CIRCULAR EXTERNA 14 DE 2009

(mayo 19)

<Fuente: Boletín Ministerio de Hacienda, Capítulo Superintendencia Financiera de Colombia, No. 138 de 22 de mayo de 2009>

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

<Ver Circular 38 de 2009, mediante la cual se modifican plazos fijados en la presente circular>

Resumen de Notas de Vigencia

NOTAS DE VIGENCIA:

- Modificada por la Circular 38 de 2009, publicada en el Boletín Ministerio de Hacienda, Capítulo Superintendencia Financiera de Colombia, No. 152 de 9 de octubre de 2009

Señores

MIEMBROS DE JUNTA DIRECTIVA, REPRESENTANTES LEGALES, REVISORES FISCALES, AUDITORES INTERNOS Y CONTRALORES NORMATIVOS DE LAS ENTIDADES SUPERVISADAS POR LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Referencia: Instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI).

Apreciados Señores:

Esta Superintendencia, en uso de sus facultades legales, en especial de la consagrada en el numeral 9o del artículo 11 del Decreto 4327 de 2005, dada la importancia que deben otorgar las entidades supervisadas al fortalecimiento de los sistemas de control interno y a la evaluación continua de su eficiencia, estima necesario que ellas estructuren, implementen y mantengan un Sistema de Control Interno (en adelante SCI) o lo adecuen, según el caso, a los lineamientos establecidos en la presente circular, de tal manera que dicho sistema contribuya al logro de sus objetivos y fortalezca la apropiada administración de los riesgos a los cuales se ven expuestas en el desarrollo de su actividad, realizándolas en condiciones de seguridad, transparencia y eficiencia.

Las reglas, parámetros generales y requisitos mínimos aquí contemplados, deben ser ajustados o implementados por las entidades supervisadas (entendiendo por tales las sometidas a la vigilancia o control de esta Superintendencia de conformidad con lo señalado en los artículos 72 y 73 del Decreto 4327 de 2005), de acuerdo con el tamaño de la respectiva organización, la naturaleza de sus actividades y la complejidad de sus operaciones, teniendo en cuenta la relación beneficio / costo. Los administradores de la respectiva entidad deberán analizar y verificar este punto teniendo en cuenta su conocimiento de la misma, del sector económico al cual pertenece y de los riesgos que enfrenta, sin que en ningún caso el costo de las medidas adoptadas exceda el beneficio que de ellas se deriven.

De acuerdo con lo anterior, a través de la presente circular se establece un marco conceptual y normativo para el SCI como elemento fundamental del gobierno corporativo de las entidades

supervisadas basado en modelos ampliamente aceptados a nivel internacional[1] que contemplan en detalle la noción, contenido y alcance del sistema de control interno, con los siguientes objetivos:

· Mejorar la eficiencia y eficacia en las operaciones de las entidades supervisadas.

· Prevenir y mitigar la ocurrencia de fraudes, originados tanto al interior como al exterior de las organizaciones.

· Orientar a los administradores de las entidades supervisadas en el cumplimiento de los deberes que les corresponde según la normatividad vigente, precisando el alcance de la responsabilidad en materia de control interno de los distintos órganos sociales.

· Fomentar tanto la autorregulación como el autocontrol, dado que sin perjuicio de la responsabilidad que corresponde a los administradores, todos los integrantes de la organización deben evaluar y controlar su propio trabajo.

Las entidades supervisadas que pertenezcan al sector público y estén obligadas a la adopción del Modelo Estándar de Control Interno - MECI según lo establecido en el Decreto 1599 de 2005 y sus reglamentos, deberán complementar dicho modelo con los aspectos incluidos en la presente circular que no se prevean dentro del MECI.

Toda vez que la Superintendencia Financiera de Colombia es consciente de que se requiere un plazo prudencial para la implementación y/o adecuación del SCI por parte de las entidades supervisadas, la evolución de la cultura organizacional y demás ajustes prácticos inherentes a dicho proceso, y en especial considerando que un sistema eficiente de control interno resulta fundamental para la operación prudente de una organización, se establece el siguiente cronograma:

1. Implementación o ajuste de los elementos mínimos para crear un adecuado ambiente de control de conformidad con los requisitos establecidos en el numeral 7.5.1 del anexo a la presente circular y sus subdivisiones, a más tardar el 30 de septiembre de 2009.

2. Implementación o ajuste de los sistemas de información y comunicación en forma tal que se tenga un grado de seguridad razonable respecto a la exactitud, validez y oportunidad de la información generada por la entidad, de conformidad con los requisitos establecidos en el numeral 7.5.4 del anexo a la presente circular y sus subdivisiones, a más tardar el 31 de diciembre de 2009.

3. Implementación o ajuste del sistema de gestión de riesgos de conformidad con los requisitos establecidos en el numeral 7.5.2 del anexo a la presente circular, a más tardar el 31 de marzo de 2010.

4. Adecuación de la composición y funcionamiento de los órganos de administración y control a que se refiere la presente circular, a más tardar el 30 de abril de 2010.

5. Implementación o ajuste de las actividades de control de conformidad con los requisitos establecidos en el numeral 7.5.3 del anexo a la presente circular, a más tardar el 31 de mayo de 2010.

6. Implementación o ajuste de los controles que permitan a la alta dirección y a los responsables de cada área monitorear de manera permanente el desempeño del SCI y realizar las acciones de

mejoramiento necesarias, de conformidad con los requisitos establecidos en el numeral 7.5.5 del anexo a la presente circular, a más tardar el 30 de junio de 2010.

7. Evaluación independiente respecto de la efectividad del SCI de conformidad con lo señalado en el numeral 7.5.6 del anexo de la presente circular, a más tardar el 31 de agosto de 2010.

La culminación de la implementación del SCI, dentro de los plazos antes mencionados, deberá abarcar todas las áreas de la organización, incluyendo entre otras las mencionadas en el numeral 7.6 del anexo a la presente circular.

La responsabilidad de los administradores sociales y demás órganos señalados en el numeral 7.7 del mencionado Anexo es permanente, de acuerdo con los deberes y responsabilidades que les asigna la normatividad vigente.

Para efectos de hacer seguimiento al cumplimiento del cronograma antes mencionado, el presidente de la junta directiva u órgano equivalente y el representante legal de cada entidad supervisada deberán enviar a esta Superintendencia, dentro de los diez (10) días hábiles siguientes al vencimiento de cada uno de los siete plazos antes señalados, una certificación acerca del cumplimiento de la meta respectiva, previa verificación de los documentos y demás elementos que soporten dicha afirmación.

Los mencionados plazos no afectan los establecidos para efectos de la implementación de los sistemas especiales de gestión de riesgos específicos exigidos por esta entidad en la Circular Básica Jurídica y en la Circular Básica Financiera y Contable (incluyendo entre otras las normas sobre gestión de riesgos de mercado –SARM, riesgo de crédito –SARC, riesgo operativo –SARO, riesgo de liquidez –SARL, riesgo de lavado de activos y de la financiación del terrorismo- SARLAFT y riesgo de garantías SARG), los cuales continuarán rigiéndose por los plazos y condiciones establecidos de manera específica para cada uno de ellos.

En cuanto a los requerimientos mínimos de seguridad y calidad que deben atender las entidades vigiladas para el manejo de la información a través de los diferentes medios y canales utilizados para la distribución de los productos y servicios que ofrecen a sus clientes y usuarios, éstos deberán cumplirse dentro de los plazos señalados en la Circular Externa 52 de 2007 y demás normas que la modifiquen.

La presente circular rige a partir de la fecha de su publicación, modifica el numeral 7o del Capítulo IX Título Primero - Control Interno de la Circular Básica Jurídica y deroga el parágrafo de la Circular Externa 10 de 2007 expedida por la Superintendencia Financiera de Colombia, así como las demás disposiciones que le resulten contrarias.

Se adjuntan las páginas pertinentes.

Cordialmente,

ROBERTO BORRÁS POLANIA

Superintendente Financiero de Colombia

* * *

1. COSO Integrado (Committe Sponsoring Organization of the Treadway Commission Committee of Sponsoring Organizations of the Treadway Commission and Enterprise Risk

Management – Integrated Framework), SOX (Sarbanes-Oxley Act of 2002, Section 404), Basilea ("FRAMEWORK FOR INTERNAL CONTROL SYSTEMS IN BANKING ORGANISATIONS" e "International Convergence of Capital Measurement and Capital Standards", emitidos por el Basle Committee on Banking Supervision), COBIT (Control Objectives for Information and related Technology) y los estándares del Instituto de Auditores Internos "IIA"

<Página 55>

Titulo I - CAPITULO NOVENO

Obligaciones especiales de las entidades vigiladas

7. SISTEMA DE CONTROL INTERNO

7.1 Consideraciones Generales

Corresponde a los administradores de las entidades supervisadas (entendiendo por tales las sometidas a vigilancia o control de la Superintendencia Financiera de Colombia de conformidad con lo señalado en los artículos 72 y 73 del Decreto 4327 de 2005 y demás normas que los modifiquen o adicionen), realizar su gestión con la diligencia propia de un buen hombre de negocios. Por ello, compete a las juntas o consejos directivos o al órgano que haga sus veces, en calidad de administradores, definir las políticas y diseñar los procedimientos de control interno que deban implementarse, así como ordenar y vigilar que los mismos se ajusten a las necesidades de la entidad, permitiéndole desarrollar adecuadamente su objeto social y alcanzar sus objetivos, en condiciones de seguridad, transparencia y eficiencia.

7.2. Ámbito de aplicación

Todas las entidades supervisadas, ya sean matrices o subordinadas, deberán implementar o ajustar su SCI a los requisitos mínimos establecidos en el presente capítulo, en forma tal que el mismo resulte acorde con el tamaño de su organización (en términos de número de empleados, valor de los activos e ingresos, recursos captados del público, número de sucursales o agencias, entre otros.) y la naturaleza de las actividades propias de su objeto social, así como de las desarrolladas por cuenta de terceros, teniendo en cuenta la relación beneficio/costo.

Las entidades supervisadas que tengan la calidad de matrices deberán procurar que sus subordinadas (sean filiales o subsidiarias) tengan un adecuado SCI, para lo cual deberán emitir los lineamientos generales mínimos que en su concepto deben aplicar, atendiendo la naturaleza, magnitud y demás características de las mismas.

7.3 Definición y objetivo del Sistema de Control Interno

Se entiende por SCI el conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por la junta directiva u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

i. Mejorar la eficiencia y eficacia en las operaciones de las entidades supervisadas. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.

ii. Prevenir y mitigar la ocurrencia de fraudes, originados tanto al interior como al exterior de las organizaciones.

iii. Realizar una gestión adecuada de los riesgos.

iv. Aumentar la confiabilidad y oportunidad en la Información generada por la organización.

v. Dar un adecuado cumplimiento de la normatividad y regulaciones aplicables a la organización.

En la medida en que se logren los objetivos antes mencionados, el SCI brindará mayor seguridad a los diferentes grupos de interés que interactúan con la entidad.

