Entidades Interesadas
- Miembros de AMV
- Miembros Autorregulados en Divisas
- Autoridades

Funcionarios Interesados
- Alta Dirección
- Área de Control Interno
- Revisor Fiscal
- Auditor Interno
- Áreas de Riesgo
- Contralores
- Área de seguridad de la información
- Recursos Humanos

Publicación:

2 de Octubre de 2012

Plazo para comentarios:
19 de Octubre de 2012

Información de contacto
Carlos Andrés Huertas Moreno – Supervisor Sénior
ahuertas@amvcolombia.org.co

Regulación aplicable
- Circular Básica Jurídica 007 de 2006
- Ley 599 de 2000 (CP)
- Código de Comercio
- Reglamento de AMV
- Circular Externa 041 de 2007 SARO
- Circular Externa 038 de 2009
- Statements on Auditing Standards (SAS)
- Normas de Auditoría del PCAOB
- Ley Sarbanes–Oxley de 2002
- Estándar Australiano AS-8001-2004
- Basilea III
- Guía para el Registro de Eventos de Pérdida por Riesgo Operacional de la ORX
- Normas para el Ejercicio Profesional de la Auditoría Interna del IIA

amv
Autorregulador del Mercado de Valores de Colombia

LAS MEJORES PRÁCTICAS ANTIFRAUDE:

Construyendo un Programa de Prevención y Respuesta al Fraude

RESUMEN EJECUTIVO

El Comité de Control Interno y Compliance del Autorregulador del Mercado de Valores - AMV, adelanta un estudio acerca de los principales factores (causas) de riesgo de fraude en las actividades de intermediación de valores, con el fin de proponer un modelo administración de este tipo de riesgo, que permita a los inversionistas, accionistas de las entidades, Junta Directiva, Alta Gerencia y demás partes interesadas (stakeholders), obtener seguridad razonable respecto de su identificación, medición y control, a través de la incorporación de estándares y mejores prácticas.

OBJETIVOS DEL DOCUMENTO

A partir del análisis casuístico y las lecciones aprendidas en la experiencia del Autorregulador y sus miembros, poner a consideración de la industria una propuesta acerca de un modelo eficiente de administración de riesgo de fraude, el cual incorpore estándares y mejores prácticas para su identificación, medición y control.

CONTENIDO

1. Introducción

Una de las prácticas delictivas que más afecta a las entidades del sector financiero y de valores, y que preocupa a sus accionistas, administradores y stakeholders[1] en general, es el **FRAUDE**. Práctica que lejos de estar suficientemente controlada en países como Colombia, no ha recibido la merecida atención por parte de la Alta Gerencia y/o de los diferentes órganos de control de las entidades.

Los factores de ocurrencia del riesgo de fraude, se deben principalmente por la mayor complejidad que revisten hoy en día los negocios y sus procesos, el carácter globalizado que han tomado los fondos de capital, el uso creciente de la tecnología, e incluso, las dificultades implícitas en las diferentes culturas en donde se desarrollan los negocios. Debido a estos factores los negocios financiero y de valores son percibidos bajo una sensación de mayor riesgo, tanto por los empresarios como por los usuarios.

Esta percepción no es ajena para los defraudadores, quienes han visto la oportunidad de lucrarse aprovechando la debilidad (o ausencia) de los sistemas de control interno y en particular de los sistemas de administración de riesgos.

El costo estimado del fraude en Colombia es de 4,2 billones de pesos al año. Esta cifra, de ser ajustada a la realidad implicaría mucho más. El fraude le cuesta a las empresas del país (privadas y del Estado) el equivalente de un salario mínimo mensual a una familia típica de 5 miembros[2].

De acuerdo con el Global Fraud Report, un estudio realizado en el segundo semestre de 2010 por The Economist Intelligence Unit para Kroll (una empresa de inteligencia empresarial), Colombia ocupó el segundo puesto entre los países más victimizados por el **fraude**, seguido solo por China y antecedido por Brasil. De acuerdo con este estudio, el fenómeno ha hecho que el crecimiento de las compañías nacionales se haya visto alarmantemente estancado.

Según Kroll, el 94% de los negocios colombianos encuestados sufrió algún tipo de fraude durante el 2010, en comparación con el 88% a nivel mundial, principalmente relacionados con fraude financiero y de la información. El 21% está en la categoría de fraudes electrónicos, que incluyen hurto de información y ciberataques.

---

[1] NA: Stakeholders: partes o terceros interesados (proveedores, clientes, Estado, entidades de vigilancia, control y autorregulación, etc.)

[2] Cifras del fraude y la corrupción, Alejandro Morales Tobón, El Colombiano, Publicado el 27 de marzo de 2010

El 25% de los eventos de fraude se han registrado en el sector financiero, y las áreas más críticas y susceptibles de ser objeto de algún tipo de fraude son la financiera y de tesorería, en las cuales ocurren el 70% de los casos de fraude, afirma el estudio.

Los intermediarios de valores y divisas no son ajenos a este flagelo, y por las características del negocio y su responsabilidad de administrar recursos de terceros (personas jurídicas y naturales), se hace imperiosa la necesidad de establecer al interior de las entidades un conjunto de políticas y procedimientos conducentes a la administración y mitigación de este tipo de riesgo.

Tanto las entidades como el legislador mismo en nuestro país, han escatimado esfuerzos en la mitigación y control de este riesgo, restándole importancia y dando lugar a que las entidades queden vulnerables.

La legislación penal colombiana no contempla específicamente la acepción de fraude como conducta delictiva, circunscribiéndose a la clasificación de este en dos tipos, fraude mediante cheque[3] y el fraude procesal[4].

La Circular Externa 038 de 2009[5] en su artículo 7.7.1.2.1, numeral vii define el fraude como "*(…) acto intencionado cometido para obtener una ganancia ilícita (…)*", entre tanto que la Circular Externa 041 de 2007[6] ofrece sendas definiciones para **fraude Interno**[7] y **fraude externo**[8].

Son muchas las modalidades de fraude que asechan a las entidades de intermediación de valores y divisas. Sin embargo, la experiencia ha dictado como las más comunes las siguientes: i) utilización temporal de los recursos de los clientes para cumplir operaciones no autorizadas por estos, ii) hurto o apropiación indebida de dineros de clientes, iii) utilización de dineros de clientes para encubrir pérdidas corporativas o de portafolios de terceros, iv) apropiación indebida de títulos, v) adelgazamiento recurrente de títulos en detrimento patrimonial de terceros, entre otros.

No obstante el fraude se ha convertido en una "práctica" generalizada en muchas organizaciones, en todos los casos puede prevenirse, implementando los controles adecuados o fortaleciendo los ya existentes.

---

[3] Capítulo cuarto, artículo 248, Código Penal Colombiano.
[4] Capítulo octavo, artículos 453 y 454, Código Penal Colombiano.
[5] Instrucciones respecto de la implementación del Sistema de Control Interno en las entidades vigiladas por la Superintendencia Financiera de Colombia
[6] Reglas Relativas a la Administración del Riesgo Operativo
[7] Artículo 2.6.1.1
[8] Artículo 2.6.1.2

A este propósito, el Comité de Control Interno & Compliance emprendió la iniciativa de estudiar y analizar los casos más relevantes de fraude que han ocurrido e impactado el mercado de valores, recopilando las lecciones aprendidas y generando el presente documento como una propuesta para el sector, coadyuvando con sus miembros, en el diseño, estructuración e implementación de un modelo eficiente para la identificación, medición y control del riesgo de fraude.

Comité de Control Interno & Compliance
AMV

2. Contexto Normativo y Regulatorio

Antes de entrar a identificar las causas más recurrentes de la materialización del riesgo de fraude, es propio dejar claro qué entendemos por fraude, así como su contexto normativo existente.

La palabra fraude se deriva del latín ***fraus***, ***fraudis*** (Mala fe, engaño, falsedad, malicia, astucia, perfidia), la cual a su vez se deriva del Griego ***φραδής*** (fradis; ingenioso, listo, astuto)[9].

El Fraude en el contexto Legislativo y Normativo Nacional

En la legislación colombiana no encontramos una definición específica y única que reúna o explique aquellas conductas o actividades que se pueden enmarcar dentro de la acepción de fraude.

La legislación penal Colombiana por ejemplo, no contempla específicamente la acepción de fraude como conducta delictiva, circunscribiéndose a la clasificación de este en dos tipos, fraude mediante cheque[10] y el fraude procesal[11].

En los artículos 251 al 260, capítulo sexto del Código Penal Colombiano (Ley 599 de 2000) se recogen las actuaciones que de acuerdo con el legislador, se consideran como defraudaciones. Dentro de la tipología de defraudación el Código Penal Colombiano señala:

> "Artículo 252 - *Aprovechamiento de error ajeno o caso fortuito. El que se apropie de bien que pertenezca a otro y en cuya posesión hubiere entrado por error ajeno o caso fortuito, (…)*".
>
> "Artículo 258 - *Utilización indebida de información privilegiada.- El que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, (…).*

[9] En la mitología romana, ***Fraus*** era la diosa de la traición, ayudante de Mercurio. Su equivalente griego es ***Apate***. En la mitología griega ***Apate*** era una de los ***daimones*** (Angeles y Demonios), que personificaba el engaño, el dolo o fraude. Fue, junto a su correspondiente masculino ***Dolos*** (el demonio de los ardides y las malas artes), uno de los espíritus que salieron de la ***caja de Pandora***. Ambos eran hijos de ***Érebo*** y de ***Nix***, o de ***Nix*** por ella misma, y solían estar acompañados por los ***pseudologos*** (las mentiras). Por ello tenían como daimón opuesto a ***Aleteia***, la verdad.

[10] Capítulo cuarto, artículo 248, Código Penal Colombiano.

[11] Capítulo octavo, artículos 453 y 454, Código Penal Colombiano.

(…) el que utilice información conocida por razón de su profesión u oficio, para obtener para sí o para un tercero, provecho mediante la negociación de determinada acción, valor o instrumento registrado en el Registro Nacional de Valores, siempre que dicha información no sea de conocimiento público".

Asimismo, en el Código de Comercio, artículos 72 y 74, se considera como fraude la doble contabilidad y aquellos vicios que atenten contra el principio de fe en los libros de contabilidad.

Por otra parte, la Circular Externa 038 de 2009[12] en su artículo 7.7.1.2.1, numeral vii define el fraude como "*(…) acto intencionado cometido para obtener una ganancia ilícita (…)*", entre tanto que la Circular Externa 041 de 2007[13] define como **fraude Interno[14]** los "*Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad o incumplir normas o leyes, en los que está implicado, al menos, un empleado o administrador de la entidad*", y como **fraude externo[15]** los "*Actos, realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes*".

