residual de cada factor de riesgo y de los riesgos asociados.

Asegurar que los controles sean comprensivos de todos los riesgos y que los mismos estén funcionando en forma oportuna, efectiva y eficiente.

Establecer indicadores descriptivos y/o prospectivos que evidencien potenciales fuentes de riesgo de LA/FT.

Asegurar que los riesgos residuales se encuentren en los niveles de aceptación establecidos por la empresa.

El monitoreo debe permitir a la empresa comparar la evolución del perfil de riesgo inherente con el perfil de riesgo residual de LA/FT.

Como resultado de esta etapa se deben desarrollar reportes que permitan establecer las evoluciones del riesgo, así como la eficiencia de los controles implementados. Igualmente se deben determinar las operaciones inusuales y sospechosas.

El monitoreo consiste en hacer seguimiento del comportamiento de la severidad a los eventos de riesgo de LA/FT en las UE y, en general, del SARLA/FT, así como detectar operaciones inusuales y/o sospechosas. Y su objetivo principal es asegurar continuamente que los controles y planes de acción definidos para los eventos de riesgo de LA/FT sean eficaces y se cumplan según lo establecido.

Una vez se han diseñado y validado los controles para tratar y administrar los riesgos, se hace necesario continuar monitoreándolos a todos, aun los de baja severidad, pues debe tenerse en cuenta que aun estos últimos nunca dejan de representar una amenaza para la organización.

Otros propósitos del monitoreo son:

El seguimiento a cada riesgo inherente y residual de los factores de riesgo y riesgos asociados identificados y con posibilidad de ocurrencia.

El seguimiento de riesgo inherente y residual consolidado.

El seguimiento periódico y efectivo de las metodologías y procedimientos establecidos en las etapas del SARLA/FT que facilite la rápida detección y corrección de las deficiencias en el mismo.

El establecimiento de indicadores descriptivos y/o prospectivos para cada factor de riesgo identificado.

El aseguramiento de que los controles estén funcionando en forma efectiva, oportuna y eficiente a través de la comparación sobre la evolución del riesgo inherente frente al riesgo residual de cada factor de riesgo y de los riesgos asociados.

El aseguramiento de que los riesgos residuales se encuentren en los niveles de aceptación establecidos por la empresa.

La elaboración de reportes sobre la efectividad de los controles implementados y sobre la evolución de los riesgos en el contexto propio de la empresa, asegurando la total comprensión y funcionamiento oportuno de los controles establecidos.

La empresa debería, además, realizar un seguimiento semestral a los perfiles de riesgo y su exposición a los riesgos asociados. Para ello se requiere:

- a) Obtener informe de novedades;
- b) Evaluar contenido de informe de novedades;
- c) Evaluar indicadores descriptivos y/o prospectivos;
- d) Establecer si los controles estén funcionando en forma efectiva, oportuna y eficiente;
- e) Analizar mapa de riesgo residual;
- f) Determinar si riesgo residual se encuentren en los niveles de aceptación establecidos;
- g) Determinar prioridad de tratamiento, y
- h) Documentar monitoreo.

El monitoreo podría estar a cargo del gerente de riesgos, quien debería presentar como resultado de esta etapa reportes que permitieran establecer las evoluciones del riesgo, así como la efectividad de los controles implementados y los ajustes necesarios para asegurar un efectivo manejo del riesgo. Así mismo, en esta etapa se deberían determinar las operaciones inusuales y sospechosas, sin perjuicio del cumplimiento en la remisión de los reportes establecidos.

Las áreas operacionales responsables de los procesos en los cuales se han identificado eventos de riesgo de LA/FT, deberían al momento de ocu-

rir dicho evento reportarlo al gerente de riesgos, según el formato que se defina para tal fin. Él sería el responsable de mantener actualizados los registros relativos a los reportes y evaluaría la necesidad de efectuar actualizaciones y/o modificaciones a los procedimientos y planes de acción relativos al SARLA/FT.

9.1. **Monitorear, medir y revisar un evento de riesgo de LA/FT**

Los objetivos de esta etapa son:

Medir el desempeño del proceso SARLA/FT para verificar el cumplimiento de las políticas y los objetivos del SARLA/FT, y reportar los resultados a la gerencia para su revisión.

Producir resultados de los análisis de los reportes, que servirán como el *input* para el programa de mejoramiento.

Calcular indicadores de gestión del riesgo.

Lograr una efectiva implementación de planes de mejoramiento continuo del SARLA/FT, que incluye la aplicación de procedimientos para ejercer acciones correctivas y preventivas, basados en los resultados de las revisiones gerenciales.

9.2. **Metodología de monitoreo de un evento de riesgo de LA/FT**

9.2.1. *Indicador de gestión (eficacia) del SIPLA/FT o del SARLA/FT: la propensión marginal de la empresa al riesgo de LA/FT*

La Circular Externa 061 de 2007, emanada de la Superfinanciera, en su numeral 3 define como “riesgo de LA/FT la posibilidad de pérdida o daño que puede sufrir una entidad vigilada por su *propensión* 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 terroristas o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades”.

Con la finalidad de proporcionar claridad sobre el significado y usos que se le pueden dar al concepto “propensión” en el contexto de la gestión del riesgo de lavado de activos y financiación del terrorismo, tomaremos las siguientes ideas expresadas en la disciplina de la economía⁽²⁾:

“Propensión” es un concepto de amplio uso entre los economistas, cuando se refieren por ejemplo a *la propensión al consumo, propensión al ahorro, propensión a la inversión*, etc. En estos casos, el concepto es un indicador del comportamiento de los consumidores o del sistema económico nacional con respecto a la *proporción* de los ingresos que se destinan al consumo, al ahorro o a la inversión.

Este concepto tiene una implicación dinámica, porque un consumidor, de acuerdo a sus expectativas y capacidad económica personales y a los comportamientos de la economía, puede variar en el tiempo la cantidad de su ingreso que destina al consumo, al ahorro o a la inversión. Y

-
- (2) *Propensión marginal al consumo*: “Expresión utilizada en macroeconomía, a nivel de los agregados económicos y monetarios. Relación entre los aumentos en el consumo y los aumentos en el ingreso. Se define como el aumento en el consumo inducido por un aumento de un peso en el ingreso. Si el ingreso de las personas aumenta en un peso, y su consumo se incrementa en 0,7 pesos, entonces su propensión marginal al consumo es 0,7. La propensión al consumo puede fluctuar entre cero y uno. A medida que el nivel de ingreso de las personas aumenta, su propensión marginal al consumo es menor. Es así que una persona que tiene un nivel de ingreso de subsistencia destinará al consumo la totalidad de cualquier aumento marginal de su ingreso. En cambio, las personas de ingresos altos pueden destinar al ahorro parte de sus aumentos de ingresos, con lo que su propensión al consumo será más baja. A su vez, la propensión al ahorro de las personas de altos ingresos será más alta que la propensión al ahorro de las personas de bajos ingresos, por cuanto esta última es el anverso de la propensión al consumo. Las propensiones al consumo o al ahorro se pueden definir para un agente económico individual, como para la economía en su conjunto. En su dimensión macroeconómica, se pueden definir las propensiones marginales al consumo, al ahorro, a invertir, a importar y a exportar. La suma de las propensiones debe ser igual a 1, pero cada una de ellas debe ser menor que 1 y mayor que cero, por cuanto los aumentos en el Ingreso Nacional se destinan a consumos, ahorro, inversiones, importaciones y exportaciones. De esta forma las propensiones marginales se definen como los aumentos que se producen en las variables mencionadas, a consecuencia de cambios unitarios (marginales) en el ingreso nacional”. Tomado de: *Diccionario de economía, administración, finanzas, marketing*, Disponible en Web: <http://www.eco-finanzas.com/diccionario/P/PROPENSION_MARGINAL_AL_CONSUMO.htm>.

puesto que puede variar en el tiempo es medida en términos de una proporción o porcentaje.

Es decir, que la propensión o proporción se refiere a variables cuantificables, por tanto, puede ser analizada mediante técnicas estadísticas.

Con base en lo anterior y para propósitos de implementación del SARLA/FT o del SIPLA/FT, bien en una empresa del sector financiero o del sector real, precisaremos el alcance del concepto *propensión* al riesgo.

9.2.2. *Variables de la propensión al riesgo de LA/FT*

El riesgo de LA/FT surge cuando una empresa realiza sus actividades de servucción o producción y de comercialización de los servicios o productos resultantes. Como ya lo expusimos anteriormente, en el contexto de la normatividad internacional y colombiana sobre prevención y control del riesgo de LA/FT y en el proceso de servucción de empresas del sector financiero, podemos identificar las siguientes variables:

- Cantidad de operaciones inusuales (OI) identificadas con respecto a la cantidad de operación realizadas en el mes.
- Cantidad de operaciones sospechosas (OS) detectadas con respecto a la cantidad de operación realizadas en el mes.
- Cantidad de operaciones normales (ON) realizadas.
- Cantidad de operaciones totales (OT) realizadas.
- Cantidad de operaciones individuales, o sea las realizadas por un solo cliente a quien corresponde, por ejemplo, un solo número de documento de identidad, una sola dirección y un solo teléfono.
- Cantidad de operaciones múltiples (OM) son las realizadas por un grupo de clientes quienes se identifican con números de documento de identidad diferentes pero que reportan, por ejemplo, igual número te-

lefónico, igual número de cuenta corriente o de ahorros en la misma entidad financiera, igual número telefónico e incluso igual dirección residencial.

Anteriormente, también expusimos las relaciones existentes entre ellas.

9.2.3. ***Definición de propensión marginal al riesgo de LA/FT (PMRLA/FT)***

El ente que está expuesto al riesgo de LA/FT es la empresa, por tanto, podremos hablar de propensión marginal de la empresa a ser utilizada para que, a través de ella, se cometa el riesgo de LA/FT.

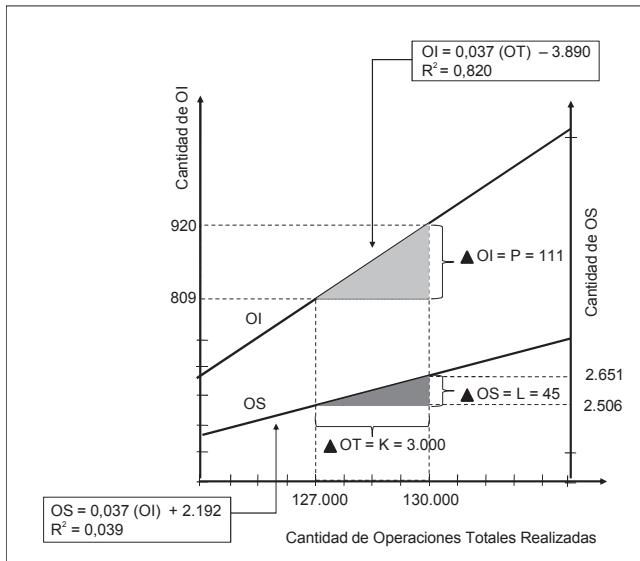
Aclarado el concepto de *propensión*, debemos aclarar el concepto *marginal*. Este último se refiere a los incrementos que se dan en una variable dependiente, cuando se generan incrementos en una variable independiente.

Teniendo en cuenta las variables de la propensión al riesgo de LA/FT y el concepto de *marginalidad*, expuestos anteriormente, definimos que “propensión marginal al riesgo de LA/FT” (PMRLA/FT) es un indicador del grado de exposición de la empresa al riesgo de LA/FT.

Las variaciones o cambios de la propensión al riesgo de LA/FT se pueden comprender mejor mediante el concepto de propensión marginal al riesgo de LA/FT. Puesto que en el proceso de gestión del riesgo de LA/FT generamos OI y OS, entonces podemos hablar de propensión marginal al riesgo de LA/FT por OI y propensión marginal al riesgo de LA/FT por OS.

En la operación de una empresa, seguramente, si la cantidad de OT se incrementa, también se incrementará la cantidad de OI y de igual manera las OS. El siguiente ejemplo numérico y su correspondiente gráfico ayudarán a comprender mejor el concepto de propensión marginal al riesgo de LA/FT.

Gráfico 30
Propensión marginal al riesgo de LA/FT (PMRLA/FT)



Un incremento K de 4.400 en la cantidad de OT realizadas generará un incremento P de 153 en la cantidad de OI identificadas, de las cuales la cantidad L = 45 corresponde al incremento de OS detectadas.

9.2.4. *Cálculo del indicador de la propensión marginal al riesgo de LA/FT*

La PMRLA/FT se puede calcular como el valor cociente resultante entre los incrementos (\blacktriangle) que se producen en la cantidad de OS cuando se incrementa la cantidad de OT, o entre las OI y las OT, e inclusive entre las OS y las OI, como se indica a continuación:

$$\text{PMRLA/FT}_{\text{OS}} = \blacktriangle \text{ OS detectadas} / \blacktriangle \text{ OT realizadas}$$

$$\text{PMRLA/FT}_{\text{OI}} = \blacktriangle \text{ OI identificadas} / \blacktriangle \text{ OT realizadas}$$

Pero, también podríamos calcular:

$$\text{PMRLA/FT}_{\text{Global}} = \blacktriangle \text{ OS detectadas} / \blacktriangle \text{ OI identificadas}$$

9.2.5. *Medidas del indicador de la PMRLA/FT*

Cuando tomamos los valores absolutos, el indicador resultante se puede expresar en unidades de operación o, de manera porcentual, como se ilustra a continuación:

$$\text{PMRLA/FT} = [k] \text{ Valor absoluto en unidades}$$

$$\text{PMRLA/FT} = k \% \text{ Valor relativo}$$

9.2.6. *Técnicas estadísticas para medir el indicador de la PMRLA/FT*

De conformidad con las técnicas estadísticas, la medida del indicador de la PMRLA/FT equivale al coeficiente de la variable independiente en una función de regresión entre las variables independiente y dependiente de ella.