7.4 PRINCIPIOS del Sistema de Control Interno

Los principios del SCI constituyen los fundamentos y condiciones imprescindibles y básicas que garantizan su efectividad de acuerdo con la naturaleza de las operaciones autorizadas, funciones y características propias, y se aplican para cada uno de los aspectos que se tratan en el presente capítulo. En consecuencia, las entidades, en el diseño e implementación o revisión o ajustes del SCI deben incluir estos principios, documentarlos con los soportes pertinentes y tenerlos a disposición de la SFC.

7.4.1 Autocontrol

Es la capacidad de todos y cada uno de los funcionarios de la organización, independientemente de su nivel jerárquico para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos en el ejercicio y cumplimiento de sus funciones, así como para mejorar sus tareas y responsabilidades.

En consecuencia, sin perjuicio de la responsabilidad atribuible a los administradores en la definición de políticas y en la ordenación del diseño de la estructura del SCI, es pertinente resaltar el deber que les corresponde a todos y cada uno de los funcionarios dentro de la organización, quienes en desarrollo de sus funciones y con la aplicación de procesos operativos apropiados deberán procurar el cumplimiento de los objetivos trazados por la dirección, siempre sujetos a los límites por ella establecidos.

7.4.2 Autorregulación

Se refiere a la capacidad de la organización para desarrollar en su interior y aplicar métodos, normas y procedimientos que permitan el desarrollo, implementación y mejoramiento del SCI, dentro del marco de las disposiciones legales aplicables.

7.4.3 Autogestión

Apunta a la capacidad de la organización para interpretar, coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz su funcionamiento.

Basado en los principios mencionados, el SCI establece las acciones, las políticas, los métodos, procedimientos y mecanismos de prevención, control, evaluación y de mejoramiento continuo de la entidad que le permitan tener una seguridad razonable acerca de la consecución de sus objetivos, cumpliendo las normas que la regulan.

7.5. Elementos del Sistema de Control Interno

Para el cumplimiento de los principios y objetivos indicados con anterioridad, las entidades supervisadas deberán consolidar una estructura de control interno que considere por lo menos los elementos que se señalan a continuación:

7.5.1 Ambiente de Control

El ambiente de control está dado por los elementos de la cultura organizacional que fomentan en todos los integrantes de la entidad principios, valores y conductas orientadas hacia el control. Es el fundamento de todos los demás elementos del SCI, dado que la eficacia del mismo depende de que las entidades cuenten con personal competente e inculquen en toda la organización un sentido de integridad y concientización sobre el control.

Los elementos mínimos para crear un adecuado ambiente de control son:

i. Determinación formal por parte de la alta dirección de los principios básicos que rigen la entidad, los cuales deben constar en documentos que se divulguen a toda la organización.

ii. Expedición de un código de conducta que incluya:

§ Valores y pautas explícitas de comportamiento.

§ Parámetros concretos determinados para el manejo de conflictos de interés, incluyendo expresamente, entre otros, los que regulen las operaciones con vinculados económicos, en adición a los que apliquen por disposición legal.

§ Mecanismos para evitar el uso de información privilegiada o reservada.

§ Órganos o instancias competentes para hacer seguimiento al cumplimiento del código.

§ Sanciones por su inobservancia, teniendo en cuenta factores tales como reincidencias, pérdidas para los clientes o a la entidad, violaciones a límites, entre otros.

En caso que algunos de los temas antes citados no se incluyan en el código de conducta deberán incluirse en el código de gobierno corporativo de la entidad o en un documento independiente, si así se considera pertinente dada su importancia para la organización.

El código de conducta debe orientar la actuación de todos los funcionarios, quienes deben comprometerse explícitamente con su cumplimiento.

iii. Adopción de procedimientos que propicien que los empleados en todos los niveles de la organización cuenten con los conocimientos, habilidades y conductas necesarios para el desempeño de sus funciones.

La entidad debe contar con estándares debidamente documentados de las competencias, habilidades, aptitudes e idoneidad de sus funcionarios. Así mismo, debe determinar las políticas y prácticas de gestión humana que aplicará la entidad al realizar los procesos de selección, inducción, formación, capacitación, sistemas de compensación o remuneración y de evaluación del desempeño de sus empleados en todos sus niveles, las cuales deben ser diseñadas e implementadas para facilitar un efectivo control interno.

iv. Determinación de una estructura organizacional que permita soportar el alcance del SCI y que defina claramente los niveles de autoridad y responsabilidad, precisando el alcance y límite de los mismos. La estructura organizacional debe estar armonizada con el tamaño y naturaleza de

las actividades de la entidad, soportando el alcance del SIC.

v. Establecimiento de objetivos que deben estar alineados con la misión, visión y objetivos estratégicos de la entidad, para que a partir de esta definición, se formule la estrategia y se determinen los correspondientes objetivos operativos, de reporte y de cumplimiento para la organización.

Estos objetivos deben ser difundidos a todos los niveles de la entidad, actualizándolos en forma periódica.

La alta dirección de la entidad deberá transmitir a todos los niveles de la organización su compromiso y liderazgo respecto de los controles internos y los valores éticos, involucrando a todos los funcionarios para que asuman la responsabilidad que les corresponde frente al SCI.

7.5.2 Gestión de Riesgos

Las entidades deben preservar la eficacia, eficiencia y efectividad de su gestión y capacidad operativa, así como salvaguardar los recursos que administren, para lo cual deberán contar con un sistema de administración de riesgos que permita la minimización de los costos y daños causados por éstos, con base en el análisis del contexto estratégico, así como la determinación de métodos para el tratamiento y monitoreo de sus riesgos, con el propósito de prevenir o evitar la materialización de eventos que puedan afectar el normal desarrollo de los procesos y el cumplimiento de los objetivos empresariales, o, en caso de que ello no resulte razonablemente posible, de mitigar su impacto.

En el caso de las entidades vigiladas, éstas deben seguir las instrucciones especiales que en materia de gestión de ciertos riesgos se establecen en la presente circular y en la Circular Básica Financiera y Contable de la SFC (incluyendo entre otras, las normas sobre gestión de riesgos de mercado –SARM, riesgo de crédito –SARC, riesgo operativo –SARO, riesgo de liquidez –SARL, riesgo de lavado de activos y de la financiación del terrorismo- SARLAFT [que aplica también para los emisores de valores] y riesgo de garantías -SARG), según resulten aplicables en virtud del objeto social de la entidad, ajustándose a los plazos y condiciones específicos establecidos de manera especial para cada uno de ellos.

En el caso de las entidades sometidas a control, para la administración de sus riesgos éstas deberán adelantar como mínimo los siguientes procedimientos[1]:

i. Identificar las amenazas que enfrenta la entidad y las fuentes de las mismas.

ii. Autoevaluar los riesgos existentes en sus procesos, identificándolos y priorizándolos a través de un ejercicio de valoración cualitativa, teniendo en cuenta los factores propios de su entorno y la naturaleza de su actividad.

iii. Medir la probabilidad de ocurrencia de los riesgos y su impacto sobre los recursos de la entidad (económicos, humanos, entre otros), así como sobre su credibilidad y buen nombre, en caso de materializarse. Esta medición podrá ser cualitativa y, cuando se cuente con datos históricos, cuantitativa.

iv. Identificar y evaluar con criterio conservador, los controles existentes y su efectividad, mediante un proceso de valoración realizado con base en la experiencia y un análisis razonable y objetivo de los eventos ocurridos.

v. Construir los mapas de riesgos que resulten pertinentes, los cuales deben ser actualizados periódicamente, permitiendo visualizarlos de acuerdo con la vulnerabilidad de la organización a los mismos.

vi. Implementar, probar y mantener un proceso para administrar la continuidad de la operación de la entidad, que incluya elementos como: prevención y atención de emergencias, administración de crisis, planes de contingencia para responder a las fallas e interrupciones específicas de un sistema o proceso y capacidad de retorno a la operación normal.

vii. Divulgar entre los funcionarios que intervienen en los procesos respectivos, los mapas de riesgos y las políticas definidas para su administración.

viii. Gestionar los riesgos en forma integral, aplicando diferentes estrategias que permitan llevarlos hacia niveles tolerables. Para cada riesgo se debe seleccionar la alternativa que presente la mejor relación entre el beneficio esperado y el costo en que se debe incurrir para su tratamiento. Entre las estrategias posibles se encuentran las de evitar los riesgos, mitigarlos, compartirlos, transferirlos, aceptarlos o aprovecharlos, según resulte procedente.

ix. Registrar, medir y reportar los eventos de pérdidas por materialización de riesgos.

x. Hacer seguimiento a través de los órganos competentes, de acuerdo al campo de acción de cada uno de ellos, estableciendo los reportes o acciones de verificación que la administración de la entidad y los jefes de cada órgano social considere pertinentes.

xi. Definir las acciones correctivas y preventivas derivadas del proceso de seguimiento y evaluación de los riesgos (planes de mejoramiento).

Sobre este tema, es recomendable que las entidades sometidas a control de esta superintendencia cuenten con una unidad responsable de la administración de riesgos (o si así se considera procedente con una unidad responsable para cada una de las principales clases de riesgos), que defina procedimientos, administre el registro de eventos, prepare informes periódicos, elabore manuales (con políticas para la administración del riesgo, estructura para su gestión, responsabilidades y procedimientos, entre otros), asesore a las demás dependencias de la organización y adelante la capacitación sobre el tema.

Es importante reiterar que la administración de riesgos es uno de los elementos fundamentales del SCI para lograr la eficacia y eficiencia de las operaciones, la confiabilidad de los reportes financieros y el cumplimiento de leyes, normas y reglamentos. Los sistemas de control interno y de administración de riesgos son transversales en todas y cada una de las actividades, procesos y áreas de la entidad, por ello su importancia en el logro de los objetivos estratégicos y de calidad de la información que genera la organización.

7.5.3 Actividades de Control

Las actividades de control son las políticas y los procedimientos que deben seguirse para lograr que las instrucciones de la administración con relación a sus riesgos y controles se cumplan. Las actividades de control se distribuyen a lo largo y a lo ancho de la organización, en todos los niveles y funciones.

Lo anterior incluye entonces, el establecimiento de unas actividades obligatorias para todas las áreas, operaciones y procesos de la entidad, entre las cuales se encuentran, entre otras, las

siguientes:

i. Revisiones de alto nivel, como son el análisis de informes y presentaciones que solicitan los miembros de junta directiva y otros altos directivos de la organización para efectos de analizar y monitorear el progreso de la entidad hacia el logro de sus objetivos; detectar problemas, tales como deficiencias de control, errores en los informes financieros o actividades fraudulentas, y adoptar los correctivos necesarios.

ii. Gestión directa de funciones o actividades.

iii. Procesamiento de la información.

iv. Controles de aplicación.

v. Limitaciones de acceso a las distintas áreas de la organización, de acuerdo con el nivel de riesgo asociado a cada una de ellas, teniendo en cuenta tanto la seguridad de los funcionarios de la entidad como de sus bienes, de los activos de terceros que administra y de su información.

vi. Acompañamiento a los visitantes de la entidad para controlar que sólo ingresen a los sitios permitidos y que no realicen ningún acto que afecte la seguridad de los equipos o de la información que en ellos se procesa.

vii. Controles físicos adicionales que resulten necesarios.

viii. Indicadores de rendimiento.

ix. Segregación de funciones.

x. Acuerdos de confidencialidad.

xi. Procedimientos de control.

xii. Difusión de las actividades de control.