Finalmente el artículo 49.1 del Reglamento de AMV, define como **defraudación** la obtención "*de provecho indebido para sí o para un tercero, afectando a un tercero o al mercado, en desarrollo de operaciones o actividades de intermediación*".

El Fraude en el contexto Legislativo Internacionali[16]

En el ámbito internacional es abundante la normativa y la literatura acerca del fraude, y así mismo la variedad de acepciones.

La norma internacional de auditoría SAS[17] No. 82, por ejemplo, define el fraude como:

[12] Instrucciones respecto de la implementación del Sistema de Control Interno en las entidades vigiladas por la Superintendencia Financiera de Colombia
[13] Reglas Relativas a la Administración del Riesgo Operativo
[14] Artículo 2.6.1.1
[15] Artículo 2.6.1.2
[16] Fuente "Key Elements of Antifraud Programs and Controls – a White Paper" de PricewaterhouseCooper
[17] Normas y procedimientos de auditoría emitidos por The Auditing Standards Executive Commitee del Instituto de Contadores Públicos de Estados Unidos (AICPA por su sigla en inglés)

"*(…) acto intencional, por parte de uno o más individuos del área de administración, personal o terceros, que produce una distorsión en los estados financieros. El fraude puede involucrar":*

"La manipulación, falsificación o alteración de registros o documentos.

- *La malversación (uso indebido) de recursos.*
- *La supresión u omisión de los efectos de las transacciones en los registros o documentos.*
- *El registro de transacciones sin sustentación.*
- *La aplicación indebida de las políticas de contabilidad".*

Igual acepción es considerada por el PCAOB[18] en la norma AU Sección 316A "*Consideraciones de Fraude en una Auditoría de Estados Financieros*", señalando además que para que un acto se entienda como fraude, este tiene que tener claras características de intencionalidad por parte del perpetrador.

En la SEC. 807 de la Ley Sarbanes-Oxley de 2002 (*la cual modifica el capítulo 63 del título 18, Código de los Estados Unidos*), se establece que comete fraude de valores:

"Quien con conocimiento ejecuta o intenta ejecutar, un esquema o artificio (1) para defraudar a una persona en conexión con un valor de un emisor (…) ; ó (2) para obtener por medio de pretensiones falsas o fraudulentas, representaciones o promesas, dinero o propiedad en conexión con la compra o venta de un valor de un emisor (…)"

Por otra parte, encontramos el Estándar Australiano 8001-2008[19] sobre **Control de Fraude y Corrupción**, el cual fue preparado por el Standards Australian

[18] Consejo de vigilancia de contabilidad de empresas públicas (PCAOB). El PCAOB es una entidad privada, corporación no lucrativa, creada por la Ley Sarbanes -Oxley de 2002, para supervisar a los auditores de las empresas que cotizan sus acciones en el mercado público de valores, con el fin de proteger los intereses de los inversores y el interés público.

[19] Sustituyó la norma AS 8001—2003. Los principales cambios al estándar se relacionaron con i) Cambios en la estructura y formato; ii) Consideraciones amplias sobre los sistemas de información como un habilitador de fraude y corrupción y como un medio para detectar fraude y corrupción; iii) Orientación ampliada sobre el rol sugerido en la función de la auditoría interna de controlar el riesgo de fraude y corrupción; iv) Diferentes consideraciones de corrupción y de las formas en que el riesgo de corrupción puede ser manejado; v) Énfasis en el papel ejemplar de altos gerentes como elemento importante dentro del marco de integridad de la entidad; vi) Metodología mejorada de evaluación de riesgo de fraude (alineados con los cambios al AS/NZS 4360:2004); vii) Mejoramiento en los lineamientos para el monitoreo de empleados; viii) Directrices de investigación de antecedentes a nuevos clientes y proveedores; ix) Referencia al rol de la auditoría externa en la detección del fraude.

Committee MB-004[20]. La Sección 1 "*Alcance y Generalidades*", numeral 1.1 de la norma australiana, establece que el fraude involucra la apropiación indebida de activos y/o la manipulación de los reportes financieros (internos o externos).

De forma tácita, el Estándar Australiano también considera como fraude:

- La revelación o uso de información engañosa o inexacta con el fin de ocultar o distraer actos ilícitos;
- El uso o negociación indebida de información, bien sea comprando o vendiendo información que haya conocido el perpetrador en razón de sus funciones, la cual no ha sido de público conocimiento;
- El uso indebido de la posición de los altos ejecutivo con el fin de obtener algún tipo de beneficio financiero.
- Revelación material o deliberada de la información contable y financiera con propósitos indebidos
- Sobrefacturación de bienes y servicios remitidos a clientes o usuarios.
- Asumir como utilidad, pagos recibidos por error en lugar de reconocerle un crédito al pagador.
- Evasión de impuestos.
- Lavado de activos.
- Práctica ilegal de venta o compra de acciones en bolsa con información privilegiada.
- Robo de propiedad intelectual.

En el continente Europeo encontramos que en la convergencia internacional de medidas y normas de capital (Basilea II), el Comité de Supervisión Bancaria de Basilea[21] define el fraude, clasificándolo de la siguiente manera:

Fraude Interno:

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa.

[20] Standards Australia es una organización independiente, sin fines de lucro, reconocida por el Gobierno de Australia como el pico no gubernamental organismo de normalización en Australia. Standards Australia se desarrolla a nivel internacional alineados normas australianas ® que ofrecen un beneficio neto de Australia y es el miembro australiano de ISO e IEC.

[21] El Comité de Basilea es la denominación usual con la que se conoce al Comité de Supervisión Bancaria de Basilea (BCBS, sigla de Basel Committee on Banking Supervision en inglés), la organización mundial que reúne a las autoridades de supervisión bancaria, cuya función es fortalecer la solidez de los sistemas financieros. El Comité fue establecido en 1975 por los presidentes de los bancos centrales de los once países miembros del Grupo de los Diez (G-10) en aquel momento. Normalmente se reúne en el Banco de Pagos Internacionales (en inglés BIS, BPI en Español), Basilea, Suiza, donde se encuentra su Secretaría permanente, de 12 miembros.

Fraude Externo:

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.

Así mismo, en el continente europeo se encuentra la base de datos de eventos de pérdida por riesgo operacional administrada por The Operational Riskdata eXchange Association -ORX[22], que desde el 2002 registra y consolida los eventos de pérdida materializados.

En la Guía para el Registro de Eventos de Pérdida por Riesgo Operacional de la ORX se define el fraude de manera general como "*pérdidas obtenidas debido a transacciones fraudulentas*", y establece ciertas características que deben considerarse para establecer el acto como fraude, así:

- La intención de frustrar u omitir los controles;
- Involucran la violación flagrante de las normas o políticas internas de la Entidad, el código de conducta o de gobierno, así como los límites y/o actividades individuales permitidos;
- La Entidad es en última instancia la victima, sea directa o indirectamente;
- Hay algún beneficio personal; este beneficio no necesariamente tiene que ser financiero (Ej. Ocultar el mal desempeño, etc.);
- En algunos casos el beneficiario puede ser un amigo o familiar del perpetrador;
- Puede incluir el desconocimiento o sobrepaso de la autoridad interna – overstepping (Exceder límites internos como el stop loss, límites de crédito, atribuciones de compras, límites de negociación, etc.).

En la citada guía de la ORX, también se define el fraude interno y externo, como sigue:

Fraude Interno: Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad o incumplir normas o leyes, en los que está implicado, al menos, un empleado o administrador de la entidad.

[22] ORX es una asociación industrial sin fines de lucro dedicada al avance de la medición y gestión del riesgo operacional en la industria global de servicios financieros. Fue fundada en 2002 con el objetivo principal de crear una plataforma para el intercambio seguro y anónimo de datos de alta calidad respecto de los eventos de pérdida por riesgo operacional. Cuenta con 61 firmas miembro, correspondientes a las entidades financieras más importantes en 18 países, tales como Austria: EE.UU, Reino Unido, España, Canadá, Francia, Australia, Alemania, Austria, Italia, Suecia, Singapur, entre otros. ORX tiene su sede en Zúrich, Suiza.

Fraude y Hurto Interno: Pérdidas debido a actos cometidos con la intención de defraudar, malversar activos y/o propiedad, o sortear regulaciones, la ley o las políticas de la compañía, excluir o discriminar eventos, en los cuales se vea involucrado al menos un empleado de la compañía.

Así mismo, la ORX menciona a modo de ejemplos de fraude interno, los siguientes:

- Soborno
- Contrabando
- Práctica ilegal de venta o compra de acciones en Bolsa con información privilegiada (Insider Trading/dealing)
- Noticia de eventos de fraude externo perpetrado con la participación de un empleado de la compañía.

El Comité de Basilea y la ORX (Operational Risk Exchange Association) mencionan en su definición, que al menos una persona o empleado interno de la compañía debe estar involucrado para considerar el evento como Fraude Interno.

- El empleado o funcionario debe haber hecho uso de su posición en la compañía, o de su acceso a los activos o a la información, para llevar a cabo el fraude.
- Esta definición incluye también a los empleados temporales o por contratos de servicios.
- También incluye empleados de otras compañías que se encuentran bajo la supervisión directa de un funcionario de la compañía, o que estén vinculados bajo una relación contractual.

El fraude interno es originado dentro de la empresa, y deber ser plena y acertadamente identificada la naturaleza de interno, de lo contrario será considerado como fraude externo.

Dentro de las actividades no autorizadas (malintencionadas) la ORX incluye:

- Transacciones no reportadas (intencionalmente)
- Transacciones no autorizadas (que involucren pérdida monetaria)
- Colocación intencionada de malas posiciones en el mercado

Fraude Externo: Actos realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

Fraude y Hurto Externo: Pérdidas debido a actos cometidos con la intención de defraudar, malversar activos y/o propiedad, o incumplir la ley por parte de terceras personas. Este tipo de fraude también pude ser perpetrado con la asistencia o complicidad de al menos un empleado interno de la entidad.

Son Ejemplos de fraude externo:

- Depósitos sin valor o ficticios (sin fondos).
- Robo / extorsión / desfalco.
- Apropiación de activos.
- Falsificación.
- Cheques alterados o sin fondos (Check Kiting)
- Sustitución o suplantación de cargos.

De acuerdo a las Normas para el Ejercicio Profesional de la Auditoría Interna del IIA, el fraude es cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios, o para asegurarse ventajas personales o de negocio.