Por ejemplo, si la función fuera lineal como la siguiente: $Y = a + bX$, el parámetro “b” sería el indicador, que también es equivalente al valor de la primera derivada de la función e indica el grado de la pendiente que adopta la línea recta.

Este método permite hacer estimaciones del incremento en el valor “Y” cuando se hacen incrementos en el valor “X”.

En esta función las variables “X” y “Y” podrían ser cambiadas de la siguiente manera: “X = OT” y “Y = OS”, o “Y = OI”.

Por tanto, la función quedaría como la cantidad de operaciones inusuales (OI) igual a “f” (cantidad de operaciones totales, OT):

$$OI = f(OT)$$

Lo que se puede definir mediante la técnica de la regresión y correlación entre variables.

9.2.7. *Interpretación del indicador de la PMRLA/FT*

Bien por su valor absoluto o por su valor relativo, puede ser utilizado como un indicador del grado de exposición de la empresa al RLA/FT.

Si se consideran las variaciones del indicador entre uno y otro período, puede ser interpretado como una medida de la eficacia de las políticas y procedimientos que utiliza la empresa para identificar OI y detectar OS y, por tanto, para prevenir y controlar el RLA/FT.

9.2.8. *Ejemplo de propensión marginal al riesgo de LA/FT*

Para explicar los anteriores conceptos, hemos tomado de la operación de una empresa y de la gestión del oficial de cumplimiento los siguientes valores de OT, OI y OS que se presentan a continuación:

Tabla 27

Ejemplo de propensión marginal al riesgo de LA/FT

Período	Operaciones totales realizadas (OT)		
	Cantidad OT	Incremento	Inc. %
Jul-08	116.543		
Ago-08	123.218	6.675	5,73%
Sep-08	138.818	15.600	12,66%
Oct-08	116.724	-22.094	15,92%
Período	Operaciones inusuales (OI)		
	Cantidad OI	Incremento	Inc. %
Jul-08	635		
Ago-08	485	-150,00	-23,62%
Sep-08	1.430	945,00	194,85%
Oct-08	580	-850,00	-59,44%
Período	Operaciones sospechosas (OS)		
	Cantidad OS	Incremento	Inc. %
Jul-08	1.425		
Ago-08	3.121	1.696,00	119,02%
Sep-08	2.825	-296,00	-9,48%
Oct-08	2.457	-368,00	-13,03%

En esta tabla, obsérvese que para cualquier período la cantidad de OS es superior a la cantidad de OI, lo cual no tendría una explicación estadística, pero sí a la luz de las políticas de detección de OS de la empresa que establecen que los clientes identificados como integrantes de operaciones múltiples (OM) correspondientes al período deben ser rastreados en la base de datos para los períodos anteriores; en ese proceso, se pueden encontrar, como efectivamente sucede en este caso, otros clientes que no realizaron operaciones en el período pero sí en los anteriores y que además tienen en común con los clientes del período, por ejemplo, el número telefónico, el remitente de giro, la dirección, etc.

9.2.9. *Ejemplo de propensión marginal de una empresa al RLA/FT por operaciones inusuales (PMRLA/FT-OI)*

Utilizando la técnica de la regresión y correlación, hemos establecido que la función de regresión que minimiza la sumatoria de las diferencias entre cada valor de la variable y su promedio respectivo es la siguiente:

$$OI = 0,037(OT) - 3890$$

$$R^2 = 0,820$$

En ella se expresa que la:

$$PMRLA/FT_{OI} = \Delta OI \text{ identificadas} / \Delta OT \text{ realizadas} = 0,037$$

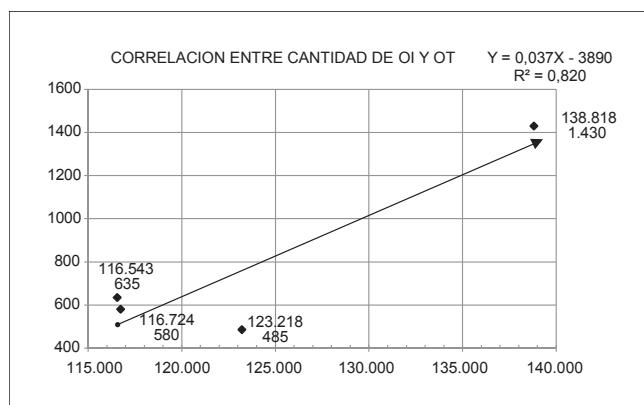
Indica que, cada vez que las OT se incrementan, por ejemplo en una (1) unidad, las OI se incrementarían en 0,037 unidades (valor absoluto), o que cada vez que las OT se incrementen en 100 unidades, las OI se incrementarán en aproximadamente 4 operaciones inusuales (indicador de valores absolutos). Si lo consideramos como valor relativo, tendremos que decir que si las OT se incrementan en un 100% las OI se incrementan en el 3,7%.

El coeficiente de correlación (R^2) indica que la función lineal estimada es capaz de minimizar en un 82% la sumatoria de las diferencias entre los valores de cada variable y su promedio correspondiente, lo cual le otor-

ga alta confiabilidad a los datos y a los análisis realizados.

9.2.10. *Ejemplos de propensión marginal de una empresa al riesgo de LA/FT por operaciones inusuales y por operaciones sospechosas*

Gráfico 31
Ejemplo 1: PMRLA/FT por operaciones inusuales en LA/FT



Procediendo de igual manera que para el caso anterior, la función lineal que se obtuvo indica que PMRLA/FT – OS/OI es de 0,338 y que su coeficiente de correlación es bastante bajo, lo que equivale a decir que no hay una estrecha correlación entre las variables:

$$OS = 0,338 (OI) + 2192$$

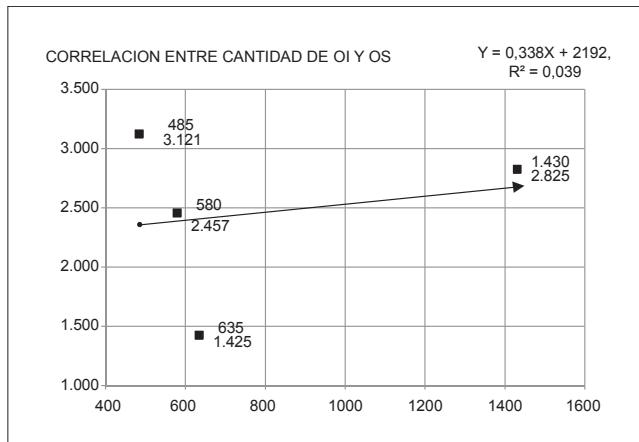
$$R^2 = 0,039$$

Por tanto, los análisis que se elaboren utilizando esa relación funcional no tienen validez estadística porque su coeficiente de correlación es muy bajo.

La carencia de correlación se debe a que los criterios, políticas y procedimientos que se utilizan para identificar las OI y las OS son fundamentalmente diferentes, aun cuando tienen el mismo objetivo de prevención y control del riesgo.

Gráfico 32

Ejemplo 2: PMRLA/FT por operaciones sospechosas en LA/FT



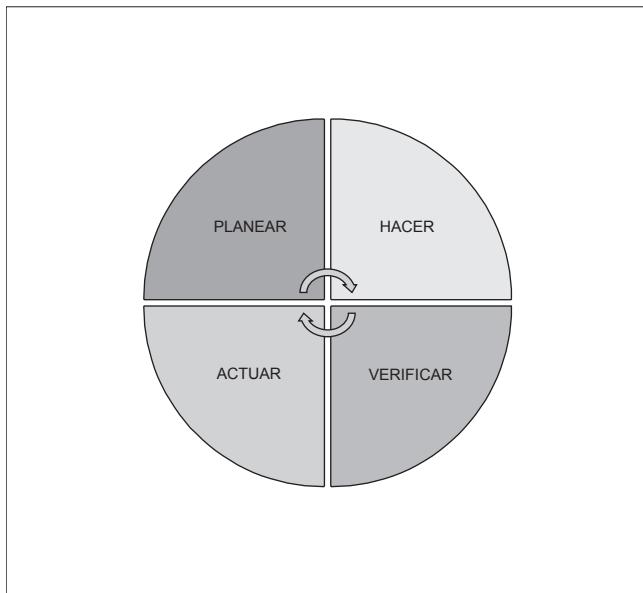
10. IMPLEMENTACIÓN DEL SARLA/FT (EL CICLO PHVA)

Dentro de este enfoque, la implantación del SARLA/FT o del SIPLA/FT en todos los procesos de la organización se realiza incrementalmente mediante el *ciclo planear-hacer-verificar-actuar* (en adelante PHVA).

Dentro del contexto del SARLA/FT o del SIPLA/FT, el PHVA es un ciclo dinámico que puede desarrollarse dentro de cada proceso de la empresa y en el sistema de procesos como un todo. Está íntimamente asociado con la planificación (planear), la implementación (hacer), el control (verificar) y la mejora continua (actuar) de los procesos de direccionamiento estratégico, de realización y de apoyo requeridos para la prestación de los servicios y productos ofrecidos por la organización.

La administración de riesgos hace parte de la estructura del ciclo PHVA de cada proceso.

Gráfico 33
Ciclo PHVA



Planear (P): fase en la cual se identifican, documentan y evalúan las unidades operativas (producto/servicio dirigidos a un segmento de mercado) expuestas al riesgo de LA/FT (evento de riesgo de LA/FT) y se listan los controles necesarios para reducir el riesgo a niveles aceptables (riesgo residual).

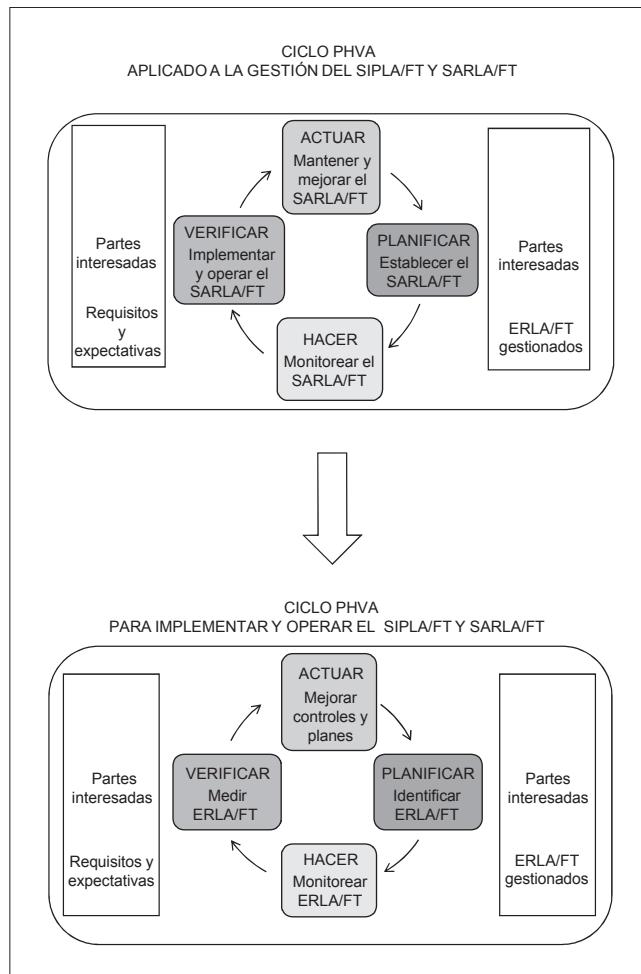
Hacer (H): fase en que se aplican las metodologías desarrolladas para identificar y evaluar los eventos de riesgo de LA/FT y se colocan en operación o implantan los controles y tratamientos, como parte de los procedimientos del proceso.

Verificar (V): en esta fase se utilizan métricas para establecer la efectividad real que tienen los controles establecidos para prevenir y controlar los eventos de riesgo de LA/FT.

Actuar (A): fase en la cual se definen e implantan acciones de mejoramiento continuo de los controles y procedimientos de administración de los eventos de riesgo de LA/FT.

El mantenimiento y la mejora continua de la capacidad del SARLA/FT o del SIPLA/FT pueden lograrse aplicando el concepto de PHVA en todos los niveles dentro de la organización, como se ilustra y se describe a continuación.

Gráfico 34
Ciclo PHVA en gestión del SIPLA/FT y del SARLA/FT



10.1. Fase Planear (establecer el SARLA/FT)

En esta fase se deben establecer las políticas, objetivos, metas y procedimientos relevantes para gestionar los riesgos, mejorar la seguridad de los procesos y entregar resultados alineados con las políticas y objetivos estratégicos de la empresa.

Las actividades que comprende son:

Definir el contexto de operación del SARLA/FT o del SIPLA/FT en la organización.

Definir las políticas y objetivos del SARLA/FT o del SIPLA/FT, en términos de las características del negocio o sus servicios, la organización, su localización, activos y tecnología para reducir los eventos de riesgo de LA/FT presentes en la unidades operativas (UO) a niveles aceptables.