Las actividades de control son seleccionadas y desarrolladas considerando la relación beneficio / costo y su potencial efectividad para mitigar los riesgos que afecten en forma material el logro de los objetivos de la organización.

Dichas actividades implican una política que establece lo que debe hacerse y adicionalmente los procedimientos para llevarla a cabo. Todas estas actividades deben tener como principal objetivo la determinación y prevención de los riesgos (potenciales o reales), errores, fraudes u otras situaciones que afecten o puedan llegar a afectar la estabilidad y/o el prestigio de la entidad.

Adicionalmente deberán considerarse las actividades de control requeridas específicamente en el numeral 7.6 de este capítulo respecto a la gestión contable y tecnológica.

7.5.4 Información y Comunicación

Teniendo en cuenta que la operación de una entidad depende en gran medida de sus sistemas de información, es necesario adoptar controles que garanticen la seguridad, calidad y cumplimiento de la información generada.

Los sistemas de información y comunicación son la base para identificar, capturar e intercambiar información en una forma y período de tiempo que permita al personal cumplir con sus

responsabilidades y a los usuarios externos contar oportunamente con elementos de juicio suficientes para la adopción de las decisiones que les corresponde en relación con la respectiva entidad.

7.5.4.1 Información

Este sistema debe ser funcional para el suministro de información que permita dirigir y controlar el negocio en forma adecuada. Asimismo, deben permitir manejar tanto los datos internos como aquellos que se reciban del exterior.

Las entidades supervisadas deben contar con sistemas que garanticen que la información cumpla con los criterios de seguridad (confidencialidad,, integridad y disponibilidad), calidad (efectividad, eficiencia, y confiabilidad) y cumplimiento, para lo cual deberán establecer controles generales y específicos para la entrada, el procesamiento y la salida de la información, atendiendo su importancia relativa y nivel de riesgo.

Ello incluye, cuando menos, las siguientes actividades:

i. Identificar la información que se recibe y su fuente.

ii. Asignar el responsable de cada información y las personas que pueden tener acceso a la misma.

iii. Diseñar formularios y/o mecanismos que ayuden a minimizar errores u omisiones en la recopilación y procesamiento de la información, así como en la elaboración de informes.

iv. Diseñar procedimientos para detectar, reportar y corregir los errores y las irregularidades que puedan presentarse.

v. Establecer procedimientos que permitan a la entidad retener o reproducir los documentos fuente origínales, para facilitar la recuperación o reconstrucción de datos, así como para satisfacer requerimientos legales.

vi. Definir controles para garantizar que los datos y documentos sean preparados por personal autorizado para hacerlo.

vii. Implementar controles para proteger adecuadamente la información sensible contra acceso o modificación no autorizada.

viii. Diseñar procedimientos para la administración del almacenamiento de información y sus copias de respaldo.

ix. Establecer parámetros para la entrega de copias, a través de cualquier modalidad (papel, medio magnético, entre otros).

x. Clasificar la información (en pública, privada o confidencial, según corresponda).

xi. Verificar la existencia o no de procedimientos de custodia de la información, cuando sea del caso, y de su eficacia.

xii. Implementar mecanismos para evitar el uso de información privilegiada, en beneficio propio o de terceros.

xiii. Detectar deficiencias y aplicar acciones de mejoramiento.

xiv. Cumplir los requerimientos legales y reglamentarios.

La información que hace posible conducir y controlar la organización debe ser difundida de acuerdo con lo que los administradores de la entidad consideren pertinente, sin perjuicio de aquella que sea de carácter privilegiado, confidencial o reservado, respecto de la cual deberán adoptarse todas las medidas que resulten necesarias para su protección, incluyendo lo relacionado con su almacenamiento, acceso, conservación, custodia y divulgación. Se entiende por información sujeta a reserva o privilegiada aquella a la cual sólo tienen acceso directo ciertas personas (sujetos calificados), en razón de su profesión u oficio, la cual, por su carácter, es confidencial, ya que de conocerse podría ser utilizada con el fin de obtener provecho o beneficio para quien la suministra o para un tercero.

Con tal propósito, los administradores de la entidad deben definir políticas de seguridad de la información, mediante la ejecución de un programa que comprenda, entre otros, el diseño, implantación, divulgación, educación y mantenimiento de las estrategias y mecanismos para administrar la seguridad de la información.

La confidencialidad es uno de los elementos más importantes de la seguridad de la información y tiene como propósito garantizar que ella sólo pueda ser conocida, consultada y divulgada por personas autorizadas. Este elemento está directamente relacionado con el principio de "prudencia", necesario para evitar la filtración, difusión inapropiada y tergiversación de la información.

Lo anterior se entiende sin perjuicio de lo establecido en el Título I, Capítulo décimo segundo de la presente circular respecto a los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios.

7.5.4.2 Comunicación

La entidad debe mantener una comunicación eficaz, que fluya en todas las direcciones a través de todas las áreas de la organización (de arriba hacia abajo, a la inversa y transversalmente).

Cada empleado debe conocer el papel que desempeña dentro de la organización y dentro del SCI y la forma en la cual las actividades a su cargo están relacionadas con el trabajo de los demás. Para el efecto, la entidad deberá disponer de medios para comunicar la información significativa, tanto al interior de la organización como hacia su exterior.

Como parte de una adecuada administración de la comunicación, se deben identificar cuando menos los siguientes elementos:

i. Canales de comunicación

ii. Responsables de su manejo

iii. Requisitos de la información que se divulga

iv. Frecuencia de la comunicación

v. Responsables

vi. Destinatarios

vii. Controles al proceso de comunicación

Adicionalmente los administradores de la entidad deben adoptar los procedimientos necesarios para garantizar la calidad, oportunidad, veracidad, suficiencia y en general el cumplimiento de todos los requisitos que incidan en la credibilidad y utilidad de la información que la respectiva organización revela al público.

El principio de transparencia que rige el mercado de valores y el sistema financiero exige que se proporcione a los consumidores financieros y demás participantes del mercado, en igualdad de condiciones, información oportuna, suficiente y de calidad sobre los datos y hechos relevantes que permitan una adecuada formación de precios y la adopción de decisiones debidamente fundamentadas. De esta manera se disminuye el riesgo de desigualdad de oportunidades para actuar en el mercado, derivado del manejo de información privilegiada.

En tal sentido, los administradores de las entidades supervisadas deben adoptarse las medidas y los controles que resulten necesarios para evitar el suministro de información privilegiada a uno o más participantes del mercado.

7.5.5 Monitoreo

Es el proceso que se lleva a cabo para verificar la calidad de desempeño del control interno a través del tiempo. Se realiza por medio de la supervisión continua que realizan los jefes o líderes de cada área o proceso como parte habitual de su responsabilidad frente al control interno (vicepresidentes, gerentes, directores, etc. dentro del ámbito de la competencia de cada uno de ellos), así como de las evaluaciones periódicas puntuales que realicen la auditoria interna u órgano equivalente, el presidente o máximo responsable de la organización y otras revisiones dirigidas.

El SCI no puede ser estático, sino dinámico, ajustándose en forma permanente a las nuevas situaciones del entorno. Con tal fin, es importante que se establezcan controles automáticos o alarmas tanto en los sistemas automatizados como en los manuales, de manera que permanentemente se valore la calidad y el desempeño del sistema en el tiempo y se realicen las acciones de mejoramiento necesarias, pues ello equivale a una actividad de supervisión y administración. Para efectos de lo anterior, dicho monitoreo se debe realizar en todas las etapas de los procesos y en tiempo real en el curso de las operaciones.

Las evaluaciones permanentes y separadas permiten a la alta dirección determinar si el control interno está presente y funciona en forma adecuada en el tiempo.

Las deficiencias de control interno deben ser identificadas y comunicadas de manera oportuna a las partes responsables de tomar acciones correctivas y, cuando resulten materiales, informarse también a la junta directiva u órgano equivalente.

7.5.6 Evaluaciones independientes

Aunque los procedimientos de seguimiento permanente, así como la autoevaluación de cada área, proporcionan una retroalimentación importante, es necesario realizar adicionalmente evaluaciones que se centren directamente sobre la efectividad del SCI, las cuales deben ser realizadas por personas totalmente independientes del proceso, como requisito indispensable para garantizar su imparcialidad y objetividad.

Se cumple con el requisito de estas evaluaciones independientes a través de los auditores internos y del revisor fiscal, en la medida en que el alcance de la evaluación hecha por éstos respecto al control interno de la respectiva entidad tenga el alcance y la cobertura requeridos en la presente circular.

Lo anterior sin perjuicio de que la administración, si así lo considera conveniente, utilice como práctica de buen gobierno corporativo el trabajo de auditores externos para revisar la efectividad del control interno.

Puede emplearse una combinación de varios esquemas, según lo que la administración considere necesario.

Las debilidades resultado de esta evaluación y sus recomendaciones de mejoramiento, deben ser reportadas de manera ascendente, informando sobre asuntos representativos de manera inmediata al Comité de Auditoría, y haciéndoles seguimiento.

7.6 ÁREAS Especiales dentro del Sistema de Control Interno

El SCI debe abarcar todas las áreas de la organización, aplicando para cada una de ellas los objetivos, principios, elementos y actividades de control, información, comunicación y otros fundamentos del sistema tratados en los numerales anteriores del presente capítulo.

No obstante, por su particular importancia se considera pertinente entrar a analizar algunos aspectos del SCI relacionados con las áreas contable y tecnológica.

7.6.1. Control Interno en la gestión contable

La información financiera y contable de una entidad, se constituye en una herramienta fundamental para que la administración pueda adoptar sus decisiones en forma oportuna y contando con suficientes elementos de juicio. Por ello, la organización debe asegurarse de que todos los estados financieros, informes de gestión y demás reportes que suministra sean confiables.

El término confiable en este contexto se refiere a la preparación de estados financieros y otros informes que presenten en forma razonable la situación financiera y resultados de la entidad y que cumplan plenamente con las normas, principios y reglamentos que resulten aplicables. Bajo esta referencia resulta claro que un eficiente SCI contable es la base sobre la que se genera información financiera oportuna, razonable y veraz. El diseño e implementación de este sistema son responsabilidad de la administración, así como la correcta preparación y presentación de los estados financieros y sus correspondientes notas.

Los representantes legales serán responsables del establecimiento y mantenimiento de adecuados sistemas de revelación y control de la información financiera, para lo cual deberán diseñar procedimientos de control sobre la calidad, suficiencia y oportunidad de la misma. Además, deberán verificar la operatividad de los controles establecidos al interior de la correspondiente entidad, e incluir en el informe de gestión que los administradores presenten a la asamblea general de accionistas u órgano equivalente la evaluación sobre el desempeño de los mencionados sistemas de revelación y control.

