SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO I
ASPECTOS GENERALES

CAPÍTULO IV: SISTEMA DE CONTROL INTERNO

CONTENIDO

1. ÁMBITO DE APLICACIÓN

2. DEFINICIÓN
2.1. Autocontrol
2.2. Autorregulación
2.3. Autogestión

3. COMPONENTES DEL SISTEMA DE CONTROL INTERNO
3.1. Ambiente de control
3.2. Gestión de riesgos
3.3. Actividades de control
3.4. Información y comunicación
3.5. Actividades de seguimiento y monitoreo

4. RESPONSABILIDADES EN EL SISTEMA DE CONTROL INTERNO
4.1. Junta Directiva u órgano que haga sus veces
4.2. Comité de Auditoría
4.3. Comité de Riesgos
4.4. Alta Gerencia
4.5. Auditoría Interna u órgano que haga sus veces

5. MODELO DE LAS TRES LÍNEAS
5.1. Asignación de funciones
5.2. Líneas de rendición de cuentas

1. ÁMBITO DE APLICACIÓN

Las entidades vigiladas (EV) por la Superintendencia Financiera de Colombia (SFC), ya sean matrices o subordinadas, deben implementar y mantener un Sistema de Control Interno (SCI) acorde con el perfil de riesgo, el plan de negocio, la naturaleza, el tamaño y la complejidad de las actividades que desarrollen, así como con el entorno económico y los mercados en los que operan.

Las EV que tengan la calidad de matrices deben procurar que sus subordinadas tengan un SCI que cumpla las instrucciones previstas en el presente Capítulo, para lo cual deben impartir lineamientos generales, atendiendo la naturaleza, tamaño, riesgos y complejidad de las actividades que cada una de ellas realiza.

Las EV que pertenezcan al sector público deberán adoptar el enfoque establecido en el Modelo Estándar de Control Interno (MECI), sin perjuicio del cumplimiento de las instrucciones del presente Capítulo que les resulten aplicables.

2. DEFINICIÓN

El SCI es el conjunto de políticas, principios, normas, procedimientos, y mecanismos de verificación y evaluación que deben implementar las EV, donde intervienen y participan los órganos de gobierno y control, así como todos sus funcionarios, con el fin de proporcionar un grado de seguridad razonable en el cumplimiento de sus objetivos estratégicos en aras de lograr, como mínimo, lo siguiente:

a. Mejorar la eficiencia en el desarrollo de sus actividades.
b. Prevenir y mitigar la ocurrencia de fraudes internos y externos.
c. Realizar una gestión adecuada de los riesgos.
d. Aumentar la confiabilidad y oportunidad en la información generada.
e. Cumplir la normatividad aplicable.
f. Proteger los activos de la organización.
g. Prevenir y mitigar la ocurrencia de actos de corrupción.

Para el logro de los anteriores propósitos, las EV deben basarse en los principios de autocontrol, autorregulación y autogestión, de acuerdo con las siguientes definiciones:

2.1. Autocontrol

Los funcionarios de las EV deben evaluar y controlar su trabajo, detectar desviaciones y adoptar correctivos en el ejercicio y cumplimiento de sus funciones.

2.2. Autorregulación

Las EV deben desarrollar métodos, normas y procedimientos internos que permitan la implementación y mejoramiento del SCI.

2.3. Autogestión

Las EV deben tener capacidad para coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz el funcionamiento del SCI.

3. COMPONENTES DEL SISTEMA DE CONTROL INTERNO

Las EV deben tener en cuenta el modelo de las tres líneas propuesto por el Instituto de Auditores Internos (IIA, por sus siglas en inglés) en la implementación del SCI, por lo menos, en la asignación de funciones. En todo caso, deben considerar, como mínimo, los elementos que se señalan a continuación:

3.1. Ambiente de control

Es el conjunto de políticas, normas internas, objetivos, procedimientos, y estructuras jerárquicas y de gobierno al que se encuentra sujeto todo el personal de las EV en el desempeño de las funciones relacionadas con el SCI.

El ambiente de control debe estar compuesto, como mínimo, por los siguientes elementos:

3.1.1. Código de ética y conducta

Las EV deben tener un código de ética y conducta que incluya, como mínimo, reglas sobre: i) la gestión de conflictos de interés en los que puedan incurrir los funcionarios y administradores de la EV; ii) el uso, acceso y custodia de la información reservada; iii) el otorgamiento de incentivos por parte de la EV a los funcionarios, a los administradores y a terceros; iv) el seguimiento al cumplimiento del código; v) el procedimiento para el reporte de los incumplimientos del código por parte de los funcionarios y administradores de la entidad, incluyendo líneas y canales adoptados; vi) la divulgación del código; vii) normas de conducta; y viii) el procedimiento sancionatorio frente a su inobservancia y las consecuencias de su incumplimiento.

3.1.2. Política de generación y remisión de informes sobre el SCI

Son los lineamientos que establecen la periodicidad y contenido de los informes dirigidos a la Junta Directiva (JD) o el órgano que haga sus veces, en los cuales se analiza la efectividad del SCI, de acuerdo con los indicadores de gestión definidos por las EV.