Definición general de fraude

Finalmente, como resultado del análisis de las diferentes normas, modelos y estándares para prevención y administración del riesgo de fraude, así como las definiciones que para fraude de ellas se desprende, es propio establecer, con el propósito de no caer en errores o malas interpretaciones, una única aserción, siendo esta la siguiente:

Fraude es cualquier acto ilegal caracterizado por ser un engaño, ocultación o violación de confianza, que no requiere la aplicación de amenaza, violencia o de fuerza física, perpetrados por individuos y/u organizaciones internos o ajenos a la entidad, con el fin de apropiarse de dinero, bienes o servicios, procurarse ventajas o beneficios individuales, mediante la frustración u omisión de controles, la violación flagrante de las normas o políticas internas de la Entidad, el código de conducta o de gobierno, así como los límites y/o actividades individuales permitidos, la defraudación, malversación de activos y/o propiedad, soborno, contrabando, práctica ilegal de venta o compra de acciones en Bolsa con información privilegiada (Insider Trading/dealing). Así mismo, se entiende por fraude las prácticas no apropiadas relacionadas con:

- La revelación o uso de información engañosa o inexacta con el fin de ocultar o distraer actos ilícitos;
- El uso o negociación indebida de información, bien sea comprando o vendiendo información que haya conocido el perpetrador en razón de sus funciones, la cual no ha sido de público conocimiento;
- El uso indebido de la posición de los altos ejecutivo con el fin de obtener algún tipo de beneficio financiero.
- Revelación material o deliberada de la información contable y financiera con propósitos indebidos;
- Sobrefacturación de bienes y servicios remitidos a clientes o usuarios;
- Evasión de impuestos;
- Lavado de activos.

Una vez unificado el concepto de fraude, el Comité de Control Interno & Compliance efectuó un análisis casuístico y de las lecciones aprendidas en la experiencia del Autorregulador y sus miembros en esta materia, y se identificaron conjuntamente los principales factores de riesgo que permitieron la materialización del mismo y el consecuente impacto sobre el estado de resultados y/o sobre los procesos de la entidad.

3. Problemática (Factores de Riesgo de Fraude)

Producto del análisis casuístico y de las lecciones aprendidas en la experiencia del Autorregulador y sus miembros, el Comité de Control Interno & Compliance identificó los factores comunes y recurrentes en la materialización de los eventos de riesgos de fraude.

Dentro de las modalidades de fraude más comunes identificadas por el Comité se encuentran:

- Utilización temporal de los recursos de los clientes para cumplir operaciones de posición propia o de terceros,
- El hurto o apropiación indebida de dineros de determinados clientes
- Utilización de dineros de clientes para encubrir pérdidas de la posición propia
- Apropiación indebida de títulos
- Adelgazamiento recurrente de títulos en detrimento patrimonial de terceros
- La revelación o uso de información engañosa o inexacta con fines de ocultamiento o distracción de actos ilícitos;
- Uso o negociación indebida de información privilegiada y/o confidencial;
- El uso indebido de la posición de los altos ejecutivo con el fin de obtener algún tipo de beneficio financiero.
- Revelación material o deliberada de la información contable y financiera con propósitos indebidos;

- Lavado de activos

La lista anterior incluye aquellos eventos de fraude más comunes y no se trata de un dossier de los diferentes tipos, toda vez que las entidades y sus procesos pueden verse vulnerados por un sinnúmero de modalidades.

A continuación se describen los factores de riesgo que de acuerdo con el análisis hecho por el Comité, se constituyen en los factores más comunes en la realización de los diferentes tipos de fraude.

3.1 Inadecuada segregación de funciones

La segregación de funciones es una de las principales actividades de control interno destinada a prevenir o reducir el riesgo de errores o irregularidades, y en especial el fraude interno en las organizaciones. Su función es la de asegurar que un individuo no pueda llevar a cabo todas las fases de una operación/transacción, desde su autorización, pasando por la custodia de activos y el mantenimiento de los registros maestros necesarios. Se daría una adecuada segregación de funciones cuando para realizar una acción fraudulenta o irregularidad se requiera la confabulación de dos o más empleados.

La inadecuada segregación de funciones entre las áreas de inversiones, incrementa el riesgo de que los funcionarios estén en condiciones tanto de cometer u ocultar errores como de perpetrar fraudes en el transcurso normal de su trabajo.

3.1.1 Factores/Causas

Las causas más relevantes que se han identificado, relacionadas con la segregación de funciones son:

- Los funcionarios del Front Office ejecutan actividades de otras áreas relacionadas, como es el caso del Middle y Back Office. Esto incrementa el riesgo de error y ocultamiento de errores.

- Los funcionarios del Front Office tienen acceso a información confidencial y/o privilegiada de otras áreas relacionadas como en el caso del Middle y Back Office. Esto incrementa el riesgo de uso indebido (utilización o venta) de información para el beneficio propio o de terceros.

- Los controles relacionados con límites y cupos (de contraparte, por operador, globales, individuales, etc.) son establecidos y ejecutados directamente por los funcionarios del Front Office.

- Los funcionarios del Front y/o del Middle office llevan a cabo el proceso de valoración de los portafolios, incrementando el riesgo de ocultamiento, alteración de información, y fraude.

- Funcionarios del área comercial que entregan información de operaciones (Extractos, estados de cuenta, papeletas de bolsa, etc.) directamente a los clientes, generando extractos o papeletas de bolsa adulterados, información falsa o inexacta a los clientes.

- Adulteración de soportes, papeletas de bolsa, órdenes físicas, extractos, etc. Casos en los que el comercial involucrado (trader), es quien recibe y entrega las papeletas de bolsa y/o los extractos de cuentas a los clientes, presentándose situaciones de adulteración de los extractos y la información del portafolio de clientes.

- Órdenes de giro de cheque a clientes generadas por el comercial.

- Desvío de dineros de clientes para el pago de obligaciones y acreencias del comercial que administra las cuentas de clientes.

- Concentración de funciones relacionadas con la elaboración de cheques a clientes, cruces restrictivos, levantamiento de sellos, medios de pago (cheque, efectivo, transferencias), restricciones de pago y/o giro, horarios de pago, conceptos, órdenes de giro por cuenta de los clientes, etc.

3.1.2 Mejores Prácticas

Las mejores prácticas señalan que las funciones que al menos deben encontrase disgregadas son: autorización, ejecución, registro, custodia, y realización de conciliaciones.

Para el caso del área de inversiones es prudente que exista una independencia estructural y funcional entre las áreas de Front, Middle y Back Office, dependiendo estas incluso de áreas funcionales diferentes[23].

[23] CE 100 de 1995, Capítulo XXI, artículo 6.2 literal c) Garantizar que en las actividades de tesorería exista una separación clara, organizacional y funcional, entre las actividades de trading, monitoreo y control; de

A continuación, las actividades que de acuerdo con las mejores prácticas deben realizar independientemente las áreas relacionadas con la intermediación de valores/divisas:

3.1.2.1 Front Office

Las áreas de negociación o Front Office, son las encargadas de tomar los riesgos de acuerdo a la estrategia que se haya definido y dentro de los límites que tengan establecidos. Independientemente del tipo de actividad que desarrollen, las funciones genéricas de las áreas de negocio en materia de control de riesgo, son las siguientes:

- Materializar la estrategia de gestión de riesgos de la entidad en posiciones reales de mercado en los diferentes negocios.
- Maximizar la rentabilidad para cada nivel de riesgo aceptado.
- Proponer al comité de riesgos, a través de área de análisis y control de riesgos, nuevas oportunidades de negocio (productos/mercados) para su aprobación e incluso en la política de gestión de riesgos de la organización.
- Proponer al área de análisis y control de riesgos los niveles de límites de riesgo de mercado y crédito necesarios para desarrollar su actividad y cumplir los objetivos establecidos.
- Realizar un seguimiento de las mediciones de riesgos realizadas por el área de análisis y control de riesgos.
- Distribuir los límites de riesgos generales en sublímites dentro de la estructura de actividad que desarrollan.
- Realizar informes de gestión en los que analicen los resultados obtenidos en función de los objetivos fijados y los riesgos asumidos.
- Implantar y cumplir las políticas, metodologías y procedimientos definidas por el comité de riesgos.

3.1.2.2 Middle Office

El análisis y control de riesgos es el departamento operativo en el cual el comité de riesgos delega las actividades diarias de análisis y control de los riesgos (mercado y crédito) asumidas por la entidad. Por tanto, las tareas que desarrolla el área de análisis y control de riesgos pueden ser agrupadas en torno a sus funciones básicas:

---

procesamiento y contabilidad. Lo anterior para que éstas sean independientes entre sí y dependan de áreas funcionales diferentes. Para ello es necesario que las operaciones de tesorería se desarrollen dentro de una estructura organizacional conformada por las siguientes áreas y/o funciones: back office, middle office y front office.

- Analizar los límites propuestos por las áreas de negocio y el área GAP.
- Analizar el reparto del capital en riesgo entre las unidades y realizar propuestas alternativas de límites al comité de riesgos.
- Medir los riesgos según las metodologías aprobadas y controlar el cumplimiento de los límites.
- Calcular los resultados de gestión y el RORAC[24] de las diferentes áreas de negocio.
- Implantar y asegurar el cumplimiento de las políticas, metodologías y procedimientos definidos por el comité de riesgos.
- Preparar los informes para el comité de riesgos.
- Preparar información sobre gestión de riesgos destinada a agentes externos.

3.1.2.3 Áreas de Soporte (Back Office, sistemas, jurídico, RRHH, Auditoría Interna)

Las áreas de soporte desarrollan un conjunto de actividades que son necesarias para la implantación de la estrategia y las políticas de control y gestión de riesgos dentro de la entidad. A continuación se indican las funciones concretas, que en materia de control y gestión de riesgos, asumen cada una de las áreas de soporte:

3.1.2.3.1 Administración y Áreas de Operaciones (Back Office)

- Procesar (registrar, confirmar, liquidar, etc.) todas las operaciones contratadas por las áreas de negocio, cumpliendo en todo momento las políticas, metodologías y procedimientos de control de riesgos establecidos por el comité de riesgos.
- Contabilizar todas las operaciones de acuerdo a las normas y criterios definidos por los reguladores.
- Asegurar la integridad de las bases de datos de operaciones, las cuales serán también utilizadas por el área de análisis y control de riesgos.
- Asegurar que se cumplen los controles y procedimientos establecidos para reducir el riesgo operativo e informar al comité de riesgos de los errores y discrepancias detectados.

3.1.2.3.2 Área de Tecnología y Sistemas

- Desarrollar, instalar y mantener los sistemas necesarios para que todas las áreas de la entidad puedan desempeñar las funciones relacionadas con la gestión y el control de riesgos.
- Establecer los controles informáticos definidos en las políticas de riesgo operativo.

[24] Rentabilidad de la posición respecto al capital en riesgo.

- Controlar la correcta utilización de los sistemas informáticos y garantizar la integridad y el funcionamiento correcto de los mismos.
- Definir el plan de contingencia de sistemas.