Igualmente, los representantes legales serán responsables de informar ante el Comité de Auditoría todas las deficiencias significativas encontradas en el diseño y operación de los

controles internos que hubieran impedido a la sociedad registrar, procesar, resumir y presentar adecuadamente la información financiera de la misma. También deberán reportar los casos de fraude que hayan podido afectar la calidad de la información financiera, así como cambios en la metodología de evaluación de la misma.

En este sentido, representa especial importancia para la administración de las entidades establecer al interior de la organización un apropiado SCI contable que garantice que los estados financieros que se presentan a la junta directiva, a las asambleas, a los entes de supervisión, fiscalización y control y que finalmente son objeto de publicación, reflejen en forma fidedigna la realidad económica de la entidad.

En virtud de todo lo anterior, a continuación se precisan algunos aspectos que deben tener en cuenta las entidades supervisadas por la SFC para el adecuado funcionamiento del SCI, reiterando que para el efecto se deben aplicar en su totalidad los fundamentos señalados en los numerales 7.4 y 7.5 del presente capítulo.

7.6.1.1 Políticas y procedimientos contables.

Las actividades de control contable normalmente implican dos componentes: una política contable, que establece lo que debe hacerse y unos procedimientos para llevarla a cabo. Bajo este criterio, las distintas instancias y el SCI contable de las entidades supervisadas, deben ser efectivos y eficientes, esto se refiere básicamente al cumplimiento de las actividades diarias asignadas, expresadas en las políticas y procedimientos establecidos por la entidad.

Lo anterior conlleva a que los administradores tomen las acciones necesarias para abordar los riesgos contables que implican no solo la forma correcta de hacer las cosas sino dirigir las tareas hacia el logro de los objetivos de la entidad. De ahí que resulte indispensable que las entidades implementen la ejecución de las políticas contables a través de toda la organización, en todos los niveles y en todas las funciones que intervienen en el proceso contable e incluyan el establecimiento de unos procedimientos obligatorios para todas las actividades de dicho proceso entre los que se encuentran:

i. Supervisión de los procesos contables.

ii. Evaluaciones y supervisión de los aplicativos, accesos a la información y archivos, utilizados en los procesos contables.

iii. Presentación de informes de seguimiento.

iv. Validaciones de calidad de la información, revisando que las transacciones u operaciones sean veraces y están adecuadamente calculadas y valoradas aplicando principios de medición y reconocimiento.

v. Comparaciones, inventarios y análisis de los activos de la entidad, realizadas a través de fuentes internas y externas.

vi. Supervisión de los Sistemas de Información.

vii. Controles generales.

viii. Autorización apropiada de las transacciones por los órganos de dirección y administración.

ix. Autorización y control de documentos

x. Autorizaciones y establecimiento de límites

7.6.1.2 Controles sobre los Sistemas de Información Contable.

Teniendo en cuenta que la operación del proceso contable depende en gran medida de sus sistemas de información, es necesario adoptar controles que garanticen la exactitud y validez de la información.

Se pueden usar dos grandes grupos de actividades de control de sistemas de información:

i. Controles generales, que rigen para todas las aplicaciones de sistemas y ayudan a asegurar su continuidad y operación adecuada. Dentro de éstos se incluyen aquellos que se hagan sobre la administración de la tecnología de información, su infraestructura, la administración de seguridad y la adquisición, desarrollo y mantenimiento del software.

ii. Controles de aplicación, los cuales incluyen pasos a través de sistemas tecnológicos y manuales de procedimientos relacionados. Se centran directamente en la suficiencia, exactitud, autorización y validez de la captura y procesamiento de datos. Ayudan a asegurar que los datos se capturan o generan en el momento de necesitarlos, que las aplicaciones de soporte estén disponibles y que los errores de interfase se detecten rápidamente. Un objetivo importante de los controles de aplicación es prevenir que los errores se introduzcan en el sistema, así como detectarlos y corregirlos una vez involucrados en él. Si se diseñan correctamente, pueden facilitar el control sobre los datos introducidos en el sistema.

7.6.2. Normas de Control Interno para la gestión de la Tecnología

La tecnología es imprescindible para el cumplimiento de los objetivos y la prestación de servicios de las entidades a sus diferentes grupos de interés, en condiciones de seguridad, calidad y efectividad. Por lo tanto, se tendrá que velar porque el diseño del SCI para la gestión de la tecnología responda a las políticas, necesidades y expectativas de la entidad, así como a las exigencias normativas sobre la materia. De otra parte, el sistema deberá ser objeto de evaluación y el mejoramiento continuo con el propósito de contribuir al logro de los objetivos institucionales y a la prestación de los servicios en las condiciones señaladas.

Las entidades deben establecer, desarrollar, documentar y comunicar políticas de tecnología y definir los recursos, procesos, procedimientos, metodologías y controles necesarios para asegurar su cumplimiento.

Las políticas deberán ser revisadas por lo menos una vez al año o al momento de presentarse cambios significativos en el ambiente operacional o del negocio, para lo cual la administración deberá contar con estándares, políticas, directrices y procedimientos debidamente aprobados, orientados a cubrir los siguientes aspectos:

i. Plan estratégico de tecnología.

ii. Infraestructura de tecnología.

iii. Relaciones con proveedores.

iv. Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio

electrónico.

v. Administración de proyectos de sistemas.

vi. Administración de la calidad.

vii. Adquisición de tecnología.

viii. Adquisición y mantenimiento de software de aplicación.

ix. Instalación y acreditación de sistemas.

x. Administración de cambios.

xi. Administración de servicios con terceros.

xii. Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.

xiii. Continuidad del negocio.

xiv. Seguridad de los sistemas.

xv. Educación y entrenamiento de usuarios.

xvi. Administración de los datos.

xvii. Administración de instalaciones.

xviii. Administración de operaciones de tecnología.

xix. Documentación.

En el caso de las entidades vigiladas, lo dispuesto en el presente numeral y sus subdivisiones se entiende sin perjuicio del cumplimiento de las instrucciones especiales impartidas por esta Superintendencia en materia de riesgo operativo –SARO y de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios, las cuales deberán cumplirse dentro de los plazos y condiciones específicos establecidos para el efecto.

Por la relevancia que representan algunas de las políticas previamente identificadas, conviene a continuación señalar en forma particular algunas de ellas.

7.6.2.1 Plan Estratégico de Tecnología.

Las entidades deberán realizar un proceso de planeación estratégica de tecnología, a intervalos de tiempo regulares, con el propósito de lograr el cumplimiento de los objetivos de la organización a través de las oportunidades que brinda la tecnología a su alcance.

El plan estratégico de tecnología deberá estar alineado con el plan estratégico institucional y en él se deberán contemplar adicionalmente, al menos, los siguientes aspectos:

i. Análisis de cómo soporta la tecnología los objetivos del negocio.

ii. Evaluación de la tecnología actual.

iii. Estudios de mercado y factibilidad de alternativas tecnológicas que respondan a las necesidades de la entidad.

iv. Planes operacionales estableciendo metas claras y concretas.

7.6.2.2 Administración de la Calidad.

Con el objeto de satisfacer las necesidades de sus clientes (internos y externos), las entidades deberán llevar a cabo la planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad de la tecnología que contengan:

i. Programas para establecer una cultura de calidad de la tecnología en toda la entidad.

ii. Planes concretos de calidad de la tecnología.

iii. Responsables por el aseguramiento de la calidad.

iv. Prácticas de control de calidad.

v. Metodología para el ciclo de vida de desarrollo de sistemas.

vi. Metodología de prueba y documentación de programas y sistemas.

vii. Diseño de informes de aseguramiento de la calidad.

viii. Capacitación de usuarios finales y del personal de aseguramiento de la calidad.

ix. Desarrollo de una base de conocimiento de aseguramiento de la calidad.

El sistema de administración de la calidad deberá ser objeto de evaluaciones periódicas para ajustarlo a las necesidades de la entidad.

7.6.2.3 Administración de Cambios.

Con el fin de minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, se deberá diseñar un sistema de administración que permita el análisis, implementación y seguimiento de los cambios requeridos y llevados a cabo a la infraestructura de tecnología que posea la entidad. Como mínimo se tendrán que contemplar los siguientes aspectos:

i. Identificación clara del cambio a realizar en la infraestructura.

ii. Categorización, priorización y procedimientos de emergencia a llevar a cabo durante el cambio.

iii. Evaluación del impacto que ocasiona el cambio en la infraestructura.

iv. Procedimiento de autorización de los cambios.

v. Procedimiento de administración de versiones.

vi. Políticas de distribución del software.

vii. Obtención de herramientas automatizadas para realizar los cambios.

viii. Procedimientos para la administración de la configuración.

ix. Rediseño de los procesos del negocio que se vean impactados por el cambio en la infraestructura.

7.6.2.4 Seguridad de los Sistemas.

Con el objeto de salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, le corresponderá a las entidades supervisadas establecer controles de acceso lógico que aseguren que los sistemas, datos y programas están restringidos exclusivamente a usuarios autorizados para lo cual se deberá contar con procedimientos y recursos sobre los siguientes aspectos:

i. Autorización, autenticación y control de acceso.

ii. Identificación de usuarios y perfiles de autorización los cuales deberán ser otorgados de acuerdo con la necesidad de tener y necesidad de conocer.

iii. Manejo de incidentes, información y seguimiento.

iv. Prevención y detección de código malicioso, virus, entre otros.

v. Entrenamiento de usuarios.

vi. Administración centralizada de la seguridad.

7.6.2.5 Administración de los datos.

Para que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento en los sistemas de información, las entidades tendrán que establecer controles generales y de aplicación sobre la operación de la tecnología, adicionales a los establecidos en el numeral 7.5.4.1, atendiendo como mínimo los siguientes aspectos:

i. Establecer controles de entrada, procesamiento y salida para garantizar la autenticidad e integridad de los datos.

ii. Verificar la exactitud, suficiencia y validez de los datos de transacciones que sean capturados para su procesamiento (generados por personas, por sistemas o entradas de interfase).

iii. Preservar la segregación de funciones en el procesamiento de datos y la verificación rutinaria del trabajo realizado. Los procedimientos deberán incluir controles de actualización adecuados, como totales de control "corrida a corrida" y controles de actualización de archivos maestros.

iv. Establecer procedimientos para que la validación, autenticación y edición de los datos sean llevadas a cabo tan cerca del punto de origen como sea posible.

v. Definir e implementar procedimientos para prevenir el acceso a la información y software sensitivos de computadores, discos y otros equipos o medios, cuando hayan sido sustituidos o se les haya dado otro uso. Tales procedimientos deberán garantizar que los datos marcados como eliminados no puedan ser recuperados por cualquier individuo interno o tercero ajeno a la entidad.

vi. Establecer los mecanismos necesarios para garantizar la integridad continua de los datos almacenados.

vii. Definir e implementar procedimientos apropiados y prácticas para transacciones electrónicas que sean sensitivas y críticas para la organización, velando por su integridad y autenticidad.

viii. Establecer controles para garantizar la integración y consistencia entre plataformas.