3.1.3. Política de recurso humano

Son los lineamientos para la selección, formación y conservación del personal competente para cumplir los objetivos estratégicos de las EV y la mitigación de los riesgos asociados a la rotación de personal. Dichos lineamientos deben contener, como mínimo: i) el esquema de remuneración y evaluación del recurso humano, ii) el programa de capacitación, iii) los planes de sucesión, y iv) el procedimiento para la elaboración y aprobación de los manuales de funciones o equivalentes.

3.1.4. Políticas de gestión de riesgos

Son los lineamientos para la gestión integral de los riesgos asociados a las actividades que desarrollan las EV de conformidad con las instrucciones en materia de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT) establecidas en el Capítulo IV del Título IV de la Parte I de la Circular Básica Jurídica (CBJ), y/o las instrucciones sobre el Marco de Gestión de Riesgos de los Conglomerados Financieros (MGR) - Capítulo XXX, Sistema Integral de Administración de Riesgos (SIAR) - Capítulo XXXI y/o el Sistema Integral de Administración de Riesgo de las Entidades Exceptuadas del SIAR (SARE) - Capítulo XXXII, contenidas en la Circular Básica Contable y Financiera (CBCF) y las disposiciones que las modifiquen o adicionen.

3.1.5. Política financiera y contable

Son los lineamientos para la preparación de la información financiera y demás informes que reflejan la situación financiera y los resultados de las EV, atendiendo las disposiciones aplicables.

3.1.6. Política de evaluaciones y autoevaluaciones

Son los lineamientos aplicables a las evaluaciones internas y externas, así como a las autoevaluaciones que deben realizar las EV para identificar las deficiencias del SCI y comunicarlas de manera oportuna a los responsables de aplicar las medidas correctivas. Los lineamientos que definan las EV deben garantizar que la periodicidad de las evaluaciones y autoevaluaciones tengan en cuenta la dinámica propia de las actividades que estas desarrollan, incluyendo aquellas tercerizadas.

3.1.7. Política de inducción y capacitación de miembros de JD u órgano que haga sus veces y de sus comités de apoyo

Son los lineamientos que definen el proceso de inducción, capacitación y su periodicidad para los nuevos miembros de JD u órgano que haga sus veces y de sus comités de apoyo con el fin de asegurar que conozcan la estructura, objetivos estratégicos, modelo funcional de las EV, marco de apetito de riesgo, el funcionamiento de dicho órgano y la normatividad que le resulte aplicable a sus miembros. Esta política comprende además los lineamientos de capacitación a los integrantes de la JD u órgano que haga sus veces y de sus comités de apoyo, cuando los miembros de tales órganos lo soliciten para adoptar decisiones sobre asuntos con un alto componente técnico.

3.1.8. Política de seguridad de la información

Son los lineamientos que definen los controles que deben implementar las EV para asegurar y proteger la información, los cuales incluyen, entre otros mecanismos, los siguientes:

a. Celebrar acuerdos de confidencialidad.
b. Permitir el acceso a sistemas, programas y datos exclusivamente a usuarios autorizados en virtud de sus funciones, entre otros, a través de:
    i. Controles de acceso físico y lógico que comprendan autorización, autenticación y control de acceso.
    ii. Protocolo de manejo de incidentes.
    iii. Herramientas para la prevención y detección de código malicioso, virus, entre otros.
    iv. Capacitaciones de personal y usuarios, en caso de ser procedente.
    v. Administración centralizada de la seguridad.
c. Los demás que defina la EV.

3.1.9. Miembros independientes de la Junta Directiva u órgano que haga sus veces

Son aquellos miembros de JD u órgano que haga sus veces, que en ningún caso sean:

a. Empleados o integrantes de la Alta Gerencia (AG) de la EV 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.
b. Accionistas que directamente o en virtud de convenio dirijan, orienten o controlen la mayoría de los derechos de voto de la EV o que determinen la composición mayoritaria de los órganos de administración, de dirección o de control de la misma.
c. Socios o empleados de asociaciones o sociedades que presten servicios de asesoría o consultoría a la EV 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 20% o más de sus ingresos operacionales.
d. Empleado o directivo de una fundación, asociación o sociedad que reciba donativos importantes de la EV. Se consideran donativos importantes aquellos que representen más del 20% del total de donativos recibidos por la respectiva institución.
e. Administrador de una entidad en cuya JD u órgano que haga sus veces participe un representante legal de la EV.
f. Persona que reciba de la EV alguna remuneración diferente a los honorarios como miembro de la JD u órgano que haga sus veces, del comité de auditoría o de cualquier otro comité creado por la JD u órgano que haga sus veces.

Las EV podrán establecer criterios adicionales a los definidos en el presente subnumeral.

3.1.10. Comité de Auditoría

Las EV deben contar con un Comité de Auditoría integrado por lo menos con 3 miembros de la JD u órgano que haga sus veces. Dichos miembros deben ser en su mayoría independientes para aquellas EV que por disposición legal o estatutaria deben contar con tales miembros en el referido órgano social. Este Comité debe ser presidido por un miembro independiente.

Los miembros del Comité de Auditoría deben contar con experiencia y conocimientos en los temas relacionados con las funciones asignadas a dicho Comité.