Describir el riesgo de LA/FT al que está expuesta la empresa y la normatividad nacional e internacional sobre el tema.

Analizar las definiciones normativas de la SFC y elaborar marco conceptual del SARLA/FT o SIPLA/FT propio para la empresa, es decir, elaborar definiciones aplicadas a la organización.

Analizar los componentes normativos del SARLA/FT o del SIPLA/FT y elaborar conceptos y metodologías propias, definiendo el SARLA/FT o el SIPLA/FT como un proceso.

Definir conceptos propios para la administración del riesgo de LA/FT, evento de riesgo de LA/FT, segmentos de factores de riesgo de LA/FT, unidad operativa (UO), perfil de una evento de riesgo de LA/FT, perfil de un segmento de factores de riesgo.

Diseñar una metodología de segmentación para los factores de riesgo que permita identificar evento de riesgo de LA/FT en una UO (utilizando por ejemplo el método de la “espina de pescado”), medir y valorar los eventos de riesgo de LA/FT encontrados en una unidad estratégica, proponer controles a cada evento de riesgo de LA/FT dentro de las unidades estratégicas utilizando por ejemplo la metodología de los “cinco por qué”

y, finalmente monitorear cada evento de riesgo de LA/FT presente en las unidades estratégicas.

Definir mecanismos para evaluar y medir el desempeño del proceso SARLA/FT o SIPLA/FT con relación a las políticas de prevención y control del riesgo de LA/FT, los objetivos y la experiencia práctica.

Diseñar metodologías para resolver la relación causa-efecto presente en un evento de riesgo a fin de identificar un evento de riesgo de LA/FT, medirlo y controlarlo.

Identificar: hallar, describir y ubicar un evento de riesgo de LA/FT.

Identificar el método de medición o valoración de riesgos que sea apropiado para el SARLA/FT y a los requerimientos legales, regulatorios identificados para la empresa y sus servicios.

Describir las situaciones de riesgo a que están expuestos los productos del portafolio de la empresa en términos de las características del negocio o sus servicios, la organización, su localización, activos y tecnología.

Caracterizar el SARLA/FT o el SIPLA/FT como un sistema que tiene procesos proveedores, entradas, actividades de transformación, salidas y procesos clientes.

Determinar los criterios de aceptación del riesgo e identificar los niveles aceptables de riesgos.

Definir la estructura organizacional, funciones y responsabilidades para el SARLA/FT o el SIPLA/FT.

Definir el plan de gestión del riesgo, en cuanto a procedimientos de control interno y revisión del SARLA/FT o del SIPLA/FT, el cual establece cómo se conducirá la gestión del riesgo en todas las actividades y procesos de la organización, de tal manera que resulte pertinente, efectiva y sostenible.

Elaborar los procedimientos para divulgación de información en cuanto a reportes externos e internos.

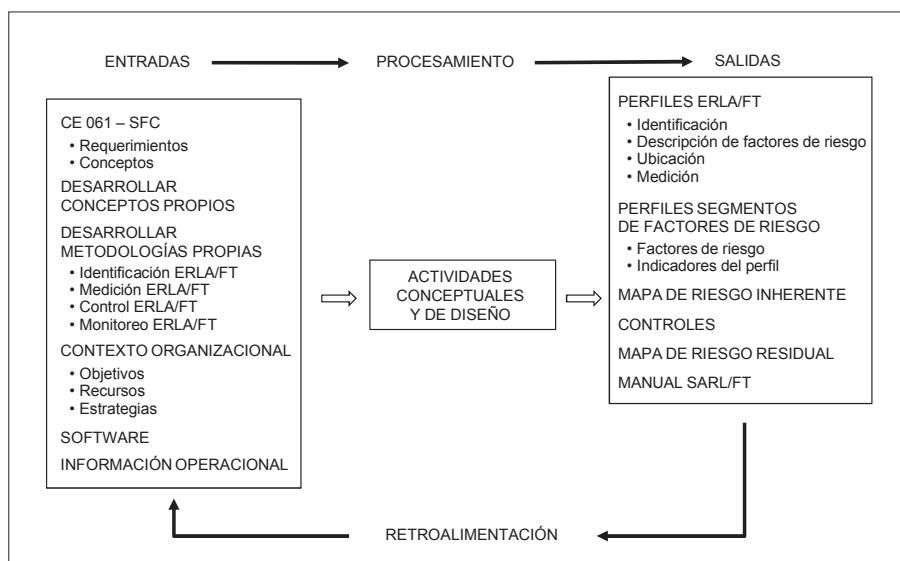
Describir la infraestructura tecnológica y el procedimiento de consolidación electrónica de operaciones.

Definir los procedimientos para documentación del SARLA/FT o del SIPLA/FT.

Esta fase también se puede expresar como un sistema, tal como se ilustra en el grafico siguiente:

Gráfico 35

Proceso para implantación de la fase *Planear* del SARLA/FT



10.2. Fase Hacer (implementar y operar el SARLA/FT)

Esta fase se refiere a la aplicación de las metodologías desarrolladas para identificar y evaluar los eventos de riesgo de LA/FT, además de implementar y operar las políticas, controles, procesos y procedimientos.

Comprende las siguientes actividades:

Elaborar cronograma de implementación del plan de gestión del riesgo.

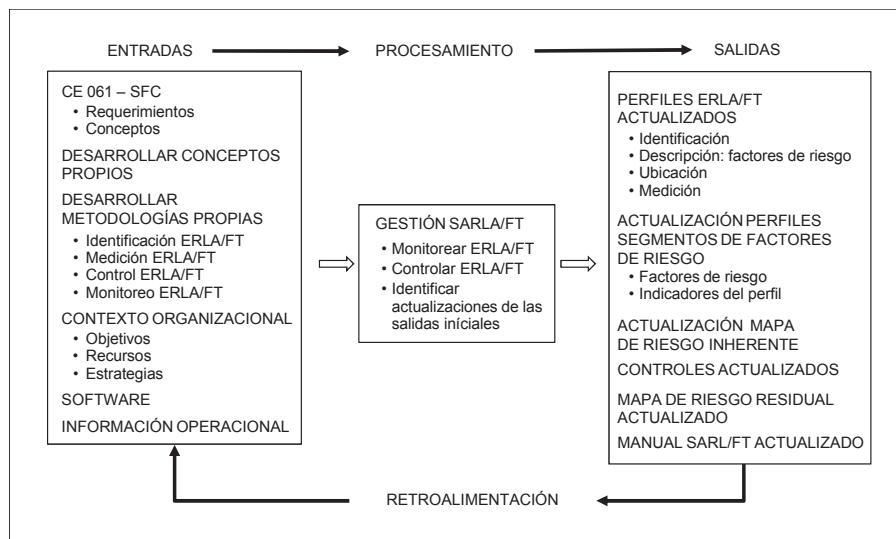
Iniciar la implementación del plan de gestión del riesgo.

Diseñar e implementar indicadores de gestión de riesgos.

Así como la fase anterior, esta también se puede representar mediante otro proceso:

Gráfico 36

Proceso para implantación de la fase hacer del SARLA/FT



10.3. Fase Verificar (monitorear, medir y revisar el SARLA/FT)

Esta fase consiste en diseñar procedimientos para evaluar y, en los casos donde se pueda aplicar, medir el desempeño del proceso SARLA/FT contra las políticas del riesgo de LA/FT, los objetivos y la experiencia práctica. Los resultados se deben reportar a la gerencia para su revisión.

Esos resultados, producto de los análisis de los reportes, servirán como el *input* para el programa de mejoramiento.

Algunos de los aspectos que se deben monitorear, medir y analizar durante esta fase son:

- a) Los niveles de control logrados (en comparación con los propuestos).
- b) El cumplimiento legal.
- c) El reporte de operaciones: inusuales, múltiples y sospechosas.
- d) La utilización de recursos.
- e) Las tendencias.
- f) Las no conformidades de los procesos (incumplimiento de requisitos de partes interesadas).
- g) Los resultados de las revisiones.

Igualmente en esta etapa, se deben definir procedimientos para el uso y análisis de reportes que deberán producirse, para que la gerencia tome decisiones y mida el desempeño de la seguridad basado en niveles de servicio y que, a la vez, sean entregables. Esto con el fin de aplicar regularmente guías de monitoreo, evaluar los resultados de las guías y presentar dichos resultados a la dirección.

10.4. Fase Actuar (mantener y mejorar continuamente el SARLA/FT o el SIPLA/FT)

En esta fase se definen los procedimientos para ejercer las acciones correctivas y preventivas, basados en los resultados de las revisiones gerenciales, para lograr el mejoramiento continuo. Para lo cual comprende las siguientes actividades:

Monitorear y evaluar la efectividad de los procesos del SARLA/FT o del SIPLA/FT.

Formular (periódicamente) los nuevos planes de mejoramiento del SARLA/FT o del SIPLA/FT y satisfacer los requerimientos del negocio desde la perspectiva de los clientes y la línea base de control establecida.

Planear e implementar nuevos procedimientos y cambios en los establecidos.

El contenido y desarrollo de este aparte del libro ha sido elaborado tomando como base la Norma NTC 5254: 2006 de Gestión del Riesgo y los conceptos y ordenación del ciclo PHVA aplicado a la gestión por procesos. Esta norma fue emitida por el INCONTEC (Instituto Colombiano de Normas Técnicas).

11. SENCILLO APLICATIVO PARA GESTIONAR EL SIPLA/FT O EL SARLA/FT

Le recordamos que la información que produce la gestión del SIPLA/FT tiene que ver con la identificación, control y monitoreo de eventos de riesgo de LA/FT, mientras que en el SARLA/FT se incluye la etapa de medición de cada uno.

No dude de que en cualquiera de los dos casos la cantidad de información que debe manejar para tomar decisiones es bastante grande, por tanto se requiere de algún tipo de aplicativo de sistemas que le ayude.

Toda la información, inclusive la propuesta por nosotros cuando se utilice nuestras metodologías, podría ser incluida en una base de datos, como por ejemplo una sencilla hoja de Excel, en la cual cada columna corresponde a un tipo de información según la etapa y cada fila corresponderá a los datos de cada uno de los eventos de riesgo de LA/FT que se estén considerando.

En el caso de información relacionada con el riesgo inherente, el diseño de encabezados para las columnas en la hoja de Excel podría ser como el que se indica:

Columnas Excel para registro de identificación y medición de eventos de riesgo de LA/FT

Identificación			Medición								
ER LA/FT			Frecuencia del riesgo inherente			Impacto del riesgo inherente				Severidad	
NOMBRE	CÓDIGO	Factor Determinante del riesgo	Eventos posibles = operaciones totales realizadas en el periodo			Valores de impacto por riesgos asociados					
Probabilidad						Riesgo legal	Riesgo reputacional	Riesgo de contagio	Riesgo		
Cantidad de eventos ocurridos	Valor de la probabilidad	Descripción de la probabilidad	Escala de la probabilidad			%	%	%	%		
										Impacto total riesgos asociados	
										Escala	Calificación

De igual forma, se podría proceder con la información que solo produce la etapa de control. Su resultado podría ser como el siguiente:

Columnas Excel para registro de medición de eventos de riesgo de LA/FT

Cod.	Medición del riesgo residual										
	Probabilidad residual				Impacto por riesgos asociados residuales					Severidad del evento de riesgo de LA/FT	
	Riesgo legal 1	Riesgo reputacional	Riesgo de contagio	Riesgo operacional	Impacto total riesgo						
	Cantidad eventos ocurridos	Valor probabilidad	Valor descriptivo de la probabilidad	Descripción de la probabilidad	0%	0%	0%	0%	0%	Escala	Calificación

Columnas Excel para registro de control de eventos de riesgo de LA/FT

Control del riesgo inherente				
Causas del evento de riesgo de LA/FT		Control y tratamiento		
Nombre del evento de riesgo de LA/FT	Código	Causa primaria	Causa última	

Establecer controles modificará el valor de la frecuencia e impacto del evento de riesgo de LA/FT y, por tanto, su severidad.

Adjunto al libro encontrará un CD-Rom con un archivo denominado “Cd aplicativo Excel para SIPLA/FT y SARLA/FT”, en el cual se utiliza la información de los 19 eventos de riesgo de LA/FT considerados en el libro.

El archivo contiene 4 hojas visibles protegidas cada una con la clave *cumplimiento* y con *las celdas bloqueadas*, a excepción de las que están resaltadas en color gris oscuro, las cuales usted puede cambiar para hacer sus ejercicios.

El contenido de cada hoja es el siguiente:

—*Hoja 1 (escalas de medición)*

Esta hoja no tiene ningún tipo de formulación en las celdas.

1. Contiene las escalas y calificaciones para medir:
 - a) La frecuencia con que se presenta cada evento de riesgo de LA/FT;
 - b) El impacto y las ponderaciones tenidas en cuenta para los riesgos asociados con cada evento de riesgo de LA/FT. Observe que sus calificaciones siempre están precedidas de un número en una escala de 1 a 5 que es igual al grado asignado a cada calificación. Si usted decide cambiarlas, le solicitamos asignar al principio de la calificación (descriptiva) el número de grado correspondiente, de otra forma el aplicativo no funcionará, y
 - c) El impacto consolidado correspondiente a los riesgos asociados.
2. Estas escalas y calificaciones son aplicadas en el ejercicio para realizar la etapa de medición de cada uno de los 19 eventos de riesgo de LA/FT considerados. Estas pueden ser cambiadas según sus preferencias.
3. Le recordamos que las actividades de control tienen por objetivo disminuir la frecuencia y/o el impacto del evento de riesgo de LA/FT, por tanto siempre se reflejarán en la frecuencia y/o en el impacto que se les haya asignado inicialmente a cada evento de riesgo de LA/FT.
4. Las mediciones de frecuencia e impacto después de aplicar los controles generan el mapa de riesgo residual.