3.1.2.3.3 Área de Asesoramiento Jurídico-legal y Fiscal

- Definir y establecer los procedimientos necesarios para poder controlar adecuadamente el riego legal de la entidad.
- Garantizar que toda la operativa cumple las reglas y las leyes establecidas por la regulación y la normativa aplicable (compliance)
- Controlar que todas las operaciones son correctamente documentadas en tiempo y contenido y evitar la pérdida de dicha documentación.
- Analizar y redactar los contratos que soportan las operaciones realizadas por las áreas de negocio.
- Controlar que se cumple adecuadamente toda la normativa existente en materia de impuestos.

3.1.2.3.4 Área de Recursos Humanos y Capacitación

- Definir e implantar políticas de selección y planes de capacitación que garanticen que todas las funciones de las áreas relacionadas con la intermediación de valores/divisas, así como las de control y gestión de riesgos, son desempeñadas por profesionales apropiados, en número, experiencia, habilidades y grado de especialización.
- Seleccionar al personal adecuado en función de las solicitudes de las diferentes áreas de la entidad.
- Llevar a cabo procedimientos y estudios de seguridad, especialmente para aquellos cargos sensibles de la entidad y susceptibles del riesgo de fraude.
- Considerar la opción de incluir un estudio poligráfico para aquellos cargos de responsabilidad, especialmente de manejo de recursos como es el caso de la tesorería o áreas de operaciones que custodian títulos y valores.
- Definir e implantar políticas de remuneración e incentivos que sean adecuadas a los perfiles que se requieren en los diferentes estamentos de la entidad y no fomenten conductas incoherentes con las políticas de conducta, ética, control y riesgo establecidas.
- Definir y asegurar el cumplimiento del código de conducta de la entidad.

3.1.2.3.5 Área de Auditoría Interna

- Examinar y valorar regularmente, de forma independiente, la idoneidad y efectividad del sistema de control interno de las áreas relacionadas con la intermediación de valores/divisas (sin despreciar las demás áreas de la entidad).

- Contrastar la implantación real de políticas y procedimientos establecidos.
- Controlar que todas las operaciones están correctamente registradas, valoradas y contabilizadas, y que se está cumpliendo toda la normatividad y criterios contables establecidos por los reguladores.
- Informar al comité de auditoría de cualquier debilidad relevante que se haya detectado como consecuencia de los análisis realizados, y proponer soluciones alternativas.

3.1.2.4 Recomendaciones de los estándares internacionales sobre estructura organizativa

A continuación se mencionan algunas de las recomendaciones de los estándares internacionales respecto del control y gestión de riesgos. Dentro de las organizaciones que emiten tales recomendaciones se encuentran, El Grupo de los Treinta, Grupo sobre Políticas para Instrumentos Financieros Derivados, Banco de Pagos Internacionales,

3.1.2.4.1 Recomendaciones del Grupo de los Treinta

- Las políticas y procedimientos de las áreas de negociación, riesgos y de las áreas de apoyo (Back Office, Sistemas, RRHH, Auditoría Interna, etc.) deben estar actualizadas, de forma que observen los cambios en el mercado y en la propia entidad.
- La Alta Dirección debe aprobar los procedimientos y controles necesarios para garantizar la implementación de las políticas, y el resto de la organización debe cumplirlos.
- Las entidades deben disponer de un área de control de riesgos independiente, la cual debe tener las siguientes responsabilidades, entre otras:

    - Desarrollar políticas para establecer límites de riesgo y controlar su cumplimiento.
    - Revisar y aprobar los modelos de valoración utilizados por las áreas de negociación (Front Office) y operaciones (Back Office), así como definir procedimientos de conciliación, si los sistemas utilizados por dichas áreas son diferentes.

3.1.2.4.2 Recomendaciones del Grupo de Políticas para Instrumentos Financieros Derivados

- Las entidades deben contar con un documento que recoja las políticas y procedimientos relacionados con las funciones y responsabilidades a ser

ejecutadas en cada una de las áreas relacionadas con la intermediación de valores/divisas, así como de las actividades de control establecidas.
- Las entidades deben requerir periódicamente una revisión independiente (auditoría externa) para garantizar que las políticas de gestión de riesgo están siendo adoptadas y los procedimientos de control están establecidos.

3.1.2.4.3 Recomendaciones del banco de Pagos Internacionales

- Definir políticas y procedimientos apropiados a la naturaleza y complejidad de los negocios en los que operan.
- Las entidades deben contar con una unidad, independiente de las unidades de negocio, que debe ser la responsable del diseño, administración e implementación de las políticas y procedimientos de las áreas relacionadas con la intermediación de valores/divisas, así como de las áreas de control y gestión de riesgos.
- Las entidades deben someterse periódicamente a auditorías internas y externas de las políticas, metodologías y sistemas empleados para el control interno y gestión de los riesgos.

3.2. Ausencia de un adecuado ambiente de control y debilidad en las políticas y procedimientos para la realización de operaciones

Como parte de la adecuada alineación de los objetivos de proceso/áreas funcionales con los objetivos corporativos de la entidad, es imperativa la necesidad de contar con un ambiente de control adecuado, enmarcado por el tono de la Alta Gerencia y su posición frente a las prácticas inapropiadas. Así mismo, es importante que la entidad defina y estructure políticas y procedimientos que guíen las funciones y responsabilidades del personal de la entidad hacia la consecución de los objetivos.

La deficiencia (o ausencia) de políticas y procedimientos que enmarquen y definan las responsabilidades de los funcionarios en las áreas de inversiones (Front, Middle y Back Office), pueden ocasionar errores en la ejecución de las operaciones, la definición de los controles, en el registro de las operaciones, transacciones y transformaciones, así como deficiencia en los procesos, incumplimiento de los objetivos corporativos, incumplimiento de normas y regulaciones, e información inexacta, incompleta, y poco confiable.

3.2.1 Factores/Causas

La experiencia indica las siguientes, como las causas más relevantes relacionadas con la defraudación producto de la debilidad del sistema de control, y en

particular en el ambiente de control, esto es, en la definición de políticas y procedimientos:

- La entidad carece de políticas, procedimientos, mecanismos y herramientas para la remisión de información exacta, integra, oportuna y confiable a los clientes, relacionada con sus estados de cuentas, operaciones, resultados, etc., y en donde se les ponga al tanto de los canales establecidos y los funcionarios y/o áreas responsables de la emisión de este tipo de información.

  Tal situación genera la probabilidad de suplantación por parte del comercial de funcionarios de otras áreas, tales como las de control, correspondencia, back office, entre otros. El comercial, mediante la creación de cuentas de correo electrónico envía mensajes a los clientes dando parte de tranquilidad respecto de las inquietudes que estos puedan tener (inconsistencias en sus portafolio, operaciones o transacciones no autorizadas, pérdidas injustificadas, etc.), haciéndose pasar por un funcionario de la auditoría interna.

- Ausencia de políticas y/o procedimientos adecuados relacionados con la ejecución de operaciones y verificación de la veracidad de las órdenes por parte de los clientes, tales como el visado de firmas, confirmación directa con los clientes, etc., lo que ha generado prácticas inapropiadas como la suplantación de clientes por parte de los comerciales a través del escaneo y/o falsificación de firmas registradas con el fin de efectuar retiros de dineros, transferencias electrónicas de fondos a cuentas de terceros, entre otras.

- Ausencia de procedimientos que indiquen claramente la manera y los medios que los clientes deben y pueden utilizar para impartir a los comerciales las respectivas órdenes de operación. Esta debilidad ha dado pie a que comerciales mediante correos electrónicos enviados al Back Office, ordenen el traslado de fondos entre clientes con el fin de encubrir pérdidas, sustentados en una supuesta (no cierta) orden telefónica impartida por un cliente y sobre la cual no existe evidencia física (grabada o escrita).

- No existen políticas y/o procedimientos (o estos son insuficientes) respecto de la asignación de los recursos consignados por los clientes o terceros, en las cuentas bancarias del intermediario. En consecuencia, los recursos son aplicados a cuentas indicadas por el comercial a través de un correo electrónico o de manera verbal al área de tesorería, soportando el registro con fotocopias o imágenes escaneadas de los comprobantes consignación, las cuales presentan información borrosa o adulterada.

- No se han definido procedimientos claros ni responsables del mantenimiento y actualización de la información de los clientes. A este respecto, se identifican casos en los cuales los comerciales son quienes se encargan de recaudar y actualizar la información de los clientes, tal como: dirección de correspondencia, correos electrónicos, teléfonos, nombres de contactos, números de cuentas bancarias y ordenantes, etc. No se evidencian controles de confirmación de la veracidad, certeza y exactitud de la información de los clientes reportada por los comerciales.

- Ausencia (o debilidad) de políticas y procedimientos relacionados con las situaciones generadoras de conflicto de interés, actuaciones prohibidas al personal, manejo de información privilegiada, relaciones con los clientes, conductas relacionadas con limitación de regalos y atenciones recibidas, entre otros.

- No se ha definido un nivel adecuado de autorizaciones conforme a las características particulares de los procesos y de las operaciones. Representa el riesgo de que se realicen operaciones que no estén explícita y completamente autorizadas en todos sus términos dentro del marco operativo de la entidad.

- Procedimientos inadecuados relacionados con el procesamiento de las operaciones. Conllevan el riesgo de errores o fallas de control en una o varias de las siguientes fases del procesamiento de las operaciones:

    - Registro: operaciones que no se registren, o son registradas de forma incorrecta, originando información errónea y para la toma de decisiones.
    - Cálculo de la posición: existencia de diferencias, no detectadas, entre la posición reportada por las áreas de negociación (Front Office) y las áreas de control.
    - Confirmación: en el proceso de confirmación no se detectan, tanto datos erróneos de las operaciones registradas, como operaciones no registradas.
    - Liquidación: los activos financieros no son recibidos o entregados en las fechas establecidas, o lo sean de forma incorrecta.
    - Acceso físico: el efectivo u otros activos (valores, cheques, etc.) sean accesibles a personal de la entidad no autorizado.
    - Acceso a los sistemas: personal no autorizado de la entidad o externo puedan consultar o modificar información contenida en los sistemas.

  - Valoración: errores en la valoración como consecuencia de la utilización de información o modelos erróneos, o para ocultar pérdidas o registra utilidades no realizadas.
  - Contabilización: registros contables incorrectos de las operaciones de acuerdo a las normas existentes, alteración de los registros contables.

- El personal de la entidad, de forma intencionada o no, incumple las políticas, procedimientos y controles establecidos.

- Ineficiencias, errores o prácticas no adecuadas en la ejecución y procesamiento de las operaciones debido a la ausencia de personal adecuado e idóneo, insuficientemente capacitado o a altas rotaciones.