7.6.2.6 Administración de las instalaciones.

Con el objeto de proporcionar un ambiente físico conveniente que proteja los equipos y el personal de tecnología contra peligros naturales o fallas humanas, las entidades deberán instalar controles físicos y ambientales adecuados que sean revisados regularmente para garantizar su buen funcionamiento teniendo en cuenta, entre otros, los siguientes aspectos:

i. Acceso a las instalaciones.

ii. Identificación clara del sitio.

iii. Controles de seguridad física.

iv. Definición de políticas de inspección y escalamiento de problemas.

v. Planeamiento de continuidad del negocio y administración de crisis.

vi. Salud y seguridad del personal.

vii. Políticas de mantenimiento preventivo.

viii. Protección contra amenazas ambientales.

ix. Monitoreo automatizado.

7.7 responsabilidades dentro del sistema de control

7.7.1 Órganos Internos

7.7.1.1 Junta Directiva u órgano equivalente

Los miembros de las Juntas Directivas u órgano equivalente, como principales gestores del gobierno corporativo, deben realizar su gestión con profesionalismo, integridad, competencia e independencia, dedicándole el tiempo necesario. Así mismo deben ser transparentes en su gestión, procurando tener un buen conocimiento de los riesgos que involucran los productos que ofrece la empresa; evaluar con profundidad los riesgos involucrados en los instrumentos de inversión que ésta utiliza y apoyar la labor de los órganos de fiscalización y control.

De la junta directiva u órgano equivalente debe provenir la autoridad, orientación y vigilancia al personal directivo superior, de manera que sus miembros deberán contar con experiencia y conocimientos adecuados acerca de las actividades, los objetivos y la estructura de la respectiva entidad.

7.7.1.1.1. Funciones generales

Sin perjuicio de las obligaciones especiales asignadas a este órgano en otras disposiciones legales, estatutarias o en reglamentos, en materia de control interno, en cumplimiento de los deberes que le señala el artículo 23 de la Ley 222 de 1995, la junta directiva u órgano equivalente es la instancia responsable de:

i. Participar activamente en la planeación estratégica de la entidad y su seguimiento, determinando las necesidades de redireccionamiento estratégico cuando se requiera.

ii. Definir y aprobar las estrategias y políticas generales relacionadas con el SCI, con fundamento en las recomendaciones del Comité de Auditoría.

iii. Establecer mecanismos de evaluación formal a la gestión de los administradores y sistemas de remuneración e indemnización atados al cumplimiento de objetivos a largo plazo y los niveles de riesgo.

iv. Definir claras líneas de responsabilidad y rendición de cuentas a través de la organización.

v. Analizar el proceso de gestión de riesgo existente y adoptar las medidas necesarias para fortalecerlo en aquellos aspectos que así lo requieran, lo cual comprende entre otros aspectos establecer protocolos de crisis que incluyan planes de contingencia.

vi. Designar a los directivos de las áreas encargadas del SCI y de la gestión de riesgos, salvo que el régimen aplicable a la respectiva entidad o sus estatutos establezcan una instancia diferente para el efecto.

vii. Adoptar las medidas necesarias para garantizar la independencia del auditor interno y hacer seguimiento a su cumplimiento.

viii. Conocer los informes relevantes respecto del SCI que sean presentados por los diferentes órganos de control o supervisión e impartir las órdenes necesarias para que se adopten las recomendaciones y correctivos a que haya lugar.

ix. Solicitar y estudiar, con la debida anticipación, toda la información relevante que requiera para contar con la ilustración suficiente para adoptar responsablemente las decisiones que le corresponden y solicitar asesoría experta, cuando sea necesario.

x. Requerir las aclaraciones y formular las objeciones que considere pertinentes respecto a los asuntos que se someten a su consideración.

xi. Aprobar los recursos suficientes para que el SCI cumpla sus objetivos.

xii. Efectuar seguimiento en sus reuniones ordinarias a través de informes periódicos que le presente el Comité de Auditoría, sobre la gestión de riesgos en la entidad y las medidas adoptadas para el control o mitigación de los riesgos más relevantes, por lo menos cada seis (6) meses, o con una frecuencia mayor si así resulta procedente.

xiii. Evaluar las recomendaciones relevantes sobre el SCI que formulen el Comité de Auditoría y los otros órganos de control interno y externos, adoptar las medidas pertinentes y hacer seguimiento a su cumplimiento.

xiv. Analizar los informes que presente el oficial de cumplimiento respecto de las labores realizadas para evitar que la entidad sea utilizada como instrumento para la realización de actividades delictivas, evaluar la efectividad de los controles implementados y de las recomendaciones formuladas para su mejoramiento.

xv. Evaluar los estados financieros, con sus notas, antes de que sean presentados a la asamblea de accionistas o máximo órgano social, teniendo en cuenta los informes y recomendaciones que le

presente el Comité de Auditoría.

xvi. Presentar al final de cada ejercicio a la Asamblea General de Accionistas, junta de socios o máximo órgano social un informe sobre el resultado de la evaluación del SCI y sus actuaciones sobre el particular.

Todas las decisiones y actuaciones que se produzcan en desarrollo de las atribuciones antes mencionadas deberán constar por escrito en el acta de la reunión respectiva y estar debidamente motivadas. La junta directiva u órgano equivalente determinará la información que deba ser divulgada a los diferentes niveles de la organización, de acuerdo con lo que considere pertinente.

7.7.1.2. Comité de Auditoría

Para el adecuado cumplimiento de la labor que le corresponde a las juntas directivas u órganos equivalentes de las entidades supervisadas por la SFC, éstas deben contar con un Comité de Auditoría, dependiente de ese órgano social, encargado de la evaluación del control interno de la misma, así como a su mejoramiento continuo, sin que ello implique una sustitución a la responsabilidad que de manera colegiada le corresponde a la junta directiva u órgano equivalente en la materia.

7.7.1.2.1 Funciones del Comité

El Comité de Auditoría tendrá como funciones primordiales las siguientes:

i. Aprobar la estructura, procedimientos y metodologías necesarios para el funcionamiento del SCI.

ii. Señalar las responsabilidades, atribuciones y límites asignados a los diferentes cargos y áreas respecto de la administración del SCI, incluyendo la gestión de riesgos.

iii. Evaluar la estructura del control interno de la entidad de forma tal que se pueda establecer si los procedimientos diseñados protegen razonablemente los activos de la entidad, así como los de terceros que administre o custodie, y si existen controles para verificar que las transacciones están siendo adecuadamente autorizadas y registradas.

iv. Velar que los administradores suministren la información requerida por los órganos de control para la realización de sus funciones.

v. Velar porque la preparación, presentación y revelación de la información financiera se ajuste a lo dispuesto en las normas aplicables, verificando que existen los controles necesarios.

vi. Estudiar los estados financieros y elaborar el informe correspondiente para someterlo a consideración de la junta directiva, con base en la evaluación no sólo de los proyectos correspondientes, con sus notas, sino también de los dictámenes, observaciones de las entidades de control, resultados de las evaluaciones efectuadas por los comités competentes y demás documentos relacionados con los mismos.

vii. Diseñar, implementar y evaluar programas y controles para prevenir, detectar y responder adecuadamente a los riesgos de fraude y mala conducta, entendiendo por fraude un acto intencionado cometido para obtener una ganancia ilícita, y por mala la violación de leyes, reglamentos o políticas internas.

viii. Supervisar las funciones y actividades de la auditoría interna u órgano que haga sus veces, con el objeto de determinar su independencia y objetividad en relación con las actividades que audita, determinar la existencia de limitaciones que impidan su adecuado desempeño y verificar si el alcance de su labor satisface las necesidades de control de la entidad.

ix. Efectuar seguimiento sobre los niveles de exposición de riesgo, sus implicaciones para la entidad y las medidas adoptadas para su control o mitigación, por lo menos cada tres (3) meses, o con una frecuencia mayor si así resulta procedente, y presentar a la Junta Directiva un informe sobre los aspectos más importante de la gestión realizada.

x. Evaluar los informes de control interno practicados por los auditores internos, contraloría, contralor normativo u otros órganos, verificando que la administración haya atendido sus sugerencias y recomendaciones.

xi. Hacer seguimiento al cumplimiento de las instrucciones dadas por la junta directiva u órgano equivalente, en relación con el SCI.

xii. Solicitar los informes que considere convenientes para el adecuado desarrollo de sus funciones.

xiii. Analizar el funcionamiento de los sistemas de información, su confiabilidad e integridad para la toma de decisiones.

xiv. Presentar al máximo órgano social, por conducto de la junta directiva, los candidatos para ocupar el cargo de revisor fiscal, sin perjuicio del derecho de los accionistas de presentar otros candidatos en la respectiva reunión. En tal sentido, la función del comité será recopilar y analizar la información suministrada por cada uno de los candidatos y someter a consideración del máximo órgano social los resultados del estudio efectuado.

xv. Elaborar el informe que la junta directiva deberá presentar al máximo órgano social respecto al funcionamiento del SCI, el cual deberá incluir entre otros aspectos:

a. Las políticas generales establecidas para la implementación del SCI de la entidad.

b. El proceso utilizado para la revisión de la efectividad del SCI, con mención expresa de los aspectos relacionados con la gestión de riesgos.

c. Las actividades más relevantes desarrolladas por el Comité de Auditoría.

d. Las deficiencias materiales detectadas, las recomendaciones formuladas y las medidas adoptadas, incluyendo entre otros temas aquellos que pudieran afectar los estados financieros y el informe de gestión.

e. Las observaciones formuladas por los órganos de supervisión y las sanciones impuestas, cuando sea del caso.

f. Si existe o no un departamento de auditoría interna o área equivalente. Si existe, presentar la evaluación de la labor realizada por la misma, incluyendo entre otros aspectos el alcance del trabajo desarrollado, la independencia de la función y los recursos que se tienen asignados. En caso de no existir, señalar las razones concretas por las cuales no se ha considerado pertinente contar con dicho departamento o área.

xvi. Las demás que le fije la junta directiva, en su reglamento interno.

7.7.1.2.2 Conformación del Comité

El Comité deberá estar integrado por lo menos por tres (3) miembros de la junta directiva u órgano equivalente, quienes deben tener experiencia, ser conocedores de los temas relacionados con las funciones asignadas al referido órgano social y ser en su mayoría independientes, esto último para aquellas entidades que por disposición legal o estatutaria cuentan con miembros independientes en el referido órgano social, entendiendo por independientes aquellas personas que en ningún caso sean:

i. Empleados o directivos de la entidad o de alguna de sus filiales, subsidiarias o controlantes, incluyendo aquellas personas que hubieren tenido tal calidad durante el año inmediatamente anterior a la designación, salvo que se trate de la reelección de una persona independiente.

ii. Accionistas que directamente o en virtud de convenio dirijan, orienten o controlen la mayoría de los derechos de voto de la entidad o que determinen la composición mayoritaria de los órganos de administración, de dirección o de control de la misma.

iii. Socios o empleados de asociaciones o sociedades que presten servicios de asesoría o consultoría a la entidad o a las empresas que pertenezcan al mismo grupo económico del cual forme parte esta, cuando los ingresos por dicho concepto representen para aquellos, el veinte por ciento (20%) o más de sus ingresos operacionales.

iv. Empleado o directivo de una fundación, asociación o sociedad que reciba donativos importantes de la entidad. Se consideran donativos importantes aquellos que representen más del veinte por ciento (20%) del total de donativos recibidos por la respectiva institución.

v. Administrador de una entidad en cuya junta directiva participe un representante legal de la entidad.

vi. Persona que reciba de la entidad alguna remuneración diferente a los honorarios como miembro de la junta directiva, del Comité de Auditoría o de cualquier otro comité creado por la junta directiva.