El Comité de Auditoría debe reunirse por lo menos una vez cada 3 meses o, con una frecuencia mayor, si así lo establece su reglamento de funcionamiento. En todo caso, el Comité puede ser convocado a reuniones extraordinarias cada vez que se requiera.

3.1.11. Comité de Riesgos

Para las EV que están obligadas a contar con un Comité de Riesgos, su estructura y funcionamiento debe corresponder con lo previsto en el SIAR y el MGR de la CBCF y las instrucciones que lo modifiquen o adicionen. En todo caso, la JD u órgano que haga sus veces, le podrá asignar funciones adicionales, siempre que estas contribuyan al desarrollo y adecuado funcionamiento del SCI.

3.1.12. Estatuto de auditoría

Es el documento que define las funciones de la auditoría interna u órgano que haga sus veces, y establece como mínimo:

a. Su posición dentro del organigrama de las EV.
b. Los mecanismos de acceso a la información y bienes de las EV que resulten necesarios para la ejecución de sus funciones.
c. Los criterios que deben cumplirse para mantener la independencia.
d. El alcance y condiciones de las funciones de aseguramiento y consultoría.

3.1.13. Plan anual de auditoría interna

Es el plan anual definido por las EV en el cual se detallan las actividades a ser desarrolladas por la auditoría interna u órgano que haga sus veces, su alcance, los plazos para su cumplimiento y los recursos necesarios para su desarrollo.

Dicho plan debe cumplirse integralmente, sin perjuicio de las modificaciones que se realicen, las cuales deben sustentarse y aprobarse siguiendo el mismo proceso que se surtió para su aprobación inicial.

Para el caso de las EV que sean subordinadas, su plan de auditoría debe estar alineado con el de su matriz (nacional o extranjera) y cumplir con lo previsto en el presente Capítulo y demás disposiciones vigentes en Colombia que sean aplicables.

En todo caso, la auditoría interna de la EV subordinada u órgano que haga sus veces, deberá verificar que su plan de auditoría interna se ajuste a su tamaño, plan estratégico, complejidad de sus actividades, y los riesgos a los que está expuesta en desarrollo de estas.

3.1.14. Política de aseguramiento y mejora de la calidad de la auditoría interna

Son los lineamientos que debe seguir el auditor interno o el funcionario que haga sus veces, para evaluar la calidad del área de auditoría interna u órgano que haga sus veces.

3.1.15. Presupuesto anual

Son los recursos asignados y aprobados para la ejecución de las actividades que las EV llevarán a cabo en el año correspondiente.

3.1.16. Plan estratégico

Son los objetivos estratégicos para el corto, mediano y largo plazo definidos por las EV, teniendo en cuenta los riesgos, la prioridad e impacto de cada objetivo.

3.1.17. Plan estratégico de tecnología

Son los desarrollos tecnológicos para el corto, mediano y largo plazo definidos por las EV, teniendo en cuenta los riesgos, la prioridad e impacto de cada objetivo.

Este plan debe contemplar, al menos, los siguientes aspectos:

a. Evaluación del estado actual de la infraestructura tecnológica de la EV.
b. Cronograma de actividades y objetivos que se ejecutarán en el corto, mediano y largo plazo en materia de desarrollos tecnológicos.
c. Capacitaciones de personal y usuarios para la implementación de los desarrollos, en caso de ser aplicable.
d. Mecanismos para la mitigación del riesgo operacional y de ciberseguridad asociados a la implementación y al funcionamiento de los desarrollos tecnológicos.
e. Justificación técnica y financiera de los desarrollos a implementar, indicando su prioridad e impacto en las actividades de la entidad.

3.2. Gestión de riesgos

Es un proceso dinámico y permanente que deben realizar las EV para gestionar los riesgos asociados a sus actividades, de acuerdo con las instrucciones en materia de Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT) previstas en el Capítulo IV, Título IV, Parte I de la CBJ, y/o las instrucciones en materia de administración de riesgos establecidas en el Marco de Gestión de Riesgos (MGR) - Capítulo XXX CBCF, en el Sistema Integral de Administración de Riesgos (SIAR) - Capítulo XXXI CBCF y/o en el Sistema Integral de Administración de Riesgos de las Entidades Exceptuadas del SIAR (SARE) - Capítulo XXXII CBCF, o las instrucciones que las modifiquen o sustituyan.

3.3. Actividades de control

Son las acciones que contribuyen a garantizar la correcta aplicación del SCI de las EV. Estas acciones se deben realizar en todos los niveles de las EV, en las diferentes etapas de los procesos de negocio, así como en el entorno tecnológico, y deben estar alineadas con la gestión de riesgos. La selección y desarrollo de las actividades de control deben determinarse considerando la relación beneficio/costo y su potencial efectividad.

Las actividades de control deben contemplar, al menos, las siguientes acciones y mecanismos:

3.3.1. Controles de alto nivel

Es el seguimiento por parte de la JD u órgano que haga sus veces, comités de apoyo y AG del funcionamiento del SCI y del progreso de las EV en el logro de sus objetivos estratégicos y definición de la cultura organizacional. Estos controles tienen como propósito detectar posibles falencias, tales como deficiencias de control, errores en la información financiera, o actividades fraudulentas, y permiten adoptar los correctivos necesarios.