—Hoja 2 (medición riesgo inherente)

1. Las columnas “B”, “C” y “D” contienen la información que permite identificar cada evento de riesgo de LA/FT.

B - Nombre del evento de riesgo de LA/FT	C - Código del evento de riesgo de LA/FT	D - Factor determinante del riesgo
--	--	------------------------------------

2. Para identificar el evento de riesgo de LA/FT, hemos utilizado nuestra metodología de la “espina de pescado”.

3. Las columnas “F”, “G”, “H”, “I” contienen la información que permite ingresar manualmente la información necesaria para *medir la frecuencia*:

Eventos posibles = Operaciones totales realizadas en el periodo		497.820	
Probabilidad inherente			
E - Número de eventos riesgo inherente ocurridos	F - Valor de la probabilidad riesgo inherente	G - Escala de la probabilidad	H - Calificación de la probabilidad riesgo inherente

4. Para que practique, solo podrá introducir información en la columna “E” y en la celda que indica la cantidad de eventos posibles; el aplicativo calculará y expresará automáticamente los valores de las columnas “F”, “G” y “H”.

5. Las columnas “K”, “L”, “M” y “N”, contienen la información que permite medir el *impacto*. Ud. podrá variar manualmente los porcentajes ponderados de impacto asignados a cada riesgo asociado con el evento de riesgo de LA/FT y la descripción de la calificación, que como ya dijimos debe estar precedida de un número; las columnas “O” y “P” serán calculadas automáticamente por el aplicativo.

Impacto del riesgo inherente					
Valores de impacto por riesgos asociados para el riesgo inherente				Impacto total riesgos inherentes asociados	
K - Riesgo legal inherente	L - Riesgo reputacional inherente	M - Riesgo de contagio inherente	N - Riesgo operacional inherente	O - Escala	P - Calificación
30%	40%	10%	20%		100%

6. En las columnas “R” y “S” se calculará automáticamente el valor de la escala y la calificación de la severidad que adopta cada evento de riesgo de LA/FT según la frecuencia e impacto consolidado, también se asignará automáticamente el color que identifica la severidad del evento de riesgo de LA/FT.

Severidad del riesgo inherente	
R - Escala	S - Calificación

—Hoja 3 (controles al riesgo inherente)

Control al riesgo inherente				
Identificación		Causas del evento de riesgo de LA/FT		F - Control y tratamiento
B - Nombre del evento de riesgo de LA/FT	C - Código	D - Causa primaria	E - Causa última	

Para cada uno de los 19 eventos de riesgo de LA/FT, hemos continuado aplicando nuestra metodología de la “espina de pescado”, y se han incluido en esta hoja algunos ejemplos que lo podrían orientar cuando esté diseñando controles para los eventos de riesgo de LA/FT de su empresa.

—Hoja 4 (mapa de riesgos)

En esta hoja encontrará en las columnas “A”, “B”, “C”, “D”, “E”, “F”, “G” y “H” la información consolidada que permite identificar cada evento de riesgo de LA/FT y los resultados que arroja automáticamente el aplicativo para la escala y calificación del impacto, de la probabilidad y de la severidad, inclusive con colores que permitirán producir el mapa de riesgos inherentes.

A - código	B - Descripción evento de riesgo de la/ft	Impacto		Probabilidad		Severidad	
		C - Escala	D - Calificación	E - Escala	F - Calificación	G - Escala	H - Calificación

En la misma hoja se producirá automáticamente el mapa de eventos de riesgo de LA/FT.

12. DOCUMENTACIÓN

Hacen parte de la documentación del SARLA/FT, el *manual*, el cual incluye tanto las políticas y procesos como los procedimientos, el código de ética y conducta y demás anexos, e instructivos, además de la información generada en el sistema de administración del riesgo LA/ FT, los requerimientos y respuestas dadas a las entidades competentes relacionadas con esta materia.

12.1. Criterios y procesos de manejo

La información y documentación de carácter física relacionada con el SARLA/FT, dependerá del área responsable del manejo y control de archivos, la cual debe disponer de lo necesario para el cumplimiento de esta disposición en cuanto la documentación sea entregada para archivo central.

Antes de que la documentación sea entregada al archivo central, cada responsable, el oficial de cumplimiento y el área al cual pertenezca y los órganos de control podrán tener la documentación por lo menos un año en sus respectivos puestos de trabajo, tanto en su forma física como electrónica.

La documentación relacionada con el SARLA/FT debería ser guardada y utilizada al interior de la empresa por el oficial de cumplimiento, el comité evaluador de operaciones o cualquiera de sus miembros con función para el manejo de la misma, los órganos de control y la junta directiva, siempre que se cumpla con la reserva legal respectiva.

Los requerimientos de entidades policivas deberían quedar en custodia del área de cumplimiento o en el área al que pertenezca el oficial de cumplimiento y podrán ser entregados al archivo central después del año calendario. Su archivo se debería efectuar en orden cronológico respecto de la fecha de recepción del requerimiento.

12.2. Guarda

Las áreas responsables, el oficial de cumplimiento, respecto de la documentación relacionada con el SARLA/FT, deben guardar la misma así:

- Para el archivo físico como mínimo un año calendario en los puestos de trabajo de cada responsable.
- Para los archivos electrónicos se debería dejar constancia mediante *backup*, en CD-Rom, DVD, discos duros, cintas de seguridad o cualquier medio electrónico conforme las definiciones utilizadas en el presente manual.
- Una vez cada responsable entregue la documentación al área administrativa encargada del archivo, dicha documentación debería reposar en el archivo central de la empresa en por el término de conservación de la misma exigido por la norma legal.

12.3. Conservación

Las áreas responsables, el oficial de cumplimiento, respecto de la documentación relacionada con el SARLA/FT, deben dar estricto cumplimiento a las normas establecidas en cuanto a reportes internos y externos y observar en todo momento las Tablas de Retención documental establecidas las cuales deberían considerar los períodos indicados por la Ley de tal forma que se garantice la conservación de documentos de forma segura.

ANEXOS

1. Calificación de la severidad de un evento de riesgo de LA/FT
2. Mapa de eventos de riesgo de LA/FT inherentes
3. Ejemplo de medición del impacto para el riesgo residual
4. Mapa de eventos de riesgo de LA/FT residual
5. Ejemplo de causas y controles para cinco eventos de riesgo de LA/FT
6. Indicadores de efectividad de los controles
7. Señales de alerta que se pueden percibir en la operación comercial o financiera de una empresa del sector real

Anexo 1

Calificación de la severidad de un evento de riesgo de LA/FT

Calificación de la probabilidad	Calificación del impacto	Indicador del nivel de severidad	Calificación del evento de riesgo de LA/FT según nivel de severidad	Acción a emprender
1	1	1	Evento de riesgo de LA/FT <i>aceptable</i>	Nivel de severidad de 1 a 5: el evento de riesgo de LA/FT es <i>aceptable</i> , porque es probable que no se requiera reducción del riesgo ya que su probabilidad de ocurrencia e impacto son relativamente bajos y su tratamiento podría requerir recursos más costosos que el valor del impacto.
2	1	2	Evento de riesgo de LA/FT <i>aceptable</i>	Realiza seguimiento periódico analizando la ocurrencia de los eventos. Revisa o define método de control.
1	2	2	Evento de riesgo de LA/FT <i>aceptable</i>	
3	1	3	Evento de riesgo de LA/FT <i>aceptable</i>	
1	3	3	Evento de riesgo de LA/FT <i>aceptable</i>	
4	1	4	Evento de riesgo de LA/FT <i>aceptable</i>	Se maneja mediante procedimientos de rutina.
2	2	4	Evento de riesgo de LA/FT <i>aceptable</i>	
1	4	4	Evento de riesgo de LA/FT <i>aceptable</i>	
5	1	5	Evento de riesgo de LA/FT <i>aceptable</i>	
1	5	5	Evento de riesgo de LA/FT <i>aceptable</i>	
3	2	6	Evento de riesgo de LA/FT <i>significativo</i>	Nivel de severidad de 6 a 9: el evento de riesgo de LA/FT es <i>significativo</i> , se requiere reducción del riesgo ya que su probabilidad de ocurrencia e impacto son relativamente altos, su tratamiento podría requerir recursos menos costosos que el valor del impacto. Se debe especificar la responsabilidad de gestión.
2	3	6	Evento de riesgo de LA/FT <i>significativo</i>	
4	2	8	Evento de riesgo de LA/FT <i>significativo</i>	
2	4	8	Evento de riesgo de LA/FT <i>significativo</i>	
3	3	9	Evento de riesgo de LA/FT <i>significativo</i>	

Calificación de la probabilidad	Calificación del impacto	Indicador del nivel de severidad	Calificación del evento de riesgo de LA/FT según nivel de severidad	Acción a emprender
5	2	10	Evento de riesgo de LA/FT <i>moderado</i>	Nivel de severidad de 10 a 12: el evento de riesgo de LA/FT es <i>moderado</i> , se requiere reducción del riesgo ya que su probabilidad de ocurrencia e impacto son relativamente altos; su tratamiento podría requerir recursos menos costosos que el valor del impacto. Se requiere una atención del personal superior
2	5	10	Evento de riesgo de LA/FT <i>moderado</i>	Determina la posibilidad de mitigar el impacto con las compañías de seguros u otro mecanismo, además plantear las acciones preventivas pertinentes en el formato de perfil de riesgo.
4	3	12	Evento de riesgo de LA/FT <i>moderado</i>	
3	4	12	Evento de riesgo de LA/FT <i>moderado</i>	
5	3	15	Evento de riesgo de LA/FT <i>catastrófico</i>	Nivel de severidad de 13 a 25: el evento de riesgo de LA/FT es <i>catastrófico</i> , se requiere <i>pronta y efectiva</i> reducción del riesgo ya que su probabilidad de ocurrencia e impacto son <i>muy altos</i> . Su tratamiento requiere de grandes costos y debe realizarse de manera inmediata; su impacto implica grandes pérdidas de dinero y hasta el cierre de la empresa. Se requiere una investigación detallada y una planificación a niveles superiores.
3	5	15	Evento de riesgo de LA/FT <i>catastrófico</i>	Realiza plan de contingencia y plantea acciones preventivas
4	4	16	Evento de riesgo de LA/FT <i>catastrófico</i>	
5	4	20	Evento de riesgo de LA/FT <i>catastrófico</i>	
4	5	20	Evento de riesgo de LA/FT <i>catastrófico</i>	
5	5	25	Evento de riesgo de LA/FT <i>catastrófico</i>	

Anexo 2

Mapa de eventos de riesgo de LA/FT inherentes

Evento de riesgo de LA/FT	Nombre	Ref.	Impacto	Probabilidad	Nivel de severidad	Puntaje riesgo
1	Realización de operaciones en las que se solicita frecuente cambio de titular, apoderado o beneficiario de un producto.	Evento de riesgo de LA/FT-14	Criticó = 4	Probable = 4	Catastrófico	16
2	Realización de operaciones en oficinas ubicadas en regiones de alto nivel de exposición al RLA/FT.	Evento de riesgo de LA/FT-16	Moderado = 3	Casi seguro = 5	Catastrófico	15
3	Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	Moderado = 3	Probable = 4	Moderado	12
4	Realización de operaciones con clientes que solicitan transferencias de propiedad a otras personas diferentes del titular o entrega de dinero a un tercero.	Evento de riesgo de LA/FT-05	Criticó = 4	Possible = 3	Moderado	12
5	Realización de operaciones con clientes/usuarios que suplantan al verdadero cliente o usuario.	Evento de riesgo de LA/FT-11	Criticó = 4	Possible = 3	Moderado	12
6	Realización de operaciones con clientes/usuarios que frecuentemente aparecen incluidos en operaciones inusuales, señales de alerta y/o múltiples con cualquiera de los productos de la empresa.	Evento de riesgo de LA/FT-09	Leve = 2	Casi seguro = 5	Moderado	10
7	Realización de operaciones con clientes/usuarios que no se identifican plenamente.	Evento de riesgo de LA/FT-10	Moderado = 3	Possible = 3	Significativo	9
8	Realización de operaciones con clientes/usuarios incluidos en operaciones sospechosas reportadas a la UIAF.	Evento de riesgo de LA/FT-07	Leve = 2	Probable = 2	Aceptable	4