A las reuniones del Comité puede ser citado cualquier funcionario de la entidad, con el fin de suministrar la información que se considere pertinente acerca de asuntos de su competencia.

7.7.1.2.3 Reglamento Interno

La junta directiva u órgano equivalente de las entidades supervisadas deberá adoptar el reglamento de funcionamiento del comité, incluyendo para el efecto, además de las funciones aquí consagradas, todas aquellas que en su criterio sean propias de la institución y se adapten a sus necesidades. Dicho reglamento deberá ajustarse a lo dispuesto en la presente circular, dentro de los tres (3) meses siguientes a la entrada en vigencia de esta norma y deberá mantenerse a disposición de la SFC, cuando lo solicite.

7.7.1.2.4 Periodicidad de las reuniones

El Comité de Auditoría deberá reunirse por lo menos cada tres (3) meses, o con una frecuencia mayor si así lo establece su reglamento o lo ameritan los resultados de las evaluaciones del SCI.

7.7.1.2.5 Informes sobre las tareas desarrolladas y las conclusiones alcanzadas por el Comité

Las decisiones y actuaciones del Comité de Auditoria deberán quedar consignadas en actas, las cuales deberán cumplir con lo dispuesto en el artículo 189 del Código de Comercio. Los documentos conocidos por el Comité que sean sustento de sus decisiones deberán formar parte integral de las actas, por lo cual en caso de no ser transcritos deberán presentarse como anexos de las mismas. Así, cada vez que se entregue un acta, deberá suministrarse al interesado tanto el cuerpo principal de la misma como todos sus anexos, los cuales deberán estar adecuadamente identificados y foliados, y mantenerse bajo medidas adecuadas de conservación y custodia.

Cuando se detecten situaciones que revistan importancia significativa, se deberá remitir un informe especial a la junta directiva u órgano equivalente y al representante legal.

La junta directiva deberá presentar a la Asamblea General de Accionistas o asociados, al cierre del ejercicio económico, un informe sobre las labores desarrolladas por el Comité.

7.7.1.3. Representante Legal

Sin perjuicio de las obligaciones especiales asignadas al representante legal en otras disposiciones legales, estatutarias o en reglamentos, en materia de control interno el representante legal es la instancia responsable de:

i. Implementar las estrategias y políticas aprobadas por la junta directiva u órgano equivalente en relación con el SCI.

ii. Comunicar las políticas y decisiones adoptadas por la junta directiva u órgano equivalente a todos y cada uno de los funcionarios dentro de la organización, quienes en desarrollo de sus funciones y con la aplicación de procesos operativos apropiados deberán procurar el cumplimiento de los objetivos trazados por la dirección, siempre sujetos a los lineamientos por ella establecidos.

iii. Poner en funcionamiento la estructura, procedimientos y metodologías inherentes al SCI, en desarrollo de las directrices impartidas por la junta directiva. garantizando una adecuada segregación de funciones y asignación de responsabilidades.

iv. Implementar los diferentes informes, protocolos de comunicación, sistemas de información y demás determinaciones de la Junta relacionados con SCI.

v. Fijar los lineamientos tendientes a crear la cultura organizacional de control, mediante la definición y puesta en práctica de las políticas y los controles suficientes, la divulgación de las normas éticas y de integridad dentro de la institución y la definición y aprobación de canales de comunicación, de tal forma que el personal de todos los niveles comprenda la importancia del control interno e identifique su responsabilidad frente al mismo.

vi. Realizar revisiones periódicas a los manuales y códigos de ética y de gobierno corporativo.

vii. Proporcionar a los órganos de control internos y externos, toda la información que requieran para el desarrollo de su labor.

viii. Proporcionar los recursos que se requieran para el adecuado funcionamiento del SCI, de conformidad con lo autorizado por la junta directiva u órgano equivalente.

ix. Velar por el estricto cumplimiento de los niveles de autorización, cupos u otros límites o controles establecidos en las diferentes actividades realizadas por la entidad, incluyendo las adelantadas con administradores, miembros de junta, matriz, subordinadas y demás vinculados económicos.

x. Certificar que los estados financieros y otros informes relevantes para el público no contienen vicios, imprecisiones o errores que impidan conocer la verdadera situación patrimonial o las operaciones de la correspondiente entidad.

xi. Establecer y mantener adecuados sistemas de revelación y control de la información financiera, para lo cual deberán diseñar procedimientos de control y revelación para que la información financiera sea presentada en forma adecuada.

xii. Establecer mecanismos para la recepción de denuncias (líneas telefónicas, buzones especiales en el sitio Web, entre otros) que faciliten a quienes detecten eventuales irregularidades ponerlas en conocimiento de los órganos competentes de la entidad.

xiii. Definir políticas y un programa antifraude, para mitigar los riesgos de una defraudación en la entidad.

xiv. Verificar la operatividad de los controles establecidos al interior de la entidad.

xv. Incluir en su informe de gestión un aparte independiente en el que se de a conocer al máximo órgano social la evaluación sobre el desempeño del SCI en cada uno de los elementos señalados en el numeral 7.5 de la presente circular. En el caso de los grupos empresariales, la evaluación sobre la eficacia del SCI que expida el representante legal de la matriz debe incluir también a las entidades subordinadas (filiales o subsidiarias).

En general el representante legal es el responsable de implementar los procedimientos de control y revelación, verificar su operatividad al interior de la correspondiente entidad y su adecuado funcionamiento, para lo cual no debe limitarse a la revisión de los informes que le presenten las diferentes áreas de la organización, sino que debe demostrar la ejecución de acciones concretas para verificar la veracidad y confiabilidad del contenido de dichos informes y la eficacia de los controles.

El representante legal debe dejar constancia documental de sus actuaciones en esta materia, mediante memorandos, cartas, actas de reuniones o los documentos que resulten pertinentes para el efecto.

Adicionalmente, debe mantener a disposición del auditor interno, el revisor fiscal y demás órganos de supervisión o control los soportes necesarios para acreditar la correcta implementación del SCI, en sus diferentes elementos, procesos y procedimientos.

7.7.1.4 Auditoría Interna o departamento que cumpla funciones equivalentes

7.7.1.4.1 Definición

La auditoría interna es una actividad que se fundamenta en criterios de independencia y objetividad de aseguramiento[2] y consulta[3], concebida para agregar valor y mejorar las operaciones de una organización, ayudándola a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

En tal sentido y ante la importancia que representa la auditoria interna en el control y gestión exitosos de una organización, la SFC estima necesario que las entidades bajo su supervisión que cuenten con un auditor interno, contralor o funcionario que cumpla funciones equivalentes, adopten como referente y cumplan normas y parámetros mínimos que garanticen el ejercicio profesional e idóneo de la auditoría interna, acorde con los estándares y mejores prácticas internacionales[4].

Para las entidades supervisadas por esta Superintendencia que pertenezcan al sector público, se admitirá el enfoque de auditoría interna establecido en el modelo MECI. En todo caso, las oficinas o áreas de control interno, auditoría interna o quienes hagan sus veces deberán cumplir, en lo que no sea contrario a las disposiciones legales aplicables, los lineamientos básicos de la presente Circular.

Las entidades que no tengan un departamento de Auditoría Interna o dependencia que cumpla funciones equivalentes deben indicar expresamente en el informe de gestión que los administradores presentan al cierre de cada ejercicio al máximo órgano social las razones por las cuales no consideran procedente que la organización cuente con el mencionado departamento.

7.7.1.4.2 Normas para el Ejercicio de la Auditoría Interna.

En el desarrollo de la actividad de Auditoría Interna o su equivalente, deberá darse aplicación, entre otras a las siguientes normas:

7.7.1.4.2.1 Normas sobre Atributos.

7.7.1.4.2.1.1 Propósito, Autoridad y Responsabilidad

El propósito, la autoridad y la responsabilidad de la actividad de Auditoría Interna deben estar formalmente definidos en un estatuto (documento) debidamente aprobado por la junta directiva u órgano equivalente, en donde quede establecido un acuerdo con la alta dirección de la entidad respecto de la función y responsabilidad de la actividad de Auditoría Interna, su posición dentro de la organización, la autorización al auditor para que tenga acceso a los registros, al personal y a los bienes relevantes para la ejecución de los trabajos y la definición del ámbito de actuación de las actividades de auditoría interna.

7.7.1.4.2.1.2 Independencia y Objetividad

La actividad de auditoria interna debe ser independiente, y los auditores internos deben ser objetivos en el cumplimiento de sus trabajos a través de una actitud imparcial y neutral, buscando siempre evitar conflictos de intereses. Dentro de este contexto, como una práctica de buen gobierno corporativo, se considera conveniente que el auditor interno o quien haga sus veces sea nombrado por la junta directiva u órgano equivalente.

Si la independencia u objetividad en cualquier momento se viese comprometida de hecho o en apariencia, los detalles del impedimento deben darse a conocer por escrito a la junta directiva u órgano equivalente.

7.7.1.4.2.1.3 Pericia y debido cuidado profesional.

Tanto el auditor interno como su equipo de trabajo deben reunir los conocimientos, las aptitudes y las competencias necesarias para cumplir con sus responsabilidades. El auditor interno debe

contar con asesoría y asistencia competente para aquellas áreas especializadas respecto de las cuales él o su personal no cuenten con los conocimientos necesarios.

Los auditores internos deben cumplir su trabajo con el cuidado y la pericia que se esperan de un especialista razonablemente prudente y competente. El debido cuidado profesional no implica infalibilidad.

7.7.1.4.2.1.4 Programa de Aseguramiento de Calidad y Cumplimiento

El auditor interno debe desarrollar y mantener un programa de aseguramiento de calidad y mejora que cubra todos los aspectos de la actividad de auditoría interna y revise continuamente su eficacia. Este programa incluye evaluaciones de calidad externas e internas periódicas y supervisión interna continua. Cada parte del programa debe estar diseñada para ayudar a la actividad de auditoría interna a añadir valor y a mejorar las operaciones de la organización y a proporcionar aseguramiento de que la actividad de auditoría interna cumple con las normas aplicables a esta actividad y el Código de Ética de los auditores.

Si bien la actividad de auditoría interna debe lograr el cumplimiento total de las normas de general aceptación para esta actividad, puede haber casos en los cuales esta meta no se logre. Cuando el incumplimiento afecte el alcance general o el funcionamiento de la actividad de auditoría interna, debe declararse esta situación a la alta dirección y al consejo o junta directiva u órgano competente, informándoles los obstáculos que se presentaron para generar esta situación.