3.3.2. Controles generales

Son las actividades que deben desarrollar las diferentes áreas de las EV para asegurar la continuidad y correcto funcionamiento de todos sus procesos.

3.3.3. Controles de aplicación

Son los mecanismos que contribuyen a garantizar la correcta implementación de procesos tecnológicos y operativos, los cuales deben estar definidos en manuales de procedimiento, indicando los pasos para su aplicación y los responsables de su ejecución.

3.3.4. Controles sobre la tecnología

Son mecanismos para: i) asegurar el cumplimiento de la política de seguridad de la información, ii) mitigar los riesgos asociados a la adquisición, funcionamiento, desarrollo y mantenimiento de la infraestructura tecnológica, y iii) identificar cambios o actualización de la tecnología.

3.3.5. Controles sobre la gestión contable y financiera

Son las actividades para asegurar el cumplimiento de la política contable y financiera de las EV y de la normativa aplicable en esta materia.

3.4. Información y comunicación

Es el proceso para el intercambio de información entre las EV y los diferentes grupos de interés, internos y externos.

El componente de información y comunicación debe contemplar, al menos, lo siguiente:

3.4.1. Política de información y comunicación

La política de información y comunicación debe establecer, como mínimo, lo siguiente:

3.4.1.1. Características de la información

La información transmitida a los grupos de interés debe ser accesible, exacta, actualizada y protegida.

3.4.1.2. Sistemas de información

Los sistemas de información de las EV deben tener la capacidad de obtener, capturar y procesar datos procedentes de fuentes internas y externas seguras, y transformarlos en información que tenga valor para las EV. Los sistemas deben ajustarse de acuerdo con las necesidades de las EV y los volúmenes de datos que deban ser procesados.

3.4.1.3. Criterios de selección de información

Las EV deben establecer criterios para definir el tipo de información que debe ser comunicados a los diferentes grupos de interés internos y externos, en atención a su importancia y criticidad.

3.4.1.4. Canales de comunicación

Las EV deben contar con canales de comunicación específicos y exclusivos para la recepción de quejas y denuncias contra los funcionarios y administradores de las EV, o contra terceros contratados por las EV, tales como: líneas telefónicas, correos electrónicos, buzones especiales en el sitio web y otros mecanismos digitales, con el fin de que las personas que adviertan o conozcan eventuales irregularidades, incumplimientos normativos, violaciones al código de ética y conducta, u otros hechos o circunstancias que afecten o puedan afectar el adecuado funcionamiento del SCI, los pongan en conocimiento de los órganos competentes de las EV.

Los canales de comunicación dispuestos para la recepción de quejas y denuncias deben contar con salvaguardas que garanticen el anonimato de los denunciantes y la confidencialidad de la información. Las EV deben diferenciar claramente estos canales de recepción de quejas y denuncias, de los canales de formulación de quejas de los consumidores financieros derivadas de las fallas en la prestación de servicios o productos.

Para la recepción y tratamiento de las quejas y denuncias se debe garantizar lo siguiente:

a. Protección a denunciantes frente a represalias.
b. Capacitación a los funcionarios de las EV en esta materia.
c. Instancias dentro de las EV que asumirán el trámite de las quejas y denuncias.
d. Procesos eficientes que permitan su trámite de manera oportuna.

3.4.1.5. Grupos de interés externos

Las EV deben definir reglas para garantizar igualdad en el acceso a la información a los grupos de interés externos, estableciendo los canales y la oportunidad para su acceso.

3.5. Actividades de seguimiento y monitoreo

Son las evaluaciones internas y externas o, una combinación de ambas, que deben adelantar las EV para determinar si los componentes del SCI están presentes y funcionan adecuadamente.

3.5.1. Evaluaciones y autoevaluaciones internas

Las EV deben realizar periódicamente evaluaciones y autoevaluaciones de los procesos internos con el propósito de verificar el funcionamiento de los diferentes componentes del SCI y ejecutar las acciones correctivas o preventivas en caso de ser necesario.

3.5.2. Evaluaciones externas

Las EV pueden contratar evaluaciones externas con el propósito de verificar el funcionamiento de los diferentes componentes del SCI, para lo cual deben definir su alcance y frecuencia.

4. RESPONSABILIDADES EN EL SISTEMA DE CONTROL INTERNO

Sin perjuicio de las funciones y responsabilidades asignadas en otras disposiciones, los órganos de las EV deben cumplir, como mínimo, con las siguientes funciones:

4.1. Funciones de la Junta Directiva u órgano que haga sus veces

La JD u órgano que haga sus veces, debe cumplir como mínimo con las funciones y responsabilidades previstas en los siguientes subnumerales:

4.1.1. Funciones de la Junta Directiva u órgano que haga sus veces respecto del ambiente de control

La JD u órgano que haga sus veces debe aprobar los siguientes documentos y políticas:

a. Código de ética y conducta.
b. Política de generación y remisión de informes sobre el SCI.
c. Política de recurso humano.
d. Política financiera y contable.
e. Política de evaluaciones y autoevaluaciones.
f. Política de inducción y capacitación de miembros de JD u órgano que haga sus veces y de sus comités de apoyo.
g. Reglamentos internos de los comités de apoyo.
h. Política de seguridad de la información.
i. Estatuto de auditoría interna.
j. Presupuesto anual.
k. Plan estratégico.
l. Plan estratégico de tecnología.
m. Política de información y comunicación.