- Ausencia o insuficiencia de políticas sobre fraude y conflicto de intereses. El personal de la entidad actúa anteponiendo sus intereses particulares a los intereses de la entidad.

- Existencia de remuneraciones variables calculadas como un porcentaje de los resultados (bonos) en algunas áreas de negocio (Front office, Tesorería, etc.). Esta práctica en particular, podría derivar en algunos casos de asunción de riesgos importante por parte de los operadores, ya que estos saben que si la apuesta les sale bien la entidad va a tener un buen resultados y ellos van a percibir una comisión proporcional a dicho resultado, mientras que si la apuesta no resulta, la entidad va a sufrir una pérdida y ellos van a seguir percibiendo la parte fija de su remuneración.

3.2.2 Mejores Prácticas

Las mejores prácticas señalan que es importante que las entidades, en cabeza de la Junta Directiva y la Alta Gerencia, definan y estructuren un adecuado ambiente de control, entendido este como el tono de la organización en relación con el entendimiento, la conciencia y comportamiento de su gente. Es el fundamento de los demás componentes de control interno, se compone de integridad, valores éticos y las competencias de las personas, la asignación de autoridad y responsabilidad (responsabilidades y funciones).

Este componente exige, en primera instancia, la elaboración y adopción formal de un código ético y reglas de conducta que generen conciencia y cultura del control interno entre los funcionarios de la entidad.

Dentro de los elementos con los cuales se crea un ambiente de control adecuado, se encuentran:

- **Filosofía del trabajo:** Política de Calidad, Código de Conducta, Manual de Inversiones, política antifraude.

- **Fundamentos empresariales:** Misión y Visión, Propósitos (Objetivos Estratégicos)

- **Organización del trabajo:** Estructura organizacional, Cadena de Valor, desarrollo de competencias, canales de información, planeación y evaluación de la gestión, Circulares normativas e informativas, Manuales de Funciones.

- **Cultura:** Valores empresariales, compromiso social (con los funcionarios, Clientes, comunidad y medio ambiente).

3.2.2.1 Código de Conducta

A través de esta política la entidad debe definir las normas y conductas que todos los empleados, en todas y cada una de las áreas de la organización, deben seguir en el transcurso de sus actividades diarias de forma que se eviten errores o prácticas no apropiadas y se salvaguarde la rectitud e integridad de la entidad, fomentando así la confianza pública en la misma.

Este código debe ser definido y aprobado y cada miembro de las áreas de la entidad, debe firmar un documento en donde manifiesten el conocimiento de su contenido, así como su compromiso a cumplirlo.

El código de conducta debes establecer las normas de obligado cumplimiento para todos los empleados de la entidad en relación con los siguientes aspectos:

- **Independencia:** el personal, especialmente aquellas de áreas sensibles como es el caso de tesorería, no puede tener intereses financieros o inversiones en las entidades con las que existen relaciones derivadas de la actividad del área, y que pudiesen suponer una falta de objetividad en el desarrollo de las operaciones.

- **Utilización de información confidencial:** establecer normas que prohíban que los empleados develen a terceros información confidencial, entendida esta como toda aquella información no pública que se maneja como consecuencia de la actividad habitual de la respectiva área a la que pertenece el empleado.

- **Conflicto de intereses:** normas que eviten y regulen los conflictos de interés que puedan surgir entre las diferentes áreas de la organización, y en particular entre la tesorería y las demás áreas, clientes, y en general, terceras partes.

- **Utilización del nombre de la entidad:** normas relacionadas con la prohibición de que ningún funcionario o empleado pueda utilizar el nombre de la entidad para realizar operaciones para las cuales no está autorizado.

3.2.2.2 Niveles de autorización

A través de esta política la alta dirección debe establecer las responsabilidades y autoridades asociadas a las responsabilidades y perfiles de los funcionarios respecto del procesamiento de operaciones de tesorería. Algunos de los aspectos que de acuerdo con las mejores prácticas, se deben regular a través de esta política son los siguientes:

- Quién puede autorizar errores operacionales y hasta que volumen
- Quién puede autorizar las correcciones de las operaciones (registros) derivadas de errores o de hechos deliberados
- Quién puede autorizar y firmar la liberación de órdenes de pago

3.2.2.3 Política Antifraude

Para el Comité de Control Interno & Compliance resulta importante que dentro del proceso de administración de riesgos de las entidades (como elemento del sistema de control interno), estas incorporen y presten especial atención a la definición de mecanismos y herramientas que permitan la prevención y/o mitigación del riesgo de fraude tanto interno como externo, teniendo en cuenta que la industria a través de la Circular Externa 038 de 2009 emitida por la Superintendencia Financiera de Colombia ha adoptado un modelo de control interno sujeto a los principio y directrices del modelo COSO.

Para el efecto es importante que las entidades definan y estructuren un "Programa antifraude", donde la alta Gerencia tenga la responsabilidad antifraude, el comité de Auditoría provea soporte en los esfuerzos antifraude y la Auditoría interna, o quien haga sus veces, sirva como una línea crítica de defensa en contra del fraude con un enfoque de riesgo - monitoreo así como también en la prevención y detección del mismo.

Si bien es cierto en los diferentes procesos existen normas y políticas que ayudan a mitigar el riesgo de fraude (Código de Conducta, Plan de vacaciones, control sobre información, perfiles de usuario, etc.), no existe bajo una única forma la

política antifraude, la cual el Comité de CI&C considera debe liderar la Presidencia de las entidades. Por lo general en la práctica, el tema de investigación del fraude es de tipo correctivo ya que una vez conocido el evento se procede a una investigación y ajuste de las fallas cometidas en el proceso.

Es por lo anterior que las entidades procuran el establecimiento de un proceso estándar y una política antifraude ya sea a través de una circular normativa, manual, cartilla, etc., en donde se fije la directriz de la entidad frente al tema (cero tolerancia al fraude), así como procedimientos para responder ante fraudes, investigaciones, reportes, monitoreo, mejores prácticas y cumplimiento.

En algunas entidades, entre otros, se está utilizando la denominada " HOTLINE" o línea ética, la cual bien manejada ha sido de gran utilidad en el tema de reportes de fraudes.

Todo lo anterior debe estar encaminado a la toma de acciones disciplinarias y penales en contra de los infractores, la recuperación y/o restablecimiento de pérdidas, y lecciones aprendidas para mejorar controles y prevenir recurrencia.

3.2.2.4 Otras políticas de Tesorería

- Operativa fuera de la sala de tesorería: las operaciones de tesorería deben efectuarse solo en la sala o mesa de negociación, con el fin de aprovechar la seguridad, la información disponible y la grabación de las conversaciones telefónicas.
- Prácticas inaceptables: definir explícitamente aquellas acciones o prácticas que se consideren inaceptables dentro de la actividad de tesorería, así como los controles necesarios para identificarlas y erradicarlas.

3.3 Ausencia o fallas en las actividades de control

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se lleven a cabo las instrucciones de la dirección de la entidad. Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la organización. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones.

Deben establecerse y ajustarse políticas y procedimientos que ayuden a conseguir una seguridad razonable de que se llevan a cabo en forma eficaz las acciones consideradas necesarias para afrontar los riesgos que existen respecto a la consecución de los objetivos de cada unidad de negocio.

3.4.1. Factores/Causas

Como factores/causas de la materialización del riesgo de fraude en las actividades de intermediación, se encuentran:

- Acceso de personas no autorizadas a ciertas funciones de los sistemas de tesorería, lo que les permitiría leer, alterar, añadir o borrar información existente en las bases de datos, o introducir transacciones no autorizadas para su procesamiento.

- La responsabilidad sobre los controles de seguridad y las claves de acceso a los sistemas de las áreas relacionadas con la intermediación de valores/divisas reposa sobre un funcionario de estas mismas áreas.

- No se han definido perfiles de acceso a los sistemas de información, o los funcionarios de las áreas relacionadas con la intermediación de valores/divisas cuentan con perfil administrador y acceso ilimitado a todos los niveles.

- El mantenimiento y actualización de las bases de datos que contiene información de clientes u otra relacionada con temas de intermediación de valores/divisas no tiene un responsable específico o este pertenece a las áreas usuarias de esta información.

- No existe control sobre las boletas de bolsa que no son imputadas directamente en los sistemas de back office desde los sistemas del Back Office.

- Utilización de celulares y mecanismos no grabados en las mesas de negociación. Permitir el uso de mecanismos no grabados en las mesas de negociación no sólo contraviene las normas existentes, también afecta la integridad, transparencia y trazabilidad de las operaciones realizadas.

- No existen políticas para el mantenimiento y conservación de las grabaciones de conversaciones por un período razonable o de acuerdo con las normas legales establecidas.

- Las áreas de control y gestión de riesgo no adelantan revisiones periódicas de las grabaciones de conversaciones.

- Los sistemas de información en las áreas relacionadas con la intermediación de valores/divisas no cuentan con controles automáticos que aseguren la integridad, exactitud y precisión de los datos.

- No se llevan a cabo procedimientos de conciliación para la transferencia de datos entre sistemas.

- Fallas o ausencia de un procedimiento de conciliación de las cuentas bancarias depositarias de los recursos propios y de clientes, los saldos de cartera, los portafolios propios y de clientes, y la cuenta puente, así como de procedimientos de monitoreo al proceso por parte de la Alta Gerencia.

- Ausencia o insuficiencia de políticas y controles relacionados con la salvaguarda de los recursos propios y de clientes, incluyendo adecuados niveles de revisión y aprobación.

- Ausencia o deficiencia en las políticas y procedimientos de tesorería y salvaguarda de los recursos propios y de clientes.

- Fallas en el reporte de estados de cuenta y remisión de información a los clientes.

- Fallas o ausencia de procedimientos para el control del flujo diario de caja, y liquidez del intermediario para atender sus compromisos de corto y mediano plazo.

- Fallas o ausencia de controles (políticas y procedimientos) que aseguren razonablemente el cumplimiento de las normas y regulaciones, la eficiencia de los procesos y la confiabilidad de la información.

- Fallas o ausencia de procedimientos de gestión por parte de la SCB o el corredor para recuperar oportunamente los saldos débitos cumplidos (cuentas por cobrar a clientes).

3.4.2 Mejores Prácticas

A continuación se describen algunas mejores prácticas que las entidades podrían implementar en el área de tesorería, y así disminuir la probabilidad de materialización del riesgo de fraude u otras prácticas no apropiadas.