Evento de riesgo de LA/FT	Nombre	Ref.	Impacto	Probabilidad	Nivel de severidad	Puntaje riesgo
9	Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	Insignificante = 1	Casi seguro = 5	Aceptable	5
10	Realización de operaciones en jurisdicciones catalogadas como de alto nivel de exposición al riesgo de LA/FT.	Evento de riesgo de LA/FT-13	Insignificante = 1	Casi seguro = 5	Aceptable	5
11	Realización de operaciones en oficinas que presentan un alto volumen de operaciones sospechosas.	Evento de riesgo de LA/FT-15	Insignificante = 1	Casi seguro = 5	Aceptable	5
12	Realización de operaciones con clientes/usuarios incluidos en listas restrictivas.	Evento de riesgo de LA/FT-06	Catastrófico = 5	Improbable = 1	Aceptable	5
13	Realización de operaciones con productos que utilizan fondos de dinero provenientes de países bloqueados o catalogados como más expuestos a LA/FT.	Evento de riesgo de LA/FT-12	Catastrófico = 5	Improbable = 1	Aceptable	5
14	Participación de socios y directivos en aprobación de operaciones posiblemente relacionadas con actividades de LA/FT.	Evento de riesgo de LA/FT-18	Catastrófico = 5	Improbable = 1	Aceptable	5
15	Realización de operaciones personales o con la empresa por parte de socios, funcionarios y directivos, posiblemente relacionada con actividades de LA/FT.	Evento de riesgo de LA/FT-19	Catastrófico = 5	Improbable = 1	Aceptable	5
16	Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	Leve = 2	Raro = 2	Aceptable	4

Evento de riesgo de LA/FT	Nombre	Ref.	Impacto	Probabilidad	Nivel de severidad	Puntaje riesgo
17	Realización de operaciones por empleados o funcionarios que adoptan comportamientos sospechosos: evaden controles, incurren en errores, impiden que otro compañero atienda a determinado cliente, se ausentan frecuentemente de su trabajo, terminan su jornada después de lo normal, tiene un estilo de vida que no se ajusta a su nivel de ingresos, etc.	Evento de riesgo de LA/FT-17	Crítico = 4	Improbable = 1	Aceptable	4
18	Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	Insignificante = 1	Possible = 3	Aceptable	3
19	Realización de operaciones con clientes/usuarios que en corto tiempo se vinculan a la empresa para múltiples productos.	Evento de riesgo de LA/FT-08	Insignificante = 1	Improbable = 1	Aceptable	1

Anexo 3

Ejemplo de medición del impacto para el riesgo residual

Identificación		Impacto por riesgos asociados residuales				
Nombre	Código	Riesgo legal residual	Riesgo reputacional residual	Riesgo de contagio residual	Riesgo operacional residual	Impacto total riesgo residual
Ponderación de riesgos asociados	Cód.	30%	40%	10%	20%	
Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	2 - Menor: Multas, gastos jurídicos e indemnizaciones entre 5 y 100 millones de pesos.	4 - Mayor: Divulgación de eventos y/o investigación por organismo regulador dado a conocer al público en medios informativos masivos y/o principales noticieros nacionales.	0	4 - Mayor: Multa - Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 1 Insignificante: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 0 a 5 mm de pesos .000 y 5 Superior: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto mayor a 5.00 mm de pesos .000 mm de pesos	3,0
Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	2 - Menor: Multas, gastos jurídicos e indemnizaciones entre 5 y 100 millones de pesos.	0	0	0	0,6
Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	3 - Importante: Multas, gastos jurídicos e indemnizaciones entre 100 y 1000 millones de pesos.	0	0	0	0,9
Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	2 - Menor: Multas, gastos jurídicos e indemnizaciones entre 5 y 100 millones de pesos	2 - Menor: aviso sorpresivo de prensa u otro medio masivo.	0	2 - Menor: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 5 Superior: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto mayor a 5.00mm de pesos y 1	1,8

Identificación		Impacto por riesgos asociados residuales				
Nombre	Código	Riesgo legal residual	Riesgo reputacional residual	Riesgo de contagio residual	Riesgo operacional residual	Impacto total riesgo residual
Ponderación de riesgos asociados	Cód.	30%	40%	10%	20%	
					Insignificante: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 0 a 5 mm de pesos .00 mm de pesos	
Realización de operaciones con clientes que solicitan transferencias de propiedad, a otras personas diferentes del titular o entrega de dinero a un tercero.	Evento de riesgo de LA/FT-05	4 - Mayor: Multas, gastos jurídicos e indemnizaciones entre 1000 y 5000 millones de pesos	4 - Mayor: Divulgación de eventos y/o investigación por organismo regulador dado a conocer al público en medios informativos masivos y/o principales noticieros nacionales.	0	4 - Mayor: Multa - Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 1 Insignificante: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto entre 0 a 5 mm de pesos .000 y 5 Superior: Insuficiencia en procesos, recursos, infraestructura o tecnología con impacto mayor a 5.00 mm de pesos .000 mm de pesos.	3,6

Anexo 4

Mapa de eventos de riesgo de LA/FT residual

	Nombre	Ref.	Cons.	Prob.	Riesgo	Puntaje de riesgo
1	Realización de operaciones en oficinas ubicadas en regiones de alto nivel de exposición al RLA/FT.	Evento de riesgo de LA/FT-16	Moderado	Casi seguro	Riesgo catastrófico	15
2	Realización de operaciones con clientes/usuarios que no se identifican plenamente.	Evento de riesgo de LA/FT-10	Moderado	Possible	Riesgo significativo	9
3	Realización de operaciones con clientes que solicitan transferencias de propiedad, a otras personas diferentes del titular o entrega de dinero a un tercero.	Evento de riesgo de LA/FT-05	Crítico	Possible	Riesgo moderado	12
4	Realización de operaciones con clientes/usuarios que suplantan al verdadero cliente o usuario.	Evento de riesgo de LA/FT-11	Crítico	Possible	Riesgo moderado	12
5	Realización de operaciones en las que se solicita frecuente cambio de titular, apoderado o beneficiario de un producto.	Evento de riesgo de LA/FT-14	Crítico	Possible	Riesgo moderado	12
6	Realización de operaciones con clientes/usuarios que frecuentemente aparecen incluidos en operaciones inusuales, señales de alerta y/o múltiples con cualquiera de los productos de la empresa.	Evento de riesgo de LA/FT-09	Leve	Casi seguro	Riesgo moderado	10
7	Realización de operaciones con dineros provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	Moderado	Possible	Riesgo significativo	9
8	Realización de operaciones con clientes/usuarios incluidos en	Evento de riesgo de LA/FT-07	Leve	Possible	Riesgo significativo	6

	Nombre	Ref.	Cons.	Prob.	Riesgo	Puntaje de riesgo
	operaciones sospechosas reportadas a la UIAF.					
9	Realización de operaciones en jurisdicciones catalogadas como de alto nivel de exposición al riesgo de LA/FT	Evento de riesgo de LA/FT-13	Insignificante	Casi seguro	Riesgo aceptable	5
10	Realización de operaciones en oficinas que presentan un alto volumen de Operaciones Sospechosas	Evento de riesgo de LA/FT-15	Insignificante	Casi seguro	Riesgo aceptable	5
11	Realización de operaciones con clientes/usuarios incluidos en listas restrictivas	Evento de riesgo de LA/FT-06	Catastrófico	Improbable	Riesgo aceptable	5
12	Realización de operaciones con productos que utilizan fondos de dinero provenientes de países bloqueados o catalogados como más expuestos a LA/FT.	Evento de riesgo de LA/FT-12	Catastrófico	Improbable	Riesgo aceptable	5
13	Participación de socios y directivos en aprobación de operaciones posiblemente relacionadas con actividades de LA/FT.	Evento de riesgo de LA/FT-18	Catastrófico	Improbable	Riesgo aceptable	5
14	Realización de operaciones personales o con la empresa por parte de socios, funcionarios y directivos, posiblemente relacionada con actividades de LA/FT.	Evento de riesgo de LA/FT-19	Catastrófico	Improbable	Riesgo aceptable	5
15	Realización de operaciones por empleados o funcionarios que adoptan comportamientos sospechosos: evaden controles, frecuentemente incurren en errores, impiden que otro compañero atienda a determinado cliente, se ausentan	Evento de riesgo de LA/FT-17	Crítico	Improbable	Riesgo aceptable	4

	Nombre	Ref.	Cons.	Prob.	Riesgo	Puntaje de riesgo
15	frecuentemente de su trabajo, frecuentemente terminan su jornada después de lo normal, tiene un estilo de vida que no se ajusta a su nivel de ingresos, etc.)					
16	Realización de operaciones por valores que no corresponden al perfil demográfico o económico.	Evento de riesgo de LA/FT-02	Insignificante	Possible	Riesgo aceptable	3
17	Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	Insignificante	Possible	Riesgo aceptable	3
18	Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	Leve	Improbable	Riesgo aceptable	2
19	Realización de operaciones con clientes/usuarios que en corto tiempo se vinculan a la empresa para múltiples productos.	Evento de riesgo de LA/FT-08	Insignificante	Improbable	Riesgo aceptable	1

Anexo 5

Ejemplo de causas y controles para cinco eventos de riesgo de LA/FT

Identificación		Causas del evento de riesgo de LA/FT e impacto por riesgos asociados inherentes		Control tratamiento
Nombre del evento de riesgo de LA/FT	Cód.	Causa primaria	Causa última	
Realización de operaciones con dinero provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	Incumplimiento de políticas, procesos y/o recomendaciones de órganos de control y oficial de cumplimiento que determinan no mantener relaciones o efectuar una mayor diligencia en razón del factor de riesgo, por estar más expuesto a LA/FT, cuando medie negligencia, imprudencia o falta de experiencia.	Empleado que intencionalmente no solicita y/o no confirma los datos suministrados por el cliente.	Realizar auditoría al proceso.
		Empleado que por falla, error u omisión no solicita y/o no confirma los datos suministrados por el cliente.	Empleado que por falla, error u omisión no solicita y/o no confirma los datos suministrados por el cliente.	Divulgar código de conducta y hacerlo firmar por el empleado.
				Realizar prueba de polígrafo.
		Fallas en el hardware y software.	Falta de mantenimiento preventivo y un plan de contingencia.	Capacitar al empleado sobre las políticas, y procedimientos antilavado.
		Cancelan anticipadamente los productos pactados a un plazo determinado.	Empleado que por falla, error u omisión no solicita y/o no confirma los datos suministrados por el cliente.	Diligenciar formulario de vinculación de cliente incluyendo soportes documentales de la información consignada.
Realización de operaciones por valores	Evento de riesgo de LA/FT-02	Aceptación de múltiples endosos en documentos.	Empleado que por falla, error u omisión no solicita y/o no confirma los datos suministrados por el cliente.	Plan de contingencia y plan de mantenimiento preventivo.
		Aceptación de solicitudes de pagos o transferencias de propiedad a otras personas diferentes del titular.		
		Inadecuada definición del perfil.	Utilización de perfiles estimados con	Aplicar técnicas estadísticas adecuadas que permiten

Identificación		Causas del evento de riesgo de LA/FT e impacto por riesgos asociados inherentes		Control tratamiento
Nombre del evento de riesgo de LA/FT	Cód.	Causa primaria	Causa última	
que no corresponden al perfil demográfico o económico.		base en información que los distorsiona, con el cual se podría exonerar de sospecha operaciones que podrían serlo.		tan la eliminación de vicios o sesgos.
		Falta de sistemas automatizados que permitan confrontar las características de la operación con las características socioeconómicas del cliente.	Falta de recursos.	Realizar manualmente la confrontación después de realizada la operación.
Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	No existen controles automáticos y en línea que permitan identificar diferentes direcciones y números telefónicos para un mismo número de edificación.	No existen señales de alerta que permiten identificar clientes con múltiples datos.	Diseñar aplicativo que genere señales de alerta para clientes con múltiples datos de georreferenciación. Diseñar políticas restrictivas y preventivas de la cantidad de cambios aceptados en dirección y teléfono y demás datos.
		Incumplimiento de políticas, procesos y/o recomendaciones de órganos de control y oficial de cumplimiento que determinan no mantener relaciones o efectuar una mayor diligencia en razón del factor de riesgo, por estar más expuesto al LA/FT, mediante negligencia o intencionalidad, imprudencia o falta de experiencia.		Capacitar al empleado sobre las políticas y procedimientos antilavado.
		Fallas en el hardware y software.	Falta de mantenimiento preventivo y un plan de contingencia.	Realizar auditoría al proceso. Divulgar código de conducta y hacerlo firmar por el empleado. Realizar prueba de polígrafo. Plan de contingencia y plan de mantenimiento preventivo.

Identificación		Causas del evento de riesgo de LA/FT e impacto por riesgos asociados inherentes		Control tratamiento
Nombre del evento de riesgo de LA/FT	Cód.	Causa primaria	Causa última	
Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	Incumplimiento intencional de políticas, procesos y/o recomendaciones de órganos de control y oficial de cumplimiento que determinan no mantener relaciones o efectuar una mayor diligencia en razón del factor de riesgo, por estar más expuesto al LA/FT, cuando medie negligencia, imprudencia o falta de experiencia.	Empleado que intencionalmente accede a pagar en efectivo incumpliendo las políticas de pago en cheque, definidas por la empresa.	Realizar auditoría al proceso. Divulgar código de conducta y hacerlo firmar por el empleado. Realizar prueba de polígrafo. Capacitar al empleado sobre las políticas, y procedimientos antilavado. Que el sistema bloquee automáticamente la operación hasta que el mismo sistema expida el cheque.
Realización de operaciones con clientes que solicitan transferencias de propiedad a otras personas diferentes del titular o entrega de dinero a un tercero.	Evento de riesgo de LA/FT-05	Incumplimiento de políticas, procesos y/o recomendaciones de órganos de control y oficial de cumplimiento sobre conocimiento del cliente, cuando medie negligencia, imprudencia o falta de experiencia.	Empleado que intencionalmente realiza transferencias de propiedad	Realizar auditoría al proceso. Divulgar código de conducta y hacerlo firmar por el empleado. Realizar prueba de polígrafo. Capacitar al empleado sobre las políticas y procedimientos antilavado.
		Fallas en el <i>hardware</i> y <i>software</i> .	Falta de mantenimiento preventivo y un plan de contingencia.	Plan de contingencia y plan de mantenimiento preventivo.