Asimismo, debe designar al auditor interno de la EV o el funcionario que haga sus veces. Lo anterior, sin perjuicio de las disposiciones aplicables a la designación del auditor interno para las entidades de naturaleza pública.

4.1.2. Funciones de la Junta Directiva u órgano que haga sus veces respecto de la gestión de riesgos

Le corresponde a la JD u órgano que haga sus veces, cumplir con las siguientes funciones:

4.1.2.1. Hacer seguimiento a las acciones ejecutadas por la AG para mitigar los riesgos asociados a las actividades previstas en la planeación estratégica.

4.1.2.2. Hacer seguimiento al funcionamiento del SCI para mitigar los riesgos asociados al logro de los objetivos estratégicos de la EV.

4.1.3. Funciones de la Junta Directiva u órgano que haga sus veces respecto de las actividades de control

Le corresponde a la JD u órgano que haga sus veces, cumplir con las siguientes funciones:

4.1.3.1. Hacer seguimiento al desempeño financiero y operacional de las EV.

4.1.3.2. Revisar los estados financieros junto con sus notas antes de que sean presentados a la Asamblea General de Accionistas o máximo órgano social, teniendo en cuenta los informes y recomendaciones que le presente el Comité de Auditoría.

4.1.3.3. Asegurar que la AG establezca procesos que permitan la identificación y evaluación de los cambios que puedan tener un impacto significativo en el SCI.

4.1.3.4. Reunirse con el Revisor Fiscal y el auditor interno o el funcionario que haga sus veces. Así mismo, podrá reunirse sin la presencia de la AG, cuando lo considere necesario.

4.1.4. Funciones de la Junta Directiva u órgano que haga sus veces respecto de la información y comunicación

Le corresponde a la JD u órgano que haga sus veces cumplir con las siguientes funciones:

4.1.4.1. Solicitar toda la información que estime necesaria sobre el desarrollo y desempeño de los controles internos para cumplir con sus responsabilidades.

4.1.4.2. Presentar en la Asamblea General Ordinaria de Accionistas o en la reunión ordinaria del órgano equivalente, un informe respecto del funcionamiento y evaluación del SCI durante el período inmediatamente anterior.

4.1.5. Funciones de la Junta Directiva u órgano que haga sus veces respecto de las actividades de seguimiento y monitoreo

Le corresponde a la JD u órgano que haga sus veces, cumplir con las siguientes funciones:

4.1.5.1. Autoevaluar su gestión al menos una vez al año.

4.1.5.2. Evaluar la gestión de la AG al menos una vez al año.

4.1.5.3. Definir acciones para solucionar los hallazgos producto de las autoevaluaciones y evaluaciones internas y externas.

4.1.5.4. Realizar seguimiento cada 6 meses a la gestión de riesgos y a las medidas adoptadas para su control o mitigación, o con una frecuencia mayor, si resulta procedente.

Se considera buena práctica de gobierno corporativo, la contratación de un tercero especializado para evaluar la gestión de la JD u órgano que haga sus veces.

4.2. Comité de Auditoría

El Comité de Auditoría debe cumplir como mínimo con las funciones y responsabilidades previstas en el presente subnumeral:

4.2.1. Funciones del Comité de Auditoría respecto del ambiente de control

Le corresponde al Comité de Auditoría cumplir con las siguientes funciones:

4.2.1.1. Aprobar los siguientes documentos y políticas:

a. Estructura, procedimientos y metodologías del SCI con líneas de responsabilidad y de rendición de cuentas.
b. Plan anual de auditoría interna.
c. Política de aseguramiento y mejora de la calidad de la auditoría interna.

4.2.1.2. Revisar y recomendar para aprobación de la JD u órgano que haga sus veces, los siguientes documentos y políticas:

a. Código de ética y conducta.
b. Política de generación y remisión de informes sobre el SCI.
c. Política de seguridad de la información.
d. Estatuto de auditoría interna.
e. Plan estratégico de tecnología.

4.2.2. Funciones del Comité de Auditoría respecto de la gestión de riesgos

Le corresponde al Comité de Auditoría cumplir con las siguientes funciones:

4.2.2.1. Presentar a la JD u órgano que haga sus veces, un informe sobre las decisiones adoptadas por el Comité de Auditoría, por lo menos cada 6 meses, o con una frecuencia mayor, si resulta procedente.

4.2.2.2. Evaluar los riesgos que puedan afectar la ejecución de la planeación estratégica y aquellos derivados de los cambios en la AG y sus impactos en el SCI y, en caso de ser necesario, recomendar las medidas que estime oportunas para mitigar dichos impactos.

4.2.2.3. Proponer a la JD u órgano que haga sus veces, controles para prevenir, detectar y responder adecuadamente a los riesgos de fraude.