7.7.1.4.2.2 Normas sobre Desempeño

7.7.1.4.2.2.1 Administración de la Actividad de Auditoría Interna

El auditor interno debe gestionar efectivamente la actividad que desarrolla para asegurar que su trabajo está generando valor agregado a la organización, para lo cual debe ejercer entre otras, las siguientes actividades:

i. Planificación. El Auditor Interno debe establecer, por lo menos anualmente, planes basados en los riesgos que afecten el logro de los objetivos de la organización, a fin de determinar las prioridades de la actividad de auditoría interna, incluyendo entre otros, el derivado de las operaciones y relaciones con otras entidades del mismo grupo económico.

ii. Comunicación y Aprobación. El Auditor Interno debe comunicar los planes y requerimientos de recursos de la actividad de auditoría interna, incluyendo los cambios provisorios significativos al Comité de Auditoría y al representante legal, para la adecuada revisión y aprobación. El Auditor Interno también debe comunicar el impacto de cualquier limitación de recursos.

iii. Administración de Recursos. Determinar los recursos que necesita para el adecuado ejercicio de su labor y solicitarlos a la junta directiva u órgano equivalente.

iv. Políticas y Procedimientos. Establecer políticas y procedimientos para guiar la actividad de auditoria interna.

v. Coordinación. El Auditor Interno debe compartir información y coordinar actividades con los otros órganos de control para lograr una cobertura adecuada y minimizar la duplicación de esfuerzos.

vi. Informes. Los informes emitidos por el Auditor Interno deben ser precisos, objetivos, claros,

constructivos, completos y oportunos. Igualmente, deberán estar debidamente soportados en evidencias suficientes y realizar seguimiento a las acciones tomadas por la administración frente a estas comunicaciones.

7.7.1.4.2.2.2 Naturaleza del Trabajo

La actividad de auditoría interna debe evaluar y contribuir a la mejora de los procesos de gestión de riesgos, control y gobierno de la entidad, utilizando un enfoque sistemático y disciplinado, así:

i. Gestión de Riesgos: El auditor interno debe evaluar la eficacia del sistema de gestión de riesgos de la organización y las exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información de la organización.

ii. Sistema de Control Interno: La actividad de auditoría interna debe asistir a la organización en el mantenimiento de controles efectivos, mediante la evaluación de la eficacia y eficiencia de los mismos y promoviendo la mejora continua, sin perjuicio de la autoevaluación y el autocontrol que corresponden a cada funcionario de la organización, de conformidad con los principios señalados en el subnumeral 7.4 del presente capítulo.

iii. Gobierno Corporativo: La actividad de auditoría interna debe evaluar y hacer las recomendaciones apropiadas para mejorar el proceso de gobierno corporativo, para lo cual debe evaluar el diseño, implantación y eficacia de los objetivos, programas y actividades de la organización.

7.7.1.4.2.2.3. Planificación del trabajo

Los auditores internos deben elaborar y registrar un plan para cada trabajo, que incluya el alcance, los objetivos, el tiempo y la asignación de recursos.

7.7.1.4.2.2.4. Desempeño del Trabajo

Los auditores internos deben identificar, analizar, evaluar y registrar suficiente información, que resulte confiable y relevante, de manera tal que les permita cumplir con los objetivos del trabajo.

Adicionalmente deben establecer requisitos de custodia para los registros del trabajo que sean consistentes con las políticas de la organización en este sentido, y realizar una adecuada supervisión sobre la calidad del trabajo realizado por los integrantes de su equipo.

Los auditores internos deben ser proactivos al analizar, monitorear, indagar, cuestionar, verificar y en general al realizar las actividades propias del aseguramiento, sin limitarse a una simple comprobación de requisitos formales.

7.7.1.4.2.2.5. Comunicación de Resultados

Los auditores internos deben comunicar los resultados de su trabajo, en forma precisa, objetiva, clara, concisa, constructiva, completa y oportuna.

Si una comunicación contiene un error u omisión significativos, debe corregirse y enviarse nuevamente a todas las partes que recibieron la comunicación original.

Por lo menos al cierre de cada ejercicio, el auditor interno o quien haga sus veces deberá

presentar un informe de su gestión y su evaluación sobre la eficacia del sistema de control

interno, incluyendo todos sus elementos. Dicho informe debe contener por lo menos lo siguiente:

i. Titulo.

ii. Identificación de los temas, procesos, áreas o materias objeto del examen, el periodo y criterios de evaluación y la responsabilidad sobre la información utilizada, precisando que la responsabilidad del auditor interno es señalar los hallazgos y recomendaciones sobre los sistemas de control interno y de administración de riesgos.

iii. Especificación respecto a que las siguientes evaluaciones se realizaron de acuerdo con la regulación, las políticas definidas por la junta directiva u órgano equivalente y mejores prácticas de auditoria sobre el particular:

a. Evaluación de la confiabilidad de los sistemas de información contable, financiera y administrativa.

b. Evaluación sobre el funcionamiento y confiabilidad del sistema de control interno.

c. Evaluación de la calidad y adecuación de los sistemas establecidos para garantizar el cumplimiento con las leyes, regulaciones, políticas y procedimientos.

d. Evaluación de la calidad y adecuación de otros sistemas y procedimientos, análisis crítico de la estructura organizacional y evaluación de la adecuación de los métodos y recursos en relación con su distribución.

iv. Los resultados de la evaluación realizada respecto a la existencia, funcionamiento, efectividad, eficacia, confiabilidad y razonabilidad de los sistemas de control interno y de riesgos.

v. Una declaración de la forma en que fueron obtenidas sus evidencias, indicando cuál fue el soporte técnico de sus conclusiones.

vi. Mencionar las limitaciones que encontraron para realizar sus evaluaciones, para tener acceso a información u otros eventos que puedan afectar el resultado de las pruebas realizadas y las conclusiones.

vii. Relación de las recomendaciones formuladas sobre deficiencias materiales detectadas, mencionando los criterios generales que se tuvieron en cuenta para determinar la importancia de las mismas.

viii. Resultados del seguimiento a la implementación de las recomendaciones formuladas en informes anteriores.

ix. Identificación, nombre y firma, ciudad y fecha de elaboración.

Lo anterior sin perjuicio de informes extraordinarios que el auditor interno deba presentar cuando detecte irregularidades graves que ameriten la atención inmediata de los órganos competentes.

7.7.1.4.2.2.6. Supervisión

El auditor interno debe establecer un proceso de seguimiento, para supervisar y verificar que las acciones de la dirección hayan sido efectivamente implantadas o que la alta dirección ha aceptado el riesgo de no tomar ninguna acción.

Cuando el auditor interno considere que la alta dirección ha aceptado un nivel de riesgo residual que en su concepto pueda ser inaceptable para la organización, debe discutir esta cuestión con el representante legal. Si la decisión referida al riesgo residual no se resuelve, el auditor interno y el representante legal deben informar esta situación a la Junta Directiva o quien haga sus veces, para que adopte la decisión pertinente.

7.7.1.4.2.2.7 Funciones

Las principales funciones del auditor interno o de quien tenga a su cargo responsabilidades equivalentes son las siguientes, sin perjuicio de la responsabilidad de autocontrol que corresponde a todos los funcionarios de la organización según los principios señalados en el numeral 7.4 del presente capítulo:

i. Elaborar el plan anual de auditoría antes de finalizar el año anterior y darle estricto cumplimiento. En el caso de entidades subordinadas para las cuales la matriz (sea nacional o extranjera) establezca los lineamientos generales del plan de auditoría, deberá velar porque éstos se ajusten a las disposiciones vigentes en Colombia para la respectiva entidad, así como a las características propias de su entorno, y realizar los ajustes pertinentes de acuerdo al tipo de negocio y a la normatividad aplicable.

ii. Someter a consideración del comité de auditoría el presupuesto anual de funcionamiento del área de auditoría interna.

iii. Realizar una evaluación detallada de la efectividad y adecuación del SCI, en las áreas y procesos de la organización que resulten relevantes, abarcando entre otros aspectos los relacionados con la administración de riesgos de la entidad, los sistemas de información, administrativos, financieros y tecnológicos, incluyendo los sistemas electrónicos de información y los servicios electrónicos.

iv. Evaluar tanto las transacciones como los procedimientos de control involucrados en los diferentes procesos o actividades de la entidad, en aquellos aspectos que considere relevantes.

v. Revisar los procedimientos adoptados por la administración para garantizar el cumplimiento con los requerimientos legales y regulatorios, códigos internos y la implementación de políticas y procedimientos.

vi. Verificar en sus auditorias la eficacia de los procedimientos adoptados por la administración para asegurar la confiabilidad y oportunidad de los reportes a esta Superintendencia y otros entes de control.

vii. Contribuir a la mejora de los procesos de gestión de riesgos, control y gobierno de la entidad, utilizando un enfoque sistemático y disciplinado.

viii. Adelantar las investigaciones especiales que considere pertinentes, dentro del ámbito de su competencia, para lo cual deberá contar con la colaboración de expertos en aquellos temas en que se requiera.

ix. Presentar comunicaciones e informes periódicos al comité de auditoría o a la junta directiva o a la administración cuando lo estime conveniente, sobre el resultado del ejercicio de sus funciones.

x. Hacer seguimiento a los controles establecidos por la entidad, mediante la revisión de la información contable y financiera.

xi. Evaluar los problemas encontrados y solicitar las acciones de mejoramiento correspondientes.

xii. Presentar a la Junta Directiva, por lo menos al cierre de cada ejercicio, un informe acerca de los resultados de su labor, incluyendo, entre otros aspectos, las deficiencias detectadas en el SCI.

Es de advertir que si bien resulta viable que la administración de las entidades supervisadas contrate externamente la realización de las actividades propias de la auditoría, en ningún caso ello implica el traslado de la responsabilidad sobre la auditoria misma. Es decir, que la administración de la entidad sólo entrega la ejecución de la labor más no la responsabilidad misma de la realización de la auditoria, la cual conservará siempre.

En tal sentido, la administración de la entidad debe realizar el direccionamiento, administración y seguimiento de la actividad realizada por el tercero, sin delegar la toma de decisiones tales como los riesgos en los cuales se debe concentrar primordialmente la auditoria o la adopción del plan de auditoria. Adicionalmente debe garantizarse el acceso permanente de la administración y del supervisor a la información de la auditoria y a los papeles de trabajo, el establecimiento de un plan de contingencias para que no cese la labor en caso de algún problema en la ejecución del contrato y la independencia entre el auditor interno y externo (si existe este último), teniendo en cuenta que las dos funciones mencionadas no pueden ser desarrolladas por la misma firma.

7.7.2 Órganos Externos

7.7.2.1 Revisor Fiscal

De conformidad con lo previsto en el numeral 4.4.2.2 de la Circular Externa 054 de 2008, incorporada en el Título I, Capítulo III, numeral 4 de la presente circular, el revisor fiscal de la entidad debe valorar los sistemas de control interno y administración de riesgos implementados por las entidades a fin de emitir la opinión a la que se refiere y en los términos consignados en el numeral 4.2.8 ibídem.

7.7.2.2 Contralor Normativo

7.7.2.2.1 Entidades a las cuales se exige contar con contralor normativo y requisitos que debe cumplir el mismo

Deben contar con la figura del contralor normativo las sociedades comisionistas de bolsa, según lo dispuesto en el artículo 21 de la Ley 964 de 2005, y las sociedades administradoras de carteras colectivas, de conformidad con el Decreto 2175 de 2007 y demás normas que lo modifiquen.