3.4.2.1 Procedimientos y controles en el Front Office

- Separación entre los operadores de posición propia y los que operan posiciones por cuenta de terceros, definiéndose procedimientos que aseguren la independencia de ambas actividades.
- Comprobar que las operaciones se realicen con contrapartes (intermediarios) autorizados por la entidad.
- Para los instrumentos en que no exista un precio de mercado de referencia, utilizar modelos de valoración previamente validados por el área de riesgos.
- Cerrar operaciones que son aceptables y que cumplen con todos los límites y autorizaciones requeridos.
- Registrar toda la información necesaria de las operaciones en el LEO
- Enviar las boletas originales al Back office para que este inicie el procesamiento de las operaciones y archivar una copia en el Front Office.
- A la hora del cierre, preparar informes de final de día con la posición y los resultados donde se deben incluir todas las operaciones realizadas durante el día.
- Definición de un control diario de la liquidez de la SCB, y su capacidad para atender compromisos de corto y mediano plazo

3.4.2.2 Procedimientos y controles en el Back Office

- Revisar la información de las operaciones, verificando que todos los datos pertinentes estén incluida en los registros, y que el operador sea el autorizado para operar el producto.
- Comparar los precios o tipo utilizados en las operaciones con fuentes independientes, con el fin de asegurarse que todas las operaciones han sido realizadas a precios de mercado o tipo.
- Identificar diariamente todas las operaciones que requieren una orden de pago y obtener todos los datos de las operaciones a liquidar.
- Preparar las órdenes de pago para que estas sean autorizadas por el responsable.
- Archivar una copia de la orden de pago con los otros documentos de la operación.
- Enviar un registro de pagos al área encargada de gestionar las cuentas de bancos correspondientes.
- Efectuar conciliaciones de posiciones, de clientes, de cobros y/o pagos, bancos, registros contables.

3.3 Fallas en el monitoreo de los procesos y los controles establecidos

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo

del tiempo. Todo el proceso debe ser supervisado, introduciéndose las modificaciones pertinentes cuando se estime necesario. De esta forma el sistema puede reaccionar ágilmente y cambiar de acuerdo a las circunstancias.

Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continuada se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones.

3.3.1 Factores/Causas

Dentro de los factores de riesgo de fraude o causas, relacionadas con la ausencia de controles de monitoreo, se encuentra:

- Exceso de confianza. Los líderes de proceso o jefes de área no ejercen sobre sus colaboradores de "confianza" actividades de monitoreo respecto del cumplimiento y adecuada ejecución de sus funciones y responsabilidades.

  El jefe de mesa (o jefe director) del comercial, bajo las premisas de delegación y confianza en su subalterno, no lleva a cabo actividades de supervisión continuada o evaluaciones periódicas sobre el desempeño de este, permitiéndole ocultar información o situaciones que bajo una adecuada y oportuna supervisión, podría brindar señales de alerta (quejas de clientes, solicitudes de cambio de asesor, errores detectados por el back office, etc.), frente a los posibles malos manejos o prácticas no adecuadas en la administración de los clientes por parte del comercial.

- Exceso de trabajo y monopolización en la atención al cliente. El comercial trasciende la atención al cliente incluso en períodos de vacaciones.

3.3.2 Mejores Prácticas

La Alta Gerencia debe monitorear el Sistema de Control Interno en la Entidad, entre otros, a través de: Comité de Auditoría, Comités Financieros, de Inversiones, de Riesgo, de Balance, Comités primarios, Seguimiento a los planes de mejoramiento, Evaluación de desempeño e Indicadores Corporativos, Satisfacción del cliente, Clima organizacional, Auditorías, revisiones aleatorias de resultados, indicadores, etc.

4. Construyendo un Programa de Prevención y Respuesta al Fraude (Propuesta)

La cultura ética en las entidades y el combate exitoso contra el fraude no se logran tan solo llevando a cabo investigaciones. De acuerdo con las estadísticas el 38% de los eventos de fraude han sido identificados por accidente o de manera casual, 33% por diligencia de la Auditoría Interna, 22% a través de los canales de quejas, reclamos y denuncias, y el 5% por intervención de la Auditoría Externa. Más del 85% de los fraudes corporativos han sido cometidos por personal interno de las entidades; más del 64% de las empresas no cuentan con una política antifraude formal; cerca del 92% de las empresas no entrenan a su personal en materia de prevención y detección de fraudes. El fraude interno y la colusión con clientes y proveedores es la segunda modalidad más preocupante con un 32%[25].

Es por esto que el Comité de Control Interno & Compliance presentan una propuesta para diseñar, desarrollar, implementar una estructura de control para prevenir, en un grado razonable, fraudes contra las entidades, o bien, evitar que estas sean utilizadas como medio para cometerlos, aplicando procedimientos de investigación y métodos técnicos.

El Programa de Prevención y Respuesta al Fraude es un esquema o estructura de carácter institucional, basado en políticas, procesos, organización y recursos, orientado a prevenir, controlar, detectar y minimizar la probabilidad de ocurrencia del riesgo de fraude, o el impacto de los eventos materializados en la actividad de intermediación valores y de divisas. La estructura para el control y prevención del fraude eficiente, debe contener al menos los siguientes elementos:

4.1. Definición de Fraude

Es importante que la entidad defina un muy pensado y elaborado concepto de lo que consideran como fraude o práctica fraudulenta al interior de la organización, teniendo en cuenta el objeto del negocio y las características de sus procesos.

[25] Fuente: "El Manejo de Riesgos es Nuestra Fortaleza" Mancera Ernst & Young firma de contadores y consultores.

4.2. Cultura Antifraude

La cultura antifraude nace desde la Alta Dirección (Junta Directiva[26]) y la Administración (Gerencia), y está definida por el tono, la cultura, los valores y principios de cero tolerancia al fraude. Dentro de los componentes de la cultura antifraude que la entidad debe observar, se encuentran:

- **Tono Gerencial:** la gerencia debe enviar un mensaje explícito y claro relacionado con el fraude y la tolerancia ante estas situaciones en la entidad.
- **Entorno de Control:** la organización debe mantener un sólido entorno de control y concientización.
- **Comunicación:** la organización definirá explícitamente las expectativas relacionadas con el fraude y el comportamiento que se considera aceptable. Así mismo, fomentará el reporte de las actividades fraudulentas o inusuales.
- **Conciencia:** la entidad debe mantener programas formales de comunicación amplia y frecuente de temas tales como el código de conducta, las expectativas de comportamiento, y las maneras y motivos para utilizar los mecanismos de denuncias.
- **Educación:** las entidades deben llevar a cabo entrenamientos formales sobre concientización de fraude y sobre las expectativas que se tienen de los líderes de los procesos o unidades de negocio, para que identifiquen y comuniquen eventos irregulares o de incumplimiento.
- **Respuesta a Incidentes de Fraude:** La Alta Gerencia junto con el Comité de Auditoría, deberán actuar de manera rápida y decisiva ante instancias de fraude. Asimismo, deberán comunicar las lecciones aprendidas de manera apropiada y oportuna.

4.3. Órgano Disciplinario[27]

Establecimiento de un órgano disciplinario –funcionalmente segregado de la dirección ejecutiva- y dependiendo de éste la unidad de investigación. Este órgano disciplinario contaría como mínimo con las siguientes responsabilidades:

- Proponer las políticas de prevención del fraude y su mejoramiento continuo a los accionistas de la organización;

[26] Consejo de Directores

[27] Basado en la Norma IRAM N° 17450 – "Sistema de Gestión para la Prevención del Fraude Corporativo" emitida por la Dirección General de Normas (DGN) del Instituto Argentino de Normalización IRAM, el 26 de agosto de 2005.

- Velar por el cumplimiento del código de ética;
- Ser la autoridad de interpretación del código y de consulta ante situaciones no contempladas;
- Capacitar en temas éticos a los miembros de la Entidad;
- Analizar denuncias de incumplimiento y ordenar su investigación;
- Sancionar los incumplimientos;
- Verificar la aplicación de las sanciones.

4.4. Política antifraude

Definición e implementación de una política general antifraude que vincule al área de sistemas no solo con las áreas involucradas en el proceso de intermediación de valores/divisas, sino con las demás áreas o unidades de negocio de la Entidad, y en donde la Junta Directiva y la Administración pongan en claro su posición de "**cero tolerancia**" al fraude o prácticas no apropiadas.

La política antifraude debes ser documentada y contener al menos los siguientes elementos:

4.4.1. Presentación

La Junta Directiva y la Administración expresan la responsabilidad que tienen de promover entre los colaboradores, clientes, proveedores y demás grupos de interés que interactúan con la Entidad, las más altas conductas éticas.

Bajo este contexto, se define la política antifraude en el marco del "Programa de Prevención y Respuesta al Fraude" en la Entidad, así como la finalidad por la cual ha sido creada. Dicha finalidad debe involucrar al menos, fortalecer la cultura ética, propender por la transparencia, confiabilidad y exactitud de los reportes financieros y demás información de la Entidad; cumplir con los lineamientos, procedimientos, planes, leyes y normas aplicables, salvaguardar los activos de la organización y promover el uso razonable y eficiente de los recursos en cumplimiento de los objetivos de la Entidad.

4.4.2. Alcance

En el alcance se establecen las áreas, colaboradores, clientes, inversionistas, y terceros en general a quienes aplica la política antifraude y el "Programa de Prevención y Respuesta al Fraude".

4.4.3. Definición

Descripción del concepto de fraude y la definición de las actividades o acciones que se consideran como fraudes o prácticas no apropiadas. Tanto la definición de fraude como la descripción de las prácticas consideradas como tal, deben ser lo suficientemente claras y descriptivas, toda vez que no induzcan al error.

4.4.4. Declaración de la Política

La entidad hace manifiesta su posición de NO TOLERANCIA al fraude y todas las formas de fraude, y su decisión de tomar todas las medidas necesarias para combatirlo, tales como:

- La implementación de mecanismos, sistemas y controles adecuados que permiten la prevención, detección y respuesta de estas conductas, propendiendo por fortalecer la cultura ética basada en el principio de "transparencia y de cero tolerancia" al fraude y en aplicación de los principios de ética y comportamiento, responsabilidad de todos los funcionarios de la entidad;
- Generación de un entorno de transparencia, integrando los diferentes sistemas desarrollados para la prevención, detección y respuesta al fraude, manteniendo los canales adecuados para favorecer la comunicación de dichos asuntos en la entidad;
- Integración y coordinación del conjunto de acciones necesarias para prevenir, detectar y dar respuesta a las posibles situaciones de fraude, como elemento fundamental y alineado con las demás políticas de la entidad.
- Actuación en todo momento bajo los lineamientos de la legislación vigente, de la normatividad interna de la entidad y, en particular, de los lineamientos establecidos por el Código de Buen Gobierno y Ética (Conducta).
- Identificación y ejecución de procedimientos para la prevención, detección y respuesta del riesgo de fraude.
- Priorización de las actividades de prevención, sin disminuir los esfuerzos en las actividades de detección y respuesta al fraude.
- Evaluaciones de los presuntos indicios de fraude bajo los principios de confidencialidad, transparencia y objetividad.
- Gestión oportuna de todas las denuncias de actos fraudulentos, independientemente de su cuantía o personal involucrado, garantizando confidencialidad, objetividad y transparencia.