4.2.3. Funciones del Comité de Auditoría respecto de las actividades de control

Le corresponde al Comité de Auditoría cumplir con las siguientes funciones:

4.2.3.1. Aprobar la metodología para definir la criticidad de los hallazgos de la auditoría interna u órgano que haga sus veces, de la revisoría fiscal y de las auditorías externas, si es el caso.

4.2.3.2. Monitorear las funciones y actividades de la auditoría interna u órgano que haga sus veces, con el objeto de verificar que mantenga su independencia y objetividad en relación con las actividades que audita, e identificar posibles limitaciones que impidan su adecuado desempeño.

4.2.3.3. Evaluar la estructura del SCI con el fin de determinar si los procedimientos diseñados protegen razonablemente los activos de la EV y de los terceros que administre o custodie.

4.2.3.4. Velar porque la preparación, presentación y revelación de la información financiera y contable se ajuste a lo dispuesto en las disposiciones vigentes y las metas de desempeño financiero definidas por la EV, verificando que existan los controles necesarios para el efecto.

4.2.3.5. Evaluar y aprobar las propuestas de la auditoría interna u órgano que haga sus veces, relativas a la contratación de auditores externos especializados.

4.2.3.6. Evaluar si el SCI asegura razonablemente el funcionamiento de los sistemas de información, su confiabilidad e integridad para la toma de decisiones, y proponer a la JD u órgano que haga sus veces, las medidas a que haya lugar para solucionar las vulnerabilidades que sean detectadas.

4.2.3.7. Evaluar los informes realizados por la auditoría interna u órgano que haga sus veces, la revisoría fiscal y los auditores externos, verificando que se hayan implementado sus sugerencias y recomendaciones.

4.2.4. Funciones del Comité de Auditoría respecto de la información y comunicación

Le corresponde al Comité de Auditoría cumplir con las siguientes funciones:

4.2.4.1. Elaborar el informe que la JD u órgano que haga sus veces debe presentar al máximo órgano social en su reunión ordinaria respecto al funcionamiento del SCI durante el período anterior, el cual debe incluir, como mínimo, lo siguiente:

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

b. Las actividades más relevantes desarrolladas por el Comité de Auditoría.
c. Las deficiencias materiales detectadas, las recomendaciones formuladas y las medidas adoptadas, incluyendo entre otros aspectos aquellos que puedan afectar los estados financieros y el informe de gestión.
d. Las observaciones formuladas por los órganos de control y las sanciones impuestas a la EV, cuando aplique.
e. En caso de contar con un departamento de auditoría interna, la evaluación de la labor realizada por dicha área, incluyendo, entre otros aspectos, el alcance del trabajo desarrollado, la independencia de la función y los recursos asignados. En caso de que la EV no cuente con un departamento de auditoría interna debe informar las razones por las cuales no se ha considerado pertinente contar con dicho departamento.

4.2.4.2. Servir de canal de comunicación en materia de control interno entre la AG y la JD u órgano que haga sus veces.

4.2.4.3. Mantener una comunicación continua con la auditoría interna u órgano que haga sus veces, a través del presidente del Comité.

4.2.4.4. Informar a la JD u órgano que haga sus veces, cuando advierta que la EV no suministra la información requerida por las autoridades competentes y los órganos de control.

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

4.2.4.6. Presentar al máximo órgano social, por conducto de la JD u órgano que haga sus veces, los candidatos para ocupar el cargo de Revisor Fiscal, sin perjuicio del derecho de los accionistas de presentar otros candidatos. Para tal efecto, corresponde al Comité 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.

4.2.5. Funciones del Comité de Auditoría respecto de las actividades de seguimiento y monitoreo

Le corresponde al Comité de Auditoría cumplir con las siguientes funciones:

4.2.5.1. Evaluar de manera continua el cumplimiento de las normas y políticas que integran el ambiente de control y solicitar a la AG los informes que estime necesarios.

4.2.5.2. Hacer seguimiento al cumplimiento de las instrucciones dadas por la JD u órgano que haga sus veces, en relación con el SCI.

4.2.5.3. Monitorear el cumplimiento del plan anual de auditoría interna.

4.2.5.4. Evaluar la eficiencia de la auditoría interna u órgano que haga sus veces en términos de recursos y resultados, reportando a la JD u órgano que haga sus veces, las ineficiencias advertidas.

4.2.5.5. Revisar y evaluar los cambios del entorno de la EV y su modelo de negocio, siempre que puedan incidir en la gestión de riesgos o en el cumplimiento de sus objetivos estratégicos.

4.3. Comité de Riesgos

El Comité de Riesgos deberá cumplir con las obligaciones y responsabilidades previstas en los Capítulos XXX MGR, XXXI SIAR y/o XXXII SARE de la CBCF y las normas que los modifiquen o adicionen, sin perjuicio de las funciones adicionales que le sean asignadas por la JD u órgano que haga sus veces, en materia de SCI a través del reglamento de funcionamiento del Comité.