Teniendo en cuenta que el citado artículo 21 indica que el contralor normativo será independiente y que el artículo 44 de la misma ley define los criterios de independencia aplicables para todos los efectos previstos en la misma, el contralor normativo en ningún caso debe tener los vínculos que se señalan a continuación:

i. Empleado o directivo de la sociedad comisionista, de la administradora de la cartera o de alguna de sus filiales, subsidiarias o controlantes y filiales de las contratantes, incluyendo aquellas personas que hubieren tenido tal calidad durante el año inmediatamente anterior a la designación.

ii. Accionistas que directamente o en virtud de convenio dirijan, orienten o controlen la mayoría de los derechos de voto de la sociedad comisionista o de la administradora de la cartera o que determinen la composición mayoritaria de los órganos de administración, de dirección o de control de las mismas.

iii. Socio o empleado de asociaciones o sociedades que presten servicios de asesoría o consultoría a la sociedad comisionista o a la administradora de la cartera o a las empresas que pertenezcan al mismo grupo económico del cual formen parte éstas, cuando los ingresos por dicho concepto representen para aquellos, el veinte por ciento (20%) o más de sus ingresos operacionales.

iv. Empleado o directivo de una fundación, asociación o sociedad que reciba donativos importantes de la sociedad comisionista o de la administradora de la cartera. Se consideran donativos importantes aquellos que representen más del veinte por ciento (20%) del total de donativos recibidos por la respectiva institución.

v. Administrador de una entidad en cuya junta directiva participe un representante legal de la sociedad comisionista o de la administradora de la cartera.

vi. Persona que reciba de la sociedad comisionista o de la administradora de la cartera alguna remuneración diferente a los honorarios como miembro de la junta directiva, del comité de auditoría o de cualquier otro comité creado por la junta directiva.

La vinculación del contralor normativo se efectuará a través de un contrato de prestación de servicios u otra modalidad que en ningún caso implique subordinación.

7.7.2.2.2 funciones y responsabilidades respecto de las Sociedades Comisionistas de Bolsa

El contralor normativo asistirá a las reuniones de la junta directiva de la sociedad con voz pero sin voto, y tendrá a su cargo, entre otras, las siguientes funciones:

i. En desarrollo de la función consagrada en el literal a) del artículo 21 de la Ley 964 de 2005, el contralor normativo debe establecer, implementar y verificar el cumplimiento de las políticas y mecanismos adecuados para:

· La detección, prevención y manejo de conflictos de interés en la realización de operaciones de intermediación que les han sido autorizadas, en particular, de los mecanismos para garantizar que las áreas, funciones y sistemas de toma de decisiones correspondientes a cada actividad, estén separadas decisoria, física y operativamente.

· La separación de los activos administrados o recibidos de sus clientes de los propios y de los que correspondan a otros clientes.

· La adecuada clasificación de clientes y la debida prestación del deber de asesoría a los clientes inversionistas.

· El cumplimiento de las disposiciones del libro de órdenes para garantizar la debida destinación de los recursos entregados por los clientes.

· La mejor ejecución de las operaciones autorizadas, incluyendo entre otras las realizadas con o por cuenta de administradores, miembros de junta, matriz, subordinadas y demás personas o entidades pertenecientes al mismo grupo económico.

· La publicación de tarifas relacionadas con los servicios que presta la sociedad comisionista y la de garantizar que se informe a los clientes sobre dichas tarifas de manera previa a la realización de operaciones que le han sido autorizadas.

· La verificación respecto a que al interior de la sociedad solo operen las personas inscritas en el Registro Nacional de Profesionales del Mercado de Valores, cuando dicha inscripción sea condición para actuar.

ii. En desarrollo de la función prevista en el literal b) del artículo 21 de la Ley 964 de 2005, el contralor normativo propondrá a la junta directiva en las reuniones de dicho órgano social el establecimiento de las medidas para procurar comportamientos éticos y transparencia en las actividades de sus funcionarios y terceros relacionados en el ejercicio de los negocios propios de la comisionista de bolsa; detectar y prevenir conflictos de interés; garantizar la exactitud y transparencia en la revelación de información financiera y evitar el uso indebido de información no pública

iii. Documentar y comunicar a la junta directiva en las reuniones que adelante dicho órgano social y al representante legal, las situaciones de incumplimiento de la normatividad, políticas o procedimientos internos de la entidad que puedan afectar el sano desarrollo de la actividad de intermediación de valores, su patrimonio, buen nombre o a sus clientes.

iv. Las demás que se establezcan en los estatutos sociales.

Estos procedimientos de verificación deben estar debidamente documentados y estar a disposición de la SFC.

El contralor normativo debe Informar de manera inmediata a la asamblea de accionistas, a la junta directiva u órgano equivalente, al Autorregulador del Mercado de Valores y a la SFC de cualquier irregularidad que advierta en relación con el desarrollo del objeto social de la comisionista o cualquier aspecto dentro del ámbito de su competencia.

7.7.2.2.3 Respecto de las Sociedades Administradoras de Carteras

El artículo 58 del Decreto 2175 de 2007 asigna a los contralores normativos, en relación con las sociedades administradoras de carteras colectivas, entre otras, la función de establecer los mecanismos y procedimientos necesarios para que se cumpla con lo dispuesto en:

i. El reglamento de las carteras colectivas.

ii. El régimen de inversiones y las políticas definidas por la junta directiva en materia de inversiones.

iii. La correcta valoración de la cartera.

iv. Las actualizaciones de los manuales y procedimientos internos, de conformidad con la normatividad aplicable.

v. El cumplimiento de normas relacionadas con operaciones prohibidas en el manejo de las carteras.

vi. Las disposiciones legales, reglamentos aplicables y manuales internos en aquellos aspectos que tengan relación con la actividad de la cartera colectiva.

Adicionalmente, el contralor normativo debe diseñar mecanismos y procedimientos que permitan hacer seguimiento y supervisión a la toma de decisiones por parte del gerente de la cartera colectiva y del comité de inversiones.

Estos procedimientos de verificación deben estar debidamente documentados y a disposición de la SFC.

El contralor normativo deberá presentar, por lo menos anualmente, un informe sobre los resultados de su gestión que incluya como mínimo: hallazgos, acciones implementadas, planes de mejoramiento y seguimiento, cronograma de ajuste y reportes de cumplimiento. Lo anterior sin perjuicio de que informe a la junta directiva u órgano equivalente y a la SFC de manera inmediata la ocurrencia de cualquier evento que impida la normal y correcta ejecución de sus funciones, así como las irregularidades que puedan afectar el sano desarrollo de la cartera colectiva.

7.8. PRODUCTOS QUE DEBEN PRESENTARSE A LA SFC

Respecto a la implementación del sistema de control interno, la SFC podrá exigir a través de la supervisión in situ o extra situ, uno o más de los documentos específicos que se relacionan a continuación, sin prejuicio de cualquier otra información que estime pertinente en ejercicio de sus atribuciones legales:

i. Planes y programas definidos por la entidad para el logro de sus objetivos, incluyendo las correspondientes acciones, responsables y cronogramas.

ii. Código de Conducta y documento emitido por el representante legal de la entidad en el cual se adopte oficialmente.

iii. Metodología y herramienta definidas para la autoevaluación, el autocontrol y la autorregulación.

iv. Mapas de procesos.

v. Mapa de riesgos, que contenga como mínimo: identificación de factores internos y externos de riesgo para la organización, riesgos identificados por procesos, análisis de probabilidad de ocurrencia de los riesgos y su impacto, identificación de los controles existentes para prevenir la ocurrencia o mitigar el impacto de los riesgos identificados, evaluación de la efectividad de los controles y definición de las acciones de mejoramiento necesarias.

vi. Documentos que soporten la socialización de los principios y valores a todos los funcionarios de la entidad.

vii. Documento que soporte la comunicación a todos los funcionarios de la entidad del mapa de riesgos y de las políticas y metodologías a que se refiere el numeral anterior.

viii. Políticas y metodología para evaluación del desempeño, a todos los niveles de la organización, incluyendo los indicadores definidos para medir la eficiencia, eficacia y efectividad.

ix. Políticas establecidas en materia de manejo de información y comunicación, que incluyan mecanismos específicos para garantizar la conservación y custodia de información reservada o confidencial y evitar su filtración

x. Política para manejo de riesgos definida por la junta directiva u órgano equivalente y la metodología e instrumentos para la gestión de riesgos en la entidad, incluyendo la definición de los comités u órganos responsables.

xi. Estructura organizacional, Manual de funciones, competencias y requisitos a nivel de cargo.

xii. Plan anual de auditoría interna.

xiii. Reportes efectuados por los distintos órganos competentes en materia de control.

xiv. Informes sobre resultados obtenidos en el proceso de seguimiento y evaluación al cumplimiento de los planes y programas, que incluya la medición de la satisfacción de los clientes, usuarios y otras partes interesadas.

xv. En relación con el consumidor financiero (según la definición establecida en el artículo 80 del Decreto 4327 de 2005), lo siguiente:

a. Políticas de servicio.

b. Políticas de transparencia e integridad en las relaciones con los mismos (información acerca de productos y tarifas, mecanismos y sistemas de atención).

c. Estrategias de servicio al cliente.

d. Mecanismos establecidos para la recepción, registro y atención de quejas, sugerencias o recomendaciones por parte de los clientes, usuarios u otros grupos de interés y acciones de mejora adelantadas con ocasión del análisis de las mismas (análisis punta a punta para los principales motivos, por productos; revisión de productos, implementación de nuevos canales, revisión de políticas parametrizadas en el sistema, etc.).

xvi. Actas y/o papeles de trabajo en que consten las decisiones y actuaciones de los órganos de control.

xvii. Programas o planes de mejoramiento.

* * *

1. Para mayor orientación sobre este tema se puede acudir a la guía de COSO Integrado (Committe Sponsoring Organization of the Treadway Commission Committee of Sponsoring Organizations of the Treadway Commission and Enterprise Risk Management – Integrated Framework).

2. Se entiende por aseguramiento el examen objetivo de evidencias con el propósito de proveer una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una organización. Por ejemplo trabajos financieros, de desempeño, de cumplimiento y de seguridad de sistemas. (Texto tomado del documento “Normas Internacionales para el ejercicio profesional de la Auditoría Interna” – Instituto de Auditores Internos de Colombia).

3. Se denomina Consultoría, a las actividades de asesoramiento y servicios relacionados, proporcionadas a los clientes, cuya naturaleza y alcance estén relacionados con los mismos y estén dirigidos a añadir valor y a mejorar los procesos de gobierno, gestión de riesgos y control, de una organización sin que el auditor interno asuma responsabilidades de gestión.

4. El Instituto de Auditores Internos “IIA”, a través del “Consejo de Normas de Auditoría Interna ” (IASB, por sus siglas en inglés), es la entidad ampliamente reconocida y autorizada técnicamente para emitir las normas para el ejercicio de la Auditoría Interna.

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Normograma de la Administradora Colombiana de Pensiones - Colpensiones
ISSN 2256-1633
Última actualización: 31 de diciembre de 2017