- Aplicación de las sanciones pertinentes de acuerdo con las normas internas y dar traslado a las autoridades competentes cuando así se requiera.
- Comunicación permanentemente y a través de los canales adecuados acerca de cualquier indicio de acciones constitutivas de fraude del que se tenga conocimiento y/o soporte.

4.4.5. Responsabilidad

Descripción de la responsabilidad directa e indirecta de la administración, funcionarios, líderes de proceso, Auditoría Interna, Comité de Auditoría de la entidad, etc., frente a la identificación, medición, control y monitoreo del riesgo de fraude, así como del procesamiento y resultados de las investigaciones.
Las responsabilidades deben ser asignadas, al menos en los siguientes tópicos:

- Prevención de Fraude
- Seguridad de la Información
- Seguridad Técnica de la Información
- Seguridad física
- Riesgo Operativo
- Gestión Humana
- Control interno
- Revisoría Fiscal
- Otros

4.4.6. Marco y/o Contexto Normativo y Regulatorio

Descripción de las normas, regulaciones, modelos y estándares (internos y externos) que sirven de marco a la política antifraude.

4.5. Comités de Apoyo

La entidad debe estructurar los comités que sean necesarios de acuerdo a la normatividad vigente y al tamaño de la organización. Entre los comités que sirven de apoyo en la ejecución del "Programa de Prevención y Respuesta al Fraude" se hallan: Comité de Fraude, Comité de Auditoría, Comité de Riesgos, Comités de seguridad de la información, Otros.

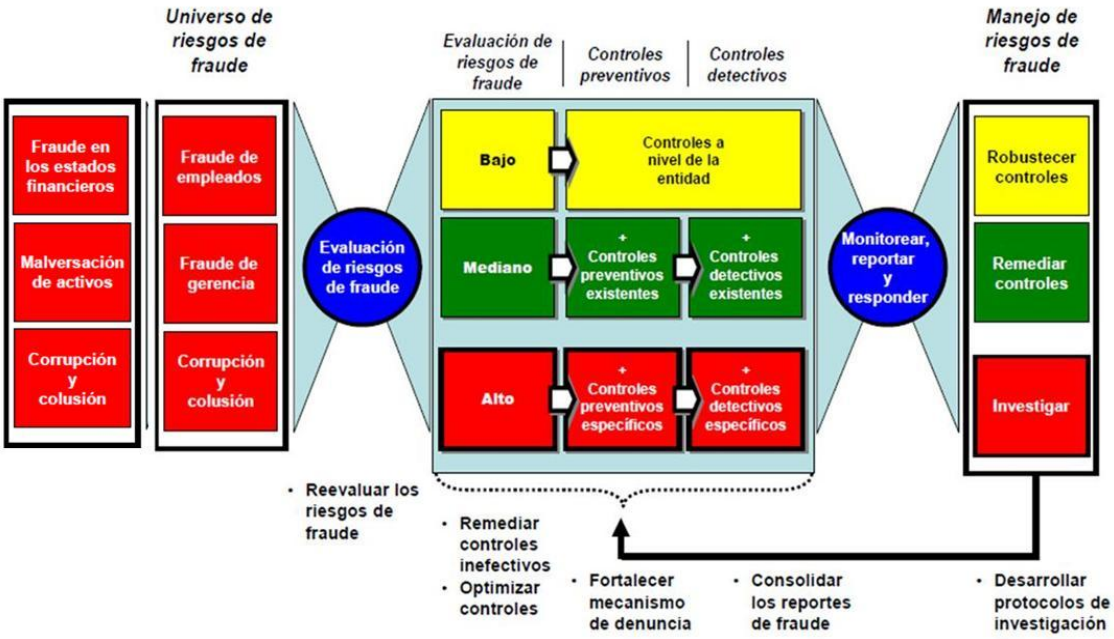
4.6. Modelo de Prevención y Respuesta al Fraude

En este punto, la entidad debe hacerse las siguientes preguntas antes de definir, adaptar o adoptar un modelo para la prevención y respuesta al fraude.

¿Dónde puede ocurrir el fraude?
¿Qué controles deben existir para prevenir o detectar el fraude?
¿Cómo se monitorean estos controles?
¿Cómo se comunican los resultados de las actividades de monitoreo?
¿Qué hacer cuando se encuentran excepciones o instancias de fraude?

Es importante tener en claro que el modelo de prevención y respuesta al fraude definido, adaptado o adoptado por la entidad, debe formar parte integral del sistema de administración de riesgos, el cual a su vez es un elemento del Sistema de Control Interno.

A este respecto, un modelo adecuado para la prevención y respuesta al fraude debe tener al menos, la siguiente estructura[28]:



[28] Fuente: "El Manejo de Riesgos es Nuestra Fortaleza" Mancera Ernst & Young firma de contadores y consultores.

4.1.6. Evaluación de Riesgos de Fraude

El proceso de evaluación de riesgos de fraude debe mantener la misma estructura y etapas que el sistema de gestión de riesgos de la entidad, esto es, identificación, clasificación, medición, control y monitoreo.

En esta primera fase del "Modelo para la Prevención y Respuesta al Fraude" la entidad debe identificar el universo de riesgos de fraude, partiendo en un conocimiento previo del negocio y sus procesos. Los riegos de fraude así identificados, serán clasificados de acuerdo con el factor generador, ya sean estos fraudes de empleados, fraudes de gerencia, o corrupción y colusión, así como su posible motivación: Presión (financieras, personal, metas corporativas poco realistas, etc.), oportunidad (debilidad de controles, empleados en puestos sensibles y de confianza, etc.), y racionalización o justificación (creencias/justificaciones como que "no es una actividad criminal", "no es un robo", "es un préstamo", etc.).

A continuación, un ejemplo del universo de riesgos que la administración debe identificar y clasificar:

Fraude en los Estados Financieros	Malversación de Activos	Corrupción/Colusión
• Reconocimiento incorrecto de ingresos • Reconocimiento incorrecto de gastos y/o activos • Fraude fiscal • Clasificaciones y revelaciones incorrectas en los estados financieros • Reportes incorrectos de la gerencia	• Hurto de efectivo • Hurto de depósitos • Operaciones no registradas • Hurto de cheques • Alteración de cheques • Desvío de pagos • Registro de desembolsos fraudulentos • Gastos de representación fraudulentos • Fraude en nómina • Falsificación de documentos • Hurto de activos • Uso no apropiado de activos	• Soborno • Conflicto de intereses • Bonos / comisiones ilegales • Extorsión económica

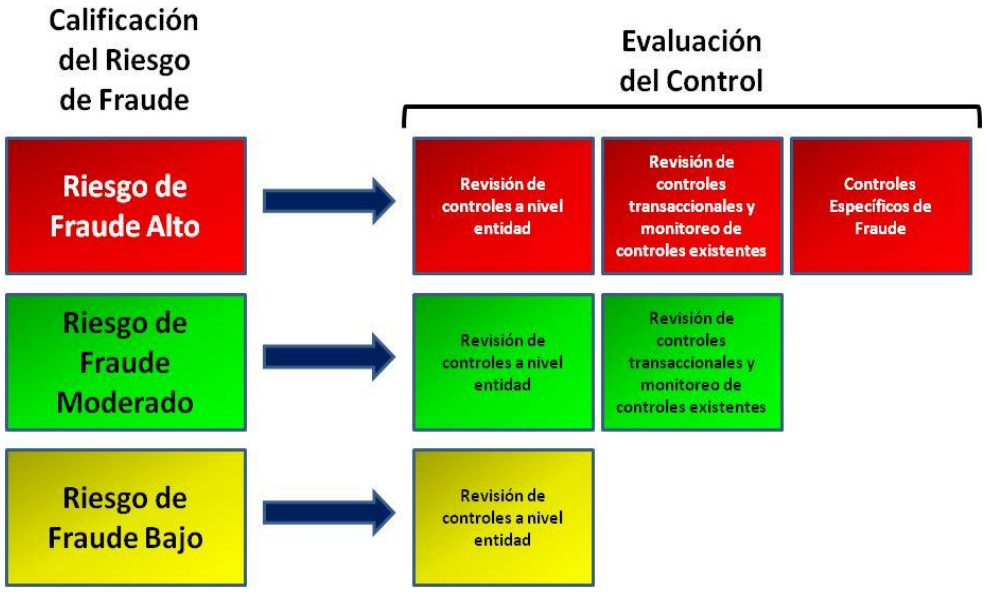
En este punto, la entidad hace una medición de la probabilidad de ocurrencia y posible impacto de los riesgos de fraude identificados, teniendo en cuenta nada más que las características de los procesos en donde se manifiestas los riesgos.

4.1.7. Evaluación de la Suficiencia y Eficiencia de los Controles

Efectuada la medición del riesgo de fraude inherente (sin tener en cuenta los controles), la entidad identificará los controles existentes, evaluando su efectividad frente a la mitigación de tales riesgos.

En esta fase del modelo, las áreas de riesgos, Auditoría Interna y Revisoría Fiscal deben trabajar de manera cooperativa, con el fin de aunar esfuerzos y hacer un uso más eficiente de los recursos (humano, económico, tecnológico, etc.).

La racionalización de los recursos en la evaluación de los controles, depende del enfoque que se dé a tal evaluación. Esto es, dependiendo de la calificación del riesgo de fraude inherente, la administración se enfocará ya sea en los controles a nivel entidad, controles transaccionales y/o control específicos de fraude.



En esta fase tanto la Junta Directiva, como la administración y los órganos de control de la entidad, deben definir las actividades de control para la prevención y/o detección del riesgo de fraude.

Los controles involucran todas aquellas actividades relacionadas con:

- Separación de tareas y responsabilidades
- Coordinación entre sectores
- Documentación
- Niveles definidos de autorización
- Registro oportuno y adecuado de las transacciones y hechos
- Acceso restringido a los recursos, activos y registros
- Rotación del personal en las tareas claves
- Control del sistema de información
- Control de la tecnología de la información

- Indicadores de desempeño
- Función de auditoría interna independiente

En la administración del riesgo de fraude, es importante colocar especial énfasis en la definición y estructuración de adecuados controles de acceso y seguridad informática, como parte vital de las políticas y procedimientos asociados a la tecnología de información, incluyendo la creación de la función de seguridad de activos de información.