4.4. Alta Gerencia

La AG debe cumplir como mínimo con las funciones y responsabilidades previstas en los siguientes subnumerales:

4.4.1. Funciones de la Alta Gerencia respecto del ambiente de control

Le corresponde a la AG cumplir con las siguientes funciones:

4.4.1.1. Someter a consideración de la JD u órgano que haga sus veces los siguientes documentos y políticas:

a. Política de recurso humano.
b. Política financiera y contable.
c. Política de información y comunicación.
d. Política de evaluaciones y autoevaluaciones.
e. Política de inducción y capacitación de miembros de JD u órgano que haga sus veces y de sus comités de apoyo.
f. Plan estratégico.
g. Presupuesto anual.
h. Reglamentos internos de los comités de apoyo.

4.4.1.2. Someter a consideración del Comité de Auditoría los siguientes documentos y políticas:

a. Estructura, procedimientos y metodologías del SCI con líneas de responsabilidad y de rendición de cuentas.
b. Código de ética y conducta.
c. Política de generación y remisión de informes sobre el SCI.
d. Política de seguridad de la información.
e. Plan estratégico de tecnología.

4.4.1.3. Establecer una cultura organizacional de control mediante la divulgación de las normas éticas y de conducta dentro de la EV y la capacitación respecto al SCI, de forma tal que el personal de todos los niveles comprenda la importancia del control interno e identifique su responsabilidad frente al mismo.

4.4.1.4. Cooperar en lo que sea requerido por la auditoría interna u órgano que haga sus veces, para el desempeño de sus funciones.

4.4.2. Funciones de la Alta Gerencia respecto de la gestión de riesgos

Le corresponde a la AG cumplir con las siguientes funciones:

4.4.2.1. Presentar a la JD u órgano que haga sus veces, los riesgos asociados a la planeación estratégica y las medidas implementadas para su mitigación.

4.4.2.2. Identificar y evaluar los cambios que impacten la gestión de riesgos de las EV, tales como cambios macroeconómicos o regulatorios, y realizar los ajustes correspondientes en el SCI para responder a estos cambios.

4.4.2.3. Monitorear la implementación y cumplimiento de las disposiciones en materia de administración de riesgos, de acuerdo con las funciones y responsabilidades previstas en el SIAR, SARE, MGR y SARLAFT y las normas que los modifiquen o adicionen.

4.4.2.4. Desarrollar mecanismos para mitigar los riesgos de fraude en las EV.

4.4.3. Funciones de la Alta Gerencia respecto de las actividades de control

Le corresponde a la AG cumplir con las siguientes funciones:

4.4.3.1. Monitorear la implementación y cumplimiento del plan estratégico.

4.4.3.2. Velar porque los responsables de las funciones de control tengan idoneidad, independencia y recursos adecuados para llevar a cabo sus funciones.

4.4.3.3. Monitorear el cumplimiento de las políticas que definen el ambiente de control, para verificar su validez y vigencia en el tiempo.

4.4.3.4. Documentar y hacer seguimiento a la implementación de los planes de acción y medidas correctivas para resolver los hallazgos identificados en las autoevaluaciones y evaluaciones internas y externas.

4.4.4. Funciones de la Alta Gerencia respecto de la información y comunicación

Le corresponde a la AG cumplir con las siguientes funciones:

4.4.4.1. Establecer mecanismos que garanticen la comunicación efectiva con las diferentes áreas de la EV para obtener de manera oportuna la información necesaria para el cumplimiento de sus funciones.

4.4.4.2. Informar a la JD u órgano que haga sus veces, así como a los comités de apoyo, sobre el funcionamiento y disponibilidad de los sistemas de información y comunicación de la EV. Para este efecto, deben establecerse los indicadores correspondientes.

4.4.4.3. Comunicar las políticas y decisiones adoptadas por la JD u órgano que haga sus veces, a los funcionarios de la EV de conformidad con sus roles y responsabilidades.

4.4.4.4. Suministrar la información requerida por los órganos de control y las autoridades competentes.

4.4.4.5. Monitorear el funcionamiento de los controles descritos en el subnumeral 3.3. del presente Capítulo, y adoptar medidas que resulten necesarias para corregir las fallas que se presenten.

4.4.4.6. Preparar y entregar con la antelación definida en su reglamento, a la JD u órgano que haga sus veces y a los diferentes órganos de gobierno, la información necesaria sobre los temas a tratar en cada reunión ordinaria o extraordinaria del respectivo órgano colegiado.

4.4.5. Funciones de la Alta Gerencia respecto de las actividades de seguimiento y monitoreo

Le corresponde a la AG cumplir con las siguientes funciones:

4.4.5.1. Verificar que se cumplan las obligaciones en materia de rendición de cuentas definidas al interior de la EV y que su cumplimiento esté documentado.

4.4.5.2. Mantener actualizados los manuales de funciones de la AG, el código de ética y el de gobierno corporativo.

4.4.5.3. Verificar el cumplimiento del marco de apetito de riesgos de la EV, de acuerdo con las disposiciones que les resulten aplicables.

4.4.5.4. Definir oportunamente los planes de acción para atender los hallazgos de las evaluaciones sobre los diferentes componentes del SCI.

4.4.5.5. Monitorear los cambios del entorno de la EV y su modelo de negocio, evaluando su incidencia en la gestión de riesgos y en el cumplimiento de sus objetivos estratégicos.

4.5. Auditoría Interna u órgano que haga sus veces

La auditoría interna u órgano que haga sus veces debe cumplir como mínimo con las funciones y responsabilidades previstas en los siguientes subnumerales:

4.5.1. Funciones de la Auditoría Interna u órgano que haga sus veces respecto del ambiente de control

Le corresponde a la auditoría interna u órgano que haga sus veces cumplir con las siguientes funciones:

4.5.1.1. Elaborar y someter a consideración del Comité de Auditoría los siguientes documentos:

a. Estatuto de auditoría interna.
b. Plan anual de auditoría interna.

c. Política de aseguramiento y mejora de la calidad de la auditoría interna.

4.5.1.2. Establecer los procedimientos para el ejercicio de la actividad de auditoría interna.

4.5.1.3. Determinar los recursos necesarios para el adecuado ejercicio de sus funciones y solicitarlos a la JD u órgano que haga sus veces.

4.5.2. Funciones de la Auditoría Interna u órgano que haga sus veces respecto de la gestión de riesgos

Le corresponde a la auditoría interna u órgano que haga sus veces, someter para aprobación del Comité de Auditoría las propuestas para la contratación de auditorías externas especializadas.

4.5.3. **Funciones de la Auditoría Interna u órgano que haga sus veces respecto de las actividades de control**

Le corresponde a la auditoría interna u órgano que haga sus veces, cumplir con las siguientes funciones:

4.5.3.1. Establecer las actividades de control al interior del área de auditoría interna que contribuyan a garantizar el cumplimiento de sus funciones.

4.5.3.2. Dar su opinión sobre la efectividad de los controles, y proponer soluciones para abordar las oportunidades de mejora identificadas, de acuerdo con lo previsto en el plan anual de auditoría.

4.5.3.3. Presentar al Comité de Auditoría los hallazgos identificados en las evaluaciones internas o externas de la EV, o del área de auditoría interna, de acuerdo con su nivel de criticidad.

4.5.3.4. Informar al Comité de Auditoría las decisiones tomadas por el área de auditoría interna que considere relevantes.

4.5.3.5. Establecer los mecanismos para garantizar la seguridad de la información del trabajo del área de auditoría interna.

4.5.3.6. Realizar seguimiento al trabajo realizado por los integrantes de su equipo, verificando que se cumplan los estándares de calidad correspondientes.

4.5.3.7. Revisar los controles adoptados por la AG para garantizar el cumplimiento de la normativa aplicable, códigos y políticas internas, de acuerdo con lo previsto en el plan anual de auditoría.

4.5.3.8. Hacer seguimiento al cumplimiento e implementación de las recomendaciones del Comité de Auditoría.

4.5.4. Funciones de la Auditoría Interna u órgano que haga sus veces respecto de la información y comunicación

Le corresponde a la auditoría interna u órgano que haga sus veces, cumplir con las siguientes funciones:

4.5.4.1. Evaluar el cumplimiento de la política de información y comunicación, de acuerdo con lo previsto en el plan anual de auditoría.

4.5.4.2. Presentar al Comité de Auditoría informes sobre su gestión, los hallazgos identificados, las recomendaciones para abordar dichos hallazgos y el cumplimiento del plan de auditoría.

4.5.4.3. Reunirse con la JD u órgano que haga sus veces, y con el Comité de Auditoría sin la presencia de la AG, cuando lo estime necesario.

4.5.4.4. Acceder a la información de la EV y entrevistar a sus funcionarios cuando lo requiera para obtener la información necesaria para el cumplimiento de sus funciones.

4.5.4.5. Presentar a la JD u órgano que haga sus veces, un informe anual de su gestión y su evaluación sobre la eficacia del SCI, de acuerdo con lo previsto en el plan anual de auditoría que contenga, como mínimo, lo siguiente:

a. Identificación de los temas, procesos, y áreas objeto del examen, el periodo y criterios de evaluación, y los responsables de la información tenida en cuenta para la elaboración del informe.
b. Descripción de los resultados de las siguientes evaluaciones:
    i. Cumplimiento de la política contable y financiera.
    ii. Funcionamiento del SCI.
    iii. Calidad de los sistemas establecidos para garantizar el cumplimiento de las disposiciones normativas aplicables y las políticas establecidas por la EV.
    iv. Análisis de la estructura organizacional de la EV.
c. Resultados de la evaluación realizada respecto del funcionamiento y efectividad del SCI y el sistema de administración de riesgos.
d. Descripción del procedimiento para obtener las evidencias, indicando el soporte técnico de sus conclusiones.
e. Limitaciones encontradas en la realización de las evaluaciones o en el acceso a información u otros eventos que hayan afectado el resultado de las pruebas realizadas y las conclusiones.
f. Recomendaciones formuladas sobre deficiencias materiales detectadas, mencionando los criterios generales que se tuvieron en cuenta para determinar su importancia.
g. Resultados del seguimiento a la implementación de las recomendaciones formuladas en informes anteriores.
h. Identificación y firma de las personas que elaboraron el informe, ciudad y fecha de elaboración.

4.5.5. Funciones de la Auditoría Interna u órgano que haga sus veces respecto de las actividades de seguimiento