Anexo 6

Indicadores de efectividad de los controles

Identificación			Comparación				
Nombre del ERLA/FT	Cód.	Factor determinante del riesgo	Severidad inherente ERLA/FT		Severidad residual del ERLA/FT		Efectividad del control (ie.)
			Valor de la severidad del ERLA/FT riesgo inherente (s_{ri})	Clasificación severidad riesgo inherente	Valor de la severidad del ERLA/FT riesgo residual (s_{rr})	Clasificación severidad riesgo residual	
Realización de operaciones con dinero provenientes de posibles actividades relacionadas con LA/FT.	Evento de riesgo de LA/FT-01	Clientes	12	12 - 4 X 3 - evento de riesgo de LA/FT con severidad moderada	9	9 - 3 X 3 - evento de riesgo de LA/FT con severidad significativa	3
Realización de operaciones por valores que no corresponden al perfil demográfico o económico	Evento de riesgo de LA/FT-02	Clientes	3	3 - 3 X 1 - evento de riesgo de LA/FT con severidad aceptable.	3	3 - 3 X 1 - evento de riesgo de LA/FT con severidad aceptable	0
Realización de operaciones con clientes/usuarios que cambian frecuentemente de datos para su localización.	Evento de riesgo de LA/FT-03	Clientes	10	10 - 5 X 2 - evento de riesgo de LA/FT con severidad moderada	3	3 - 3 X 1 - evento de riesgo de LA/FT con severidad aceptable	7
Realización de operaciones con clientes/usuarios que se niegan a recibir dineros en cheques o transferencias bancarias, exigiendo que sean en efectivo.	Evento de riesgo de LA/FT-04	Clientes	2	2- 1 X 2- evento de riesgo de LA/FT con severidad aceptable	1	1 - 1 X 1 - evento de riesgo de LA/FT con severidad aceptable	1
Realización de operaciones con clientes que solicitan transferencias de propiedad a otras personas diferentes del titular o entrega de dinero a un tercero.	Evento de riesgo de LA/FT-05	Clientes	9	9 - 3 X 3 - evento de riesgo de LA/FT con severidad significativa	9	9 - 3 X 3 - evento de riesgo de LA/FT con severidad significativa	0

Identificación			Comparación					Efectividad del control (ie_c)	
Nombre del ERLA/FT	Cód.	Factor determinante del riesgo	Severidad inherente ERLA/FT		Severidad residual del ERLA/FT				
			Valor de la severidad del ERLA/FT riesgo inherente (s_{ri})	Clasificación severidad riesgo inherente	Valor de la severidad del ERLA/FT riesgo residual (s_{rr})	Clasificación severidad riesgo residual			
Realización de operaciones con clientes/usuarios incluidos en listas restrictivas.	Evento de riesgo de LA/FT-06	Clientes	4	4 - 4 X 1 - evento de riesgo de LA/FT con severidad aceptable	4	4 - 4 X 1 - evento de riesgo de LA/FT con severidad aceptable	0		
Realización de operaciones con clientes/usuarios incluidos en operaciones sospechosas reportadas a la UIAF.	Evento de riesgo de LA/FT-07	Clientes	4	4 - 4 X 1 - evento de riesgo de LA/FT con severidad aceptable	3	3 - 3 X 1 - evento de riesgo de LA/FT con severidad aceptable	1		
Realización de operaciones con clientes/usuarios que en corto tiempo se vinculan a la empresa para múltiples productos.	Evento de riesgo de LA/FT-08	Clientes	1	1 - 1 X 1 - evento de riesgo de LA/FT con severidad aceptable	1	1 - 1 X 1 - evento de riesgo de LA/FT con severidad aceptable	0		
Realización de operaciones con clientes/usuarios que frecuentemente aparecen incluidos en operaciones inusuales, señales de alerta y/o múltiples con cualquiera de los productos de la empresa.	Evento de riesgo de LA/FT-09	Clientes	10	10 - 5 X 2 - evento de riesgo de LA/FT con severidad moderada	10	10 - 5 X 2 - evento de riesgo de LA/FT con severidad moderada	0		
Realización de operaciones con clientes/usuarios que no se identifican plenamente.	Evento de riesgo de LA/FT-10	Clientes	9	9 - 3 X 3 - evento de riesgo de LA/FT con severidad significativa	12	9 - 3 X 3 - evento de riesgo de LA/FT con severidad significativa	-3		
Realización de operaciones con clientes/usuarios que suplantan al	Evento de riesgo de LA/FT-11	Clientes	9	9 - 3 X 3 - evento de riesgo de LA/FT con	9	9 - 3 X 3 - evento de riesgo de LA/FT con	0		

Identificación			Comparación				
Nombre del ERLA/FT	Cód.	Factor determinante del riesgo	Severidad inherente ERLA/FT		Severidad residual del ERLA/FT		Efectividad del control (ie _c)
			Valor de la severidad del ERLA/FT riesgo inherente (s _{ri})	Clasificación severidad riesgo inherente	Valor de la severidad del ERLA/FT riesgo residual (s _{rr})	Clasificación severidad riesgo residual	
verdadero cliente o usuario.				severidad significativa		severidad significativa	
Realización de operaciones con productos que utilizan fondos de dinero provenientes de países bloqueados o catalogados como más expuestos a LA/FT.	Evento de riesgo de LA/FT-12	Producto	4	4 - 1 X 4 - evento de riesgo de LA/FT con severidad significativa	4	4 - 1 X 4 - evento de riesgo de LA/FT con severidad significativa	0
Realización de operaciones en jurisdicciones catalogadas como de alto nivel de exposición al riesgo de LA/FT.	Evento de riesgo de LA/FT-13	Jurisdicción	10	10 - 5 X 2- evento de riesgo de LA/FT con severidad moderada	10	10 - 5 X 2- evento de riesgo de LA/FT con severidad moderada	0
Realización de operaciones en las que se solicita frecuente cambio de titular, apoderado o beneficiario de un producto.	Evento de riesgo de LA/FT-14	Clientes	12	12 - 4 X 3 - evento de riesgo de LA/FT con severidad moderada	9	9 - 3 X 3 - evento de riesgo de LA/FT con severidad significativa	3
Realización de operaciones en oficinas que presentan un alto volumen de operaciones sospechosas.	Evento de riesgo de LA/FT-15	Canal	10	10 - 5 X 2- evento de riesgo de LA/FT con severidad moderada	10	10 - 5 X 2- evento de riesgo de LA/FT con severidad moderada	0
Realización de operaciones en oficinas ubicadas en regiones de alto nivel de exposición al RLA/FT.	Evento de riesgo de LA/FT-16	Canal	10	10 - 5 X 2 - evento de riesgo de LA/FT con severidad moderada	10	10 - 5 X 2 - evento de riesgo de LA/FT con severidad moderada	0

Identificación			Comparación					Efectividad del control (ie _c)	
Nombre del ERLA/FT	Cód.	Factor determinante del riesgo	Severidad inherente ERLA/FT		Severidad residual del ERLA/FT				
			Valor de la severidad del ERLA/FT riesgo inherente (s _{ri})	Clasificación severidad riesgo inherente	Valor de la severidad del ERLA/FT riesgo residual (s _{rr})	Clasificación severidad riesgo residual			
Realización de operaciones por empleados o funcionarios que adoptan comportamientos sospechosos: evaden controles, frecuentemente incurren en errores, impiden que otro compañero atienda a determinado cliente, se ausentan de su trabajo, terminan su jornada después de lo normal, tiene un estilo de vida que no se ajusta a su nivel de ingresos, etc.).	Evento de riesgo de LA/FT-17	Empleados y funcionarios	4	4 - 1 X 4 - evento de riesgo de LA/FT con severidad significativa	4	4 - 1 X 4 - evento de riesgo de LA/FT con severidad significativa	0		
Participación de socios y directivos en aprobación de operaciones posiblemente relacionadas con actividades de LA/FT.	Evento de riesgo de LA/FT-18	Empleados y funcionarios	4	4 - 1 X 4 - evento de riesgo de LA/FT con severidad significativa	4	4 - 1 X 4 - evento de riesgo de LA/FT con severidad significativa	0		
Realización de operaciones personales o con la empresa por parte de socios, funcionarios y directivos, posiblemente relacionada con actividades de LA/FT.	Evento de riesgo de LA/FT-19	Empleados y Funcionarios	4	4 - 1 X 4 - evento de riesgo de LA/FT con severidad significativa	4	4 - 1 X 4 - evento de riesgo de LA/FT con severidad significativa	0		

Anexo 7

Señales de alerta que se pueden percibir en la operación comercial o financiera de una empresa del sector real

1. Señales de alerta relacionadas con el cliente

1.1. *Señales de alerta en personas naturales o jurídicas*

- Actúan a nombre de terceros intentando ocultar la identidad del cliente real.
- Fraccionan transacciones para evitar requerimientos de documentación.
- Amenazan o intentan sobornar al empleado de la entidad con el fin de que acepte información incompleta, falsa o para que no diligencie el formulario de registro de información.
- Inicialmente realizan transacciones por montos bajos, pero al corto tiempo las incrementan en altas cantidades.
- Realizan múltiples operaciones en efectivo en la misma o en diferentes agencias.
- Son personas ajena a la entidad quienes tienen firma registrada para el manejo financiero.
- Poseen gran solvencia económica y sin embargo les resulta difícil la consecución de referencias o codeudores.
- Realizan operaciones en cantidades o valores no acordes con su actividad económica.
- Realizan transferencias múltiples de grandes cantidades de dinero a otras ciudades o países y dirigidas a diferentes clientes.
- Registran la misma dirección y/o teléfono de otras personas con las que no tienen relación aparente.

- Cambian frecuentemente sus datos, verbigracia dirección, teléfono, ocupación, etc.
- Poseen número de identificación correspondiente a un empleado retirado por manejos fraudulentos.
- Definen su actividad económica como “independiente” y manejan grandes cantidades de dinero.
- Compran y pagan en efectivo cartas de crédito.
- Se niegan a soportar una operación o a actualizar la información básica.
- Intentan realizar operaciones con dinero falso.
- Diligencian los formularios o formatos con letra ilegible.
- Solicitan que se les exonere procedimientos de control sin tener derecho a ello.
- Son recomendados por clientes que exhiben actitudes poco confiables.
- Adquieren productos o sostienen relaciones comerciales en un barrio o localidad diferente y distante a la sede de los negocios del cliente y/o a su lugar de residencia.
- Exigen ser atendidos o manifiestan marcada preferencia por un funcionario específico de la empresa.
- Suministran información falsa, de difícil verificación o insuficiente.
- Se muestran renuentes o molestos cuando se les solicita una adecuada identificación o el diligenciamiento de los formatos sobre operaciones que superen los montos señalados en la ley o en normas internas.
- Se muestran nerviosos, al preguntárseles la información requerida, dudan en las respuestas y/o traen escrita la información solicitada.

- Ofrecen productos o servicios con precios o por debajo de los costos normales del mercado, o de compra más elevados.
- Cambian frecuentemente billetes de baja denominación por billetes de alta denominación y viceversa.
- Clientes que efectúan operaciones con identidades falsas.
- El cliente entrega información insuficiente o falsa.
- Al confirmar los datos, estos cambian con respecto a los informados por el cliente.
- Al digitar la identificación reporta que en el sistema existe otra persona con el mismo número.
- Autorizan a terceros para tramitar las operaciones (testaferros).
- Realizan varias transacciones a cargo de una misma persona por sumas que están por debajo de las sometidas a control especial.
- Inexistencia de referencias personales y comerciales o falsedad en las mismas.
- Realizan múltiples operaciones en efectivo en la misma o en diferentes agencias, sin justificación para su fraccionamiento.

1.2. *Señales en personas jurídicas*

- Tienen nuevos propietarios, las empresas han sido adquiridas con dificultades económicas, cambian su naturaleza y presentan en corto lapso utilidades desbordadas
- Tienen como propietarios o directivos a personas de estratos bajos y con dificultades económicas y que manejan grandes volúmenes de dinero.
- Han sido constituidas con bajos capitales, recibiendo poco después grandes sumas de inversión, principalmente extranjera.

- Realizan grandes inversiones no obstante haber sido creadas muy recientemente.
- Reciben ingresos no operacionales por mayor cuantía que los ingresos operacionales.
- Tienen un capital suscrito muy bajo y/o un objeto social muy amplio.
- Tienen en común socios, gerentes, administradores o representantes legales con otras personas jurídicas o empresas (*outsourcing*).

2. **Señales por operaciones múltiples**

- Operaciones por montos similares por diferentes clientes, quienes registran un mismo número telefónico y/o la misma dirección.
- Operaciones en diferentes ciudades del país, por un mismo cliente.
- Múltiples operaciones por grandes cantidades de dinero dirigidas a varias ciudades países y/o dirigidas a diferentes clientes.

3. **Señales por operaciones individuales**

- Solicitud de entrega de productos a nombre de una persona o negocio diferente del comprador.
- Respuestas dadas por un cliente, contactado telefónicamente, quien manifiesta que no conoce la existencia del pedido.
- No existe registro de dirección por parte del cliente, con el argumento de que él mismo recogerá el pedido.
- Clientes que no se pueden contactar telefónicamente.
- Consultas por parte de clientes sobre la existencia de otros pedidos para ellos o para terceras personas.
- El cliente suministra información falsa, de difícil verificación o insuficiente.

- Se muestran renuentes o molestos cuando se les solicita una adecuada identificación o el diligenciamiento de los formatos sobre operaciones que superen los montos señalados en la Ley o en normas internas.
- Amenazan o intentan sobornar al empleado de la entidad con el fin de que acepte información incompleta, falsa o para que no diligencie el formulario de registro de información.
- Se muestran nerviosos al preguntárseles la información requerida, dudan en las respuestas y/o traen escrita la información solicitada.
- Clientes que tratan de colocar un dedo diferente del índice derecho en los documentos que requieren la huella digital.
- Usuarios que presentan enfermedad en el índice derecho y tratan de colocar el índice izquierdo en los documentos que requieren la huella digital.
- Transacciones con personas relacionadas en listas del Departamento de Estado Norteamericano (Lista OFAC, Clinton o similares).
- Usuarios que presentan un documento de identificación con señales de ser falso, de haber sido adulterado o ilegible por deterioro.
- Usuarios que no son conocidos en el número telefónico indicado en la orden del pedido o factura.
- Clientes que consultan sus datos en un papel.
- Usuarios de apariencia (vestido o forma de hablar) humilde realizando operaciones por sumas iguales o superiores al máximo valor definido como política por la empresa.
- Cuando la persona que se molesta y viene a hacer un reclamo es diferente al cliente.
- Cuando el cliente se acerca a la agencia sin ser notificado previamente y al proporcionar los datos requeridos para su comprobación resultan falsos o errados.

4. Señales de alerta relacionadas con el producto

Cuando el valor individual o acumulado de una venta supera la cifra establecida por la empresa para calificar una operación como inusual.

5. Señales de alerta relacionadas con los canales de distribución

Cuando la sede del negocio del cliente está ubicada en zona de alto riesgo de LA/FT.

6. Señales de alerta relacionadas con las jurisdicciones

Nivel de exposición del país, región, ciudad o lugar al lavado de activos, al terrorismo, a la corrupción administrativa, al secuestro, a la prostitución, al contrabando, al tráfico de armas, al tráfico de personas y a todos aquellos delitos conexos con el LA/FT.

Países denominados “paraísos fiscales”, utilizados por delincuentes para realizar operaciones de LA/FT.

Generalmente estas señales de alerta son definidas por las autoridades policivas y judiciales.

7. Señales en operaciones internacionales

- Compra o vende más de una cantidad de dólares o pesos colombianos establecida por política en cualquier tiempo dentro del año calendario.
- Acumula más de una cantidad de dólares o pesos colombianos establecida por política en el mes calendario.
- Acumula más de una cantidad de dólares o pesos colombianos establecida por política en cualquier periodo del año.
- Compra hasta una cantidad máxima de dólares o pesos colombianos en el año establecida por política interna de la empresa.

- Requiere actualización de la información, pues ya cumplió el año.
- Reintegros por concepto de exportaciones realizadas a países diferentes al del origen de la transacción, tales como paraísos fiscales.
- Reintegros por exportaciones sin la intermediación de la empresa.
- Reintegro por exportaciones atípicas no acordes con el país de origen y/o destino y por un valor de venta superior al establecido para su compra.
- Recepción de grandes sumas de inversión extranjera por parte de empresas constituidas con muy bajos capitales.
- Operaciones internacionales a nombre de empresas cuya denominación social o nombre se asemeja a empresas reconocidas en Colombia o en el exterior, sin que exista vínculo aparente entre ellas.

8. Señales de alerta que se pueden percibir por fuera de la operación comercial o financiera

Son todas aquellas actitudes y comportamientos que presenta cualquier empleado de la empresa, cualquiera que sea su nivel jerárquico y organizacional durante su permanencia al interior de la empresa, o durante su vida laboral, social y familiar, que hacen prever su participación o realización de actividades tendientes a favorecer el lavado de activos y que cualquier funcionario de la empresa, independientemente de su nivel jerárquico u organizacional, pueda detectar con base en su observación y buen criterio.

A continuación se hacen una selección de las principales señales de alerta respecto de los empleados:

- Tramitan frecuentemente operaciones con excepciones, evaden los controles internos o de aprobación establecidos, o ayudan en transacciones de usuarios con identidad desconocida.
- Tienen un estilo de vida que no corresponde con el monto de su salario.

- Impiden que otros compañeros de trabajo atiendan a determinados clientes.
- Son renuentes a disfrutar vacaciones, a aceptar cambios de su actividad o promociones que impliquen no continuar ejecutando las mismas actividades.
- Se ausentan del lugar de trabajo con frecuencia.
- Permanecen frecuentemente en la oficina más allá de la hora de cierre o concurren a ella por fuera del horario habitual.
- Se descuadran con frecuencia dando explicación insuficiente o inadecuada.
- Directivo, funcionario o colaboradores que aparentan no conocer un cliente preferente.
- Funcionarios que no soportan debidamente la información de vinculación del cliente.
- No confrontan la huella dactilar del cliente tomada en el formulario de vinculación contra la que aparece en el documento de identidad.
- Agencias que comienzan a manejar mucho dinero en efectivo sin que aumenten los reportes de las transacciones proporcionalmente.
- Alguna agencia empieza a enviar una cantidad de dinero más que proporcional a sus promedios.

9. Señales de alerta según la forma como se producen

- Señales de alerta producidas por el sistema previa programación de las mismas.
- Señales de alerta que debe identificar el funcionario mediante su percepción.

Son todas aquellas actitudes y comportamientos que presenta un cliente cuando está adquiriendo algún producto de la empresa del sector real, que hacen prever la posibilidad de cualquier tipo de actividad tendiente a lavar activos y que cualquier funcionario puede detectar con base en su observación externa y buen criterio.

La experiencia, el sentido común, el criterio comercial, el conocimiento que se tiene del cliente, de su actividad u oficio, así como el origen, volumen y características de sus operaciones, son elementos necesarios a tener en cuenta para la utilización de las señales de alerta y detección de operaciones inusuales.

10. Señales de alerta en operaciones notariales susceptibles de estar particularmente vinculadas con el lavado de activos

Las siguientes señales de alerta fueron tomadas de la Resolución N° 033 de 2007 (abril 9) emanada de la Unidad Administrativa Especial de Información y Análisis Financiero, por la cual se impone a los notarios de todos los Círculos del territorio nacional, la obligación de reportar de manera directa a la UIAF.

Sector inmobiliario e inversiones de finca raíz:

- Utilización de testaferros. En la mayoría de los casos, se utilizan terceras personas (testaferros), para comprar, vender, administrar o manejar numerosas propiedades a nombre o por instrucción de otra.
- La naturaleza o monto de las operaciones activas o pasivas de los compradores, no corresponden con su actividad económica o antecedentes financieros.
- Compra de bienes inmobiliarios realizadas en forma sucesiva (doble e inmediata compra-venta), para transferir la propiedad a diferentes personas en poco tiempo, sin una causa aparente.
- Compras realizadas para terceros (fiduciarios), que sugieren el deseo del anonimato en la propiedad de los bienes.

- Adquisiciones masivas de bienes inmobiliarios por personas determinadas y sin justificación aparente.
- Compra de bienes inmobiliarios a favor de menores de edad.
- Fechas cercanas en la compra de bienes inmobiliarios por un mismo comprador o por compradores relacionados entre sí.
- Compra de bienes inmobiliarios de alto valor, por parte de entidades con escaso capital o sin aparente capacidad económica.
- Compra de bienes inmobiliarios por personas con domicilio desconocido, con dirección exclusiva para correspondencia o con datos de difícil verificación.
- Compradores de lejana procedencia dentro del territorio nacional que se desplazan solo para comprar el inmueble.
- Realizan trámites de compra-venta sin haber registrado actos anteriores en la oficina de instrumentos públicos respectiva.
- Indicios de que el comprador no actúa por su cuenta y que intenta ocultar la identidad del verdadero comprador.
- Donación de inmuebles que no corresponde con las actividades o características del beneficiario.

Constitución de sociedades

Otra modalidad utilizada para lavar dinero es la constitución de sociedades de fachada (funcionan y desarrollan una actividad ilícita junto con otra aparentemente lícita), o sociedades de papel (existen legalmente pero su funcionamiento y en operaciones son ficticias), las cuales se utilizan para disfrazar el movimiento de dinero proveniente de actividades ilícitas o encubrir a los propietarios reales de la empresas, utilizando representantes legales o testaferros. Algunas señales de alerta relacionadas con esta tipología son:

- Constitución de empresas con nombre similar al de empresas de trayectoria reconocida.
- Constitución de empresas con capitales que no guardan relación con su actividad económica.
- Constitución de empresas con capitales o socios provenientes de países considerados de alto riesgo.
- Constitución de empresas con un objetivo social muy amplio.
- Constitución de empresas cuyos dueños son otras empresas o es difícil identificar al propietario real.
- Constitución de varias empresas en fechas cercanas por los mismos propietarios relacionados entre sí o con características comunes.
- Compra-venta de empresas quebradas o en dificultades económicas por parte de personas sin trayectoria en el sector.
- Constitución de empresas sin ánimo de lucro con objeto social inconsistente o sospechoso.
- Individuos sin capacidad económica asumen deudas, ceden acciones o derechos de compañías en dificultades económicas.
- Creación de varias empresas con propietarios, accionistas o miembros de juntas directivas comunes.
- Constitución de empresas con objeto social que incluya manejo de donaciones (nacionales o internacionales).
- Constitución de sociedades con altos aportes de dinero en efectivo.
- Nombramiento de administradores que aparentemente carecen de idoneidad profesional para cumplir el cargo.
- Nombramiento del mismo administrador o de los mismos miembros de junta directiva en varias empresas.

Cancelación de gravámenes hipotecarios o liquidación de sociedades

- Cancelación anticipada de hipotecas con pago de elevadas sumas de dinero en efectivo.
- Cuando un bien es hipotecado varias veces y se cancela el valor de las hipotecas antes de su vencimiento.
- Cuando hay cancelación de escrituras de empresas en fechas cercanas por los mismos propietarios relacionados entre sí o con características comunes.
- Cuando se liquida una sociedad sin motivo o justificación aparente.
- Cuando se modifica la escritura de una sociedad para incluir o excluir a socios relacionados entre sí o con otras empresas.

BIBLIOGRAFÍA

- Basel Committee on Banking Supervision (BCBS), International Association of Insurance Supervisors (IAIS), e International Organization of Securities Commissions (IOSCO). “Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism”. Disponible en Web: <<http://www.bis.org/publ/joint05.pdf?noframes=1>> (Consulta: octubre 14 de 2009).
- “Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism – Update January 2005-”. Disponible en Web: <<http://www.bis.org/publ/joint11.pdf?noframes=1>> (Consulta: octubre 14 de 2009).
- Basel Committee on Banking Supervision (BCBS), “Debida diligencia con la clientela de los bancos”. Disponible en Web: <<http://www.bis.org/publ/bcbs85s.pdf>> (consultada el 7 de octubre de 2009).
- “Prevención del uso criminal del sistema bancario para fines de lavado de activos”. Disponible en Web: <<http://www.bis.org/publ/bcbsc137.pdf?noframes=1>> (Consulta: octubre 7 de 2009).
- Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering, diciembre de 2008, Disponible en Web: <<http://www.bis.org/publ/bcbsc137.pdf?noframes=1>>.
- Código Penal Colombiano (L. 599 de 2000), artículos 323 (modificado por la L. 1121 de 2006), 325, 326, 327, 446 y 447.
- Código de ética y conducta de la empresa.
- Comisión Interamericana para el Control del Abuso de Drogas (CICAD), “Reglamento modelo sobre delitos de lavado de activos relacionados con el tráfico ilícito de drogas y otros delitos graves”.

- Comité de Ministros de la Unión Europea, “Convención del Consejo de Europa sobre Blanqueo de Capitales, Investigación, Incautación y Decomiso de los Productos del Delito”, Disponible en Web: <<http://conventions.coe.int/Treaty/EN/Treaties/Word/198.doc>> (Consulta: octubre 26 de 2009).
- Corte Constitucional, Sentencia C-176 de abril 12 de 1994, M.P. Alejandro Martínez Caballero.
 - Sentencia C-374 de agosto 13 de 1997, M.P. José Gregorio Hernández Galindo.
 - Sentencia C-851 de agosto 17 de 2005, M.P. Manuel José Cepeda Espinosa.
 - Sentencia SU-157 de marzo 10 de 1999, M.P. Alejandro Martínez Caballero.
 - Sentencia T-468 de junio 5 del 2003, M.P. Rodrigo Escobar Gil.
- Cuellar, María Mercedes, Discurso de clausura del VII Congreso Panamericano de Control y Prevención del Lavado de Activos y Financiación del Terrorismo pronunciado el día 27 de julio de 2007 en Cartagena de Indias (Colombia).
- Cumbre de las Américas, Declaración de principios y Plan de acción, 1994.
- Decreto-Ley 663 de abril 2 de 1993, Diario Oficial N° 40.820, de abril 5 de 1993.
- Estatuto Orgánico del Sistema Financiero, artículos 102 a 107.
- García, Jean-Paul, “Objetivos administrativos y operativos de Tracfin”, En: *Memorias del III Congreso de Administración del Riesgo*, organizado por Asobancaria, Rionegro, noviembre 14 y 15 de 1996.
- Gay, Phillips, “Acciones gremiales en la lucha contra el lavado de activos en los Estados Unidos de América”, En: *Memorias del III Congreso de Administración del Riesgo*, Asobancaria, Rionegro, noviembre 14 y 15 de 1996.

- Grupo de Acción Financiera Internacional (GAFI), Página web oficial disponible en: <<http://www.fatf-gafi.org>> (Consulta: octubre 15 de 2009).
- “Las Cuarenta Recomendaciones”, Disponible en Web: <<http://www.fatf-gafi.org/dataoecd/38/53/34030987.pdf>> (Consulta: octubre 15 de 2009).
- “Notas Interpretativas de las Cuarenta Recomendaciones”, Disponible en Web: <http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236920_33988956_1_1_1_1,00.html#General_information> (Consulta: octubre 15 de 2009).
- “Las Ocho Recomendaciones especiales”.
- Grupo de Acción Financiera del Caribe (GAFIC), Las Diecinueve Recomendaciones que complementan Las Cuarenta del GAFI.
- Grupo de Acción Financiera de Sudamérica (GAFISUD), Compromisos.
- Grupo Egmont, Página web oficial disponible en: <<http://www.egmontgroup.org/>>.
- “Best Practices for the Exchange of Information Between Financial Intelligence Units”, 2004, Disponible en Web: <<http://www.egmontgroup.org/library/egmont-documents>> (Consulta: noviembre 10 de 2009).
- “Information Paper on Financial Intelligence Units and the Egmont Group”, Disponible en Web: <<http://www.egmontgroup.org/library/egmont-documents>> (Consulta: noviembre 10 de 2009).
- “Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases”, The Hague, 13 June 2001, Disponible en Web: <<http://www.egmontgroup.org/library/egmont-documents>> (Consulta: noviembre 10 de 2009).
- “Statement of Purpose of the Egmont Group of Financial Intelligence Units”, Guernsey, 23rd June 2004, Disponible en Web: <<http://www.egmontgroup.org/library/egmont-documents>> (Consulta: noviembre 10 de 2009).

- Hernández Quintero, Hernando, *El lavado de activos*, 2da ed., Bogotá: Ed. Gustavo Ibáñez, 1997.
- KPMG Colombia, Basilea II, “Una mirada más cercana. Administración del riesgo operacional”, En: *Boletín Financiero*, abril de 2004, Disponible en Web: <http://www.kpmg.com.co/publicaciones/bol_fin/2004/bolfin%20abril_04.pdf>.
- L'Express, “Así opera el lavado mundial de dineros sucios”, En: *Revisita Summa*, edición N° 86.
- Ley 1121 de 2006 (diciembre 29), Diario Oficial N° 46.497 del 30 de diciembre de 2006.
- Ley 190 de 1995 (junio 6), Estatuto Anticorrupción, Diario Oficial N° 41.878 del 6 de abril de 1993.
- Ley 526 de 1999, por la cual se crea la Unidad de Información y Análisis Financieros (UIAF) adscrita al Ministerio de Hacienda y Crédito Público.
- Martínez Sánchez, Wilson Alejandro, *El lavado de activos en el mercado de valores*, Bogotá: Ed. Gustavo Ibáñez, 2004.
- Norma NTC 5254, Gestión de riesgos.
- Norma NTC ISO 9001:2000.
- Organización de Naciones Unidas. Consejo Económico y Social, Comisión de Estupefacientes, Página web oficial disponible en: <<http://www.un.org/spanish/Depts/dpi/boletin/drogas/fiscalizacion.shtml>> (Consulta: octubre 21 de 2009).
 - “Convención contra el Tráfico Ilícito de Estupefacientes y Substancias Sicotrópicas” (Convención de Viena, 1988), Disponible en Web la versión en inglés del texto completo en: <http://www.unodc.org/pdf/convention_1988_en.pdf> (Consulta: octubre 21 de 2009).
 - “Convención contra la Delincuencia Organizada Trasnacional” (Convención de Palermo), Disponible en Web: <<http://www.un.org/>

- disarmament/convarms/ArmsTradeTreaty/docs/Background%20documents/Firearms%20Protocol%20-%20S.pdf> (Consulta octubre 16 de 2009).
- Programa de Asistencia Legal para Latinoamérica y el Caribe adscrito a la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), Página web oficial en: <<http://www.bis.org/publ/bcbsc137.pdf?noframes=1>> (Consulta: octubre 7 de 2009).
- UNODC, “Riesgo de lavado de activos en instrumentos financieros, usuarios y empleados de instituciones financieras”, 1º versión, agosto de 2006, Disponible en Web: <http://www.superbancos.gob.pa/aspec_prevencion/documentos/UNODC_Instrumentos_Financieros_200608.pdf> (Consulta: octubre 6 de 2009).
- Ospina Velasco, Jaime, “Análisis crítico y perspectivo de la detección, prevención y control del lavado de activos en Colombia”, En: *Memorias del III Congreso de Administración del Riesgo*, Asobancaria, Rionegro, noviembre 14 y 15 de 1996.
- Silva Sánchez, Jesús-María, *La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, Madrid: Ed. Civitas, 1999.
- Sintura, Francisco, *Concesión de beneficios por colaboración eficaz con la justicia. El lavado de activos. Normas penales y estados de excepción*, Bogotá: Ed. Diké, 1995.
- Sullivan, Michael, “Acciones y recomendaciones para la prevención del lavado de activos”, En: *Memorias del III Congreso de Administración del Riesgo*, Asobancaria, Rionegro, noviembre 14 y 15 de 1996.
- Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales (DIAN), Circular Externa N° 0170 de octubre 10 del 2002.
- Unidad de Información y Análisis Financiero (UIAF), Carta Circular N° 001 de marzo 12 de 2009.
- Concepto de junio 21 de 2007, Disponible en Web: <http://www.uiaf.gov.co/index.php?idcategoria=1340&uiaf_2008=f88de3cb178328aa37926f25a09340fa#> (Consulta: septiembre 16 de 2009).

- “Compilación y descripción de las tipologías producidas por la unidad de información y análisis financiero” (documento público), versión de septiembre de 2006, UIAF, Disponible en Web: <http://www.uiaf.gov.co/index.php?idcategoria=35&uiaf_2008=f88de3cb178328aa37926f25a09340fa> (Consulta: septiembre 16 de 2009).
- “Guía de reporte y control”, versión 2009, UIAF, Disponible en Web: <http://www.uiaf.gov.co/index.php?idcategoria=2516&uiaf_2008=f88de3cb178328aa37926f25a09340fa#> (Consulta: septiembre 16 de 2009).
- “Instrumento de calificación de reporte de operaciones sospechosas”, versión de mayo de 2005, UIAF, Disponible en Web: <http://www.uiaf.gov.co/index.php?idcategoria=316&download=Y&uiaf_2008=f88de3cb178328aa37926f25a09340fa> (Consulta: septiembre 16 de 2009).
- Oficio N° 29020 enviado al señor Superintendente Financiero de Colombia.
- Resolución 285 de 2007.
- Resolución 062 de junio 12 de 2007.
- Resolución 111 de agosto 21 de 2007.

Superintendencia Bancaria de Colombia

- Concepto N° 2000069551-1 de diciembre 20 de 2000.
- Concepto N° 2002046102-1 de septiembre 12 de 2002.
- Concepto N° 2003044819-1 de septiembre 15 de 2003.
- Concepto N° 2004006247-1 de abril 2 de 2004.
- Concepto N° 2004053989-2 de octubre 15 de 2004.
- Concepto N° 2004066219-4 de diciembre 21 de 2004.
- Concepto N° 2005004064-001 de septiembre 14 de 2005.

Superintendencia Financiera de Colombia

- Circular Básica Jurídica N° 7 de 1996.
- Circular Externa N° 75 de 1992.
- Circular Externa N° 023 de 2005.
- Circular Externa N° 022 de 2007.
- Circular Externa N° 052 de 2007.
- Circular Externa N° 061 de 2007.
- Circular Externa N° 026 de 2008.
- Circular Externa N° 054 de 2008.
- Circular Externa N° 060 de 2008.
- Circular Externa N° 008 de 2009.
- Circular Externa N° 009 de 2009.
- Concepto N° 2000069551-1 de diciembre 20 de 2000.
- Concepto N° 2005049770-004 de febrero 27 de 2006.
- Concepto N° 2005060654-1 de enero 24 de 2006.
- Concepto N° 2005062113-1 de enero 27 de 2006.
- Concepto N° 2006017379-002 de agosto 9 de 2006.
- Concepto N° 2006018977-001 de mayo 23 de 2006.
- Concepto N° 2008003821-001 de enero 28 de 2008.
- Concepto N° 2008009451-001 de abril 2 de 2008.
- Concepto N° 2008009513-001 de marzo 11 de 2008.
- Concepto N° 2008024244-001 de junio 5 de 2008.
- Concepto N° 2008026810-001 de julio 7 de 2008.

- Concepto N° 2008027339-001 de mayo 15 de 2008.
- Concepto N° 2008031221-001 de junio 9 de 2008.
- Concepto N° 2008040297-002 de octubre 10 de 2008.
- Concepto N° 2008040595-001 de junio 24 de 2008.
- Concepto N° 2008060521-002 de octubre 16 de 2008.
- Concepto N° 2008061356-001 de enero 8 de 2009.
- Concepto N° 2008072629-001 de diciembre 15 de 2008
- Concepto N° 2008088852-001 de enero 26 de 2009.
- Concepto N° 2009006724-001 de marzo 6 de 2009.
- Concepto N° 2009010745-001 de marzo 10 de 2009.
- Concepto N° 2009017224-003 de abril 22 de 2009.
- Concepto N° 2009044020-001 de julio 9 de 2009.

CONTENIDO DEL CD-ROM

1. Aplicativo para gestionar el SIPLA/FT o el SARLA/FT

(La explicación de este aplicativo está en la segunda parte del libro en el capítulo 3, numeral 11).

2. Ejemplos de perfil descriptivo de ERLA/FT

3. Riesgo de lavado de activos en instrumentos financieros, usuarios y empleados de instituciones financieras (DOCUMENTO UNODC)

4. Normatividad para empresas del sector financiero y del sector real

4.1. Sector financiero Colombia

- Circular Externa 026 de 2008, Superfinanciera
- Circular Externa 022 de 2007, Superfinanciera
- Carta Circular Externa 001 de 2006, Superfinanciera
- Circular Externa 001 de 2006, Superfinanciera
- Circular Externa 004 de 2006, Superfinanciera

4.2. Sector Real Colombia

4.2.1. Compraventa de oro

- Resolución 363 de 2008, UIAF

4.2.2. Profesionales compraventa de divisas

- Documento Técnico, Resolución 062 de 2007 (Modificado)
- Resolución 062 de 2007, UIAF

4.2.3. Supersociedades

- Circular Externa 100-004 de 2009

4.2.4. Supervigilancia

- Circular Externa 003 de 2009
- Circular Externa 007 de 2006
- Circular Externa 009 de 2004 (contenido)
- Circular Externa 009 de 2004 (histórico de registro)
- Circular Externa 009 de 2004 (lista de chequeo)

4.2.5. Compraventa de vehículos

- Resolución 114 de 200Z, UIAF

4.2.6. Supernotariado

- Documento Técnico 033 de 2007, versión 2
- Resolución 033 de 2007, UIAF
- Resolución 044 de 2007, UIAF
- Instrucción Administrativa 8 de 2007
- Instrucción Administrativa 02-07 de 2002

4.2.7. Supersolidaria

- Circular Externa 007 de 2003, capítulo 11

4.2.8. DIAN

- Resolución 285 de 2007, UIAF
- Circular Externa 170 de 2002 (contenido)
- Circular Externa 170 de 2002 (señales de alerta)
- Circular Externa 170 de 2002 (formato ROS)

4.2.9. Supersalud

- Resolución 78 de 2007, UIAF

- Resolución 141 de 2006, UIAF
- Resolución 142 de 2006, UIAF
- Documento Técnico Resolución 141 de 2006, UIAF
- Documento Técnico Resolución 142 de 2006, UIAF
- Resolución 1453 de 2006, ETESA
- Resolución 1111 de 2006, ETESA
- Circular Externa 081 de 1999

4.2.10. Supervalores

- Circular Externa 003 de 2005 (contenido)
- Circular Externa 003 de 2005 (anexo II)
- Circular Externa 010 de 2005

4.3. UIAF

- Resolución 78 de 2007 (aclaración sobre las resoluciones 141 y 142)

4.4. Entidades obligadas y normativas

4.5. Fundamentos legales sectores reportantes

5. **Normatividad internacional**

- Convención de Viena en 1988. Declaración de Principios de Basilea acordada el 12 diciembre de 1988.
- Reglamento Modelo de la CICAD aprobado por la Asamblea General de la Organización de Estados Americanos.
- Las Cuarenta Recomendaciones sobre el Lavado de Activos del Grupo de Acción Financiera (GAFI)
- Las Diez y Nueve Recomendaciones del Grupo de Acción Financiera del Caribe (GAFIC)
- Las Nueve Recomendaciones del Grupo de Acción Financiera de Sudamérica (GAFISUD)

6. **Índice normatividad**

Este libro se terminó de imprimir,
en octubre de 2014, en la planta industrial de Legis S.A.,
Av. Calle 26 N° 82-70 Tel. 4255255 A.A. 98888
Bogotá, D.C. - Colombia