Tales controles deben cubrir al menos los siguientes aspectos:

- Diseño de sistemas
- Diseño de bases de datos
- Programación
- Sistema de control de accesos
- Perfiles de usuarios
- Resguardo de programas y de datos
- Procedimientos de controles de procesamiento de información y datos
- Procedimientos de integridad de bases
- Controles lógicos de los programas
- Limitaciones de ingreso por fecha-valor.
- Seguridad de la información
- Seguridad Física
- Proceso seguro de destrucción de Información
- Canales de servicio

La administración debe determinar cuáles son los controles que deben ser evaluados, incluyendo todos aquéllos que están designados como un control antifraude. La actividad de auditoría interna que se relaciona con la identificación y detección del fraude debe ser adecuada, según los riesgos de la organización. La función de auditoría interna debe reportar de manera directa al comité de auditoría. El Comité de Auditoría debe demostrar un nivel adecuado de participación e interacción, tanto proactivo como reactivo, con la auditoría interna en relación con los temas de fraude.

4.1.8. Monitoreo, Reporte y Tratamiento de los Riesgos de Fraude

En esta etapa la Entidad deberá establecer procedimientos periódicos para la evaluación de la operatividad y efectividad de los controles antifraude, así como para el monitoreo del perfil de riesgo de fraude. La definición de indicadores es muy importante, pues permiten a la Alta Dirección de la entidad y a los organismos de control, identificar alertas tempranas frente a la materialización de eventos de fraude.

Existen indicadores de riesgo de fraude que proporcionan consideraciones del riesgo para la administración, que pueden utilizarse al desarrollar y poner en práctica un enfoque de evaluación del riesgo de fraude. Estos indicadores se utilizan para facilitar la acumulación de información en relación con el factor de riesgo de fraude y como una guía para el diálogo con los individuos responsables de los controles a nivel de proceso y de entidad. Aunque no es concluyente, la existencia o ausencia de los indicadores de fraude dentro de la entidad, o en sus procesos, proporcionaría conocimientos y experiencia respecto al alcance apropiado para el monitoreo, evaluación y supervisión del fraude[29].

Existen algunos indicadores del fraude como por ejemplo:

El exceso de confianza: es uno de los indicadores más notables de la oportunidad del fraude y ocurre generalmente con algunos empleados cercanos quienes como "personas de confianza" tienen la autorización de sus jefes para llevar a cabo funciones propias de estos, como firmar en su nombre documentos bajo el argumento de agilizar los procedimientos.

El acceso privilegiado: que tienen algunas personas para ingresar a lugares exclusivos, como archivos confidenciales, base de datos, registro de firmas, etc., les permite tener una gran fuente de información.

[29] Fuente: Revista Contaduría Pública del Instituto Mexicano de Contadores Públicos. Roberto Adad, CP, CFE, CICA; Socio de Protiviti; Managing Director Centro Bursátil

Conocimiento del terreno: a partir de la observación del movimiento financiero y de las actividades propias de la institución, personas (funcionarios) pueden calcular sus riesgos de responsabilidad, orientando sus actividades a lo ilícito.

Períodos de vacaciones acumulados: es un indicador bastante importante, pues las áreas sensibles en donde los funcionarios han acumulado varios períodos de vacaciones, son más vulnerables a los fraudes.

La Falta de control: es uno de los factores que impulsan a cometer inicialmente irregularidades administrativas y luego actividades ilícitas, pues se piensa que no hay posibilidad de ser descubierto.

El riesgo de fraude y los temas relacionados necesitan estar en el programa de actividades de las reuniones del Comité de Auditoría, del comité de divulgación y del comité ejecutivo (o del Comité Ejecutivo para la administración o gestión del riesgo) en los momentos apropiados. Debe existir la documentación adecuada de dichas consideraciones de supervisión para establecer la viabilidad y el contenido del programa antifraude.

Identificar e investigar las denuncias anónimas en una manera eficaz y oportuna

Como parte del monitoreo y reporte, deben existir procedimientos adecuados para atender las quejas o reclamaciones y aceptar la información proporcionada de manera confidencial o anónima sobre las preocupaciones, en relación con los temas o asuntos cuestionables respecto a la contabilidad y la auditoría. ¿Ha establecido el Comité de Auditoría los procedimientos adecuados para manejar las quejas o reclamaciones confidenciales y anónimas, y todas las presentaciones de información en relación con los informes financieros y/o las irregularidades de las auditorías? ¿Cuál es la frecuencia en la que se producen los fraudes reportados? ¿Existe algún procedimiento que haya sido implementado para asegurar las investigaciones independientes y las soluciones? ¿Cuál es el periodo de tiempo existente entre la recepción de la denuncia inicial y la investigación resultante? ¿Cuál es el periodo de tiempo que existe entre la comunicación de los resultados de la investigación y el completamiento de las soluciones? ¿Cuáles pruebas se llevan a cabo para determinar si se ha reportado, investigado y resuelto un fraude, en la manera descrita en el programa antifraude?

Remediar las deficiencias de manera oportuna

Cuando las deficiencias en el programa antifraude y en los controles relacionados son identificadas, éstas deben ser solucionadas o remediadas de manera oportuna. La administración también debe considerar si existen indicadores que sugieran que dichas deficiencias han sido explotadas, por ejemplo, si alguien ha aprovechado la oportunidad de manera interna o externa al tomar ventaja de las debilidades de los controles para el beneficio personal o corporativo.

Consultar con los asesores o consultores

La administración debe consultar con los asesores legales, los especialistas en fraude y los auditores externos, la medida en la que los documentos de la empresa evalúan, refinan y mejoran el programa antifraude y los controles relacionados.

5. Consideraciones finales

A continuación, y como conclusión del presente documento de investigación, el Comité de Control Interno & Compliance incluye 10 sugerencias para que la Junta Directiva y la Alta Dirección de las entidades establezcan un programa antifraude eficaz.

5.1. Establecer el entendimiento del programa. Determinar y asegurar que el programa antifraude cuenta con todos los elementos que se requieren.

5.2. Predicar con el ejemplo de la administración (Tune of the Top). Evaluar la evidencia relacionada con el comportamiento ético de la administración, incluyendo las políticas y procesos que prohíben la cancelación de los controles por su parte.

5.3. Evaluar el riesgo de fraude. Debido a que la definición del fraude varía en gran medida entre las comunidades legales, de auditoría y negocios, es importante determinar cómo se define dentro del contexto de la organización, para lograr identificación de riesgos de fraudes específicos de la industria, geográficos, así como otros riesgos relevantes.

5.4. Identificar los controles de mitigación. Los controles deben estar relacionados o vinculados a un riesgo de fraude específico identificado, tanto en el nivel de

entidad como en el de proceso. En relación con el diseño de los controles, la documentación de la empresa debe abarcar: "el diseño de los controles para prevenir, evitar o detectar el fraude, incluyendo a la persona que implementa los controles y la segregación de actividades o tareas relacionadas"[30].

5.5. Llevar a cabo pruebas de fraude. La administración debe determinar cuáles son los controles que deben ser evaluados, incluyendo todos aquéllos que están designados como un control antifraude. La actividad de auditoría interna que se relaciona con la identificación y detección del fraude debe ser adecuada, según los riesgos de la organización. La función de auditoría interna debe reportar de manera directa al comité de auditoría. El Comité de Auditoría debe demostrar un nivel adecuado de participación e interacción, tanto proactivo como reactivo, con la auditoría interna en relación con los temas de fraude.

5.6. Mantener un código de conducta efectivo y eficaz. El Código de Conducta debe recoger al menos las disposiciones acerca de conflictos de interés, transacciones de las partes relacionadas, acciones ilegales y el monitoreo del código por parte de la administración.

5.7. Llevar a cabo la supervisión del programa antifraude. El riesgo de fraude y los temas relacionados necesitan estar en el programa de actividades de las reuniones del Comité de Auditoría, del comité de divulgación y del comité ejecutivo (o del Comité Ejecutivo para la administración o gestión del riesgo) en los momentos apropiados. Debe existir la documentación adecuada de dichas consideraciones de supervisión para establecer la viabilidad y el contenido del programa antifraude.

5.8. Identificar e investigar las denuncias anónimas de una manera eficaz y oportuna. Deben existir los procedimientos adecuados para atender las quejas o reclamaciones y aceptar la información proporcionada de manera confidencial o anónima sobre las preocupaciones, en relación con los temas o asuntos cuestionables respecto a la contabilidad y la auditoría.

[30] Fuente: The Public Company Accounting Oversight Board – PCAOB (Consejo de Supervisión de Contabilidad de las Empresas Públicas en EEUU)

5.9. Remediar las deficiencias de manera oportuna. Cuando las deficiencias en el programa antifraude y en los controles relacionados son identificadas, éstas deben ser solucionadas o remediadas de manera oportuna. La administración también debe considerar si existen indicadores que sugieran que dichas deficiencias han sido explotadas, por ejemplo, si alguien ha aprovechado la oportunidad de manera interna o externa al tomar ventaja de las debilidades de los controles para el beneficio personal o corporativo.

5.10. Consultar con los asesores o consultores. La administración debe consultar con los asesores legales, los especialistas en fraude y los auditores externos, la medida en la que los documentos de la entidad evalúan, refinan y mejoran el programa antifraude y los controles relacionados.

DISCLAIMER

CLAUSULA DE EXENCIÓN DE RESPONSABILIDAD

El presente *documento de investigación* se encuentra en estado "Proyecto de Borrador"; lo cual implica que la información aquí contenida tiene propósito investigativo sobre el tema.

Se comparte como insumo de trabajo a personas o entidades que tengan especial interés y conocimiento del tema. No ha sido adoptada ni aprobada por el Autorregulador del Mercado de Valores - AMV, ni por ninguno de sus directivos, por lo que no deben tomarse como declaraciones de esta entidad y no compromete de manera alguna la política de AMV.

El presente documento no ha sido validado por AMV, por lo cual no asume ninguna responsabilidad por la exactitud de los datos contenidos en el documento, ni por el uso que se haga posteriormente de los mismos.

En razón de lo anterior, solicitamos utilizar la información contenida en el documento como un referente para formular comentarios a los funcionarios del AMV, abstenerse de distribuirlo a terceros, dado que el documento es confidencial y solamente puede ser utilizado por su destinatario. Igualmente, abstenerse de reproducir el documento o citarlo, en razón a su naturaleza confidencial.

Se recomienda no utilizarlo como un concepto jurídico o referencia final para casos concretos, ni tomarlo como soporte concluyente en la decisión de procesos disciplinarios. En caso de existir una pregunta específica sobre la aplicación de la normatividad que por su naturaleza requiera la realización de un estudio especial, se recomienda formular una solicitud de concepto a AMV o demás autoridades competentes. Este documento no puede ser considerado como un reemplazo de un concepto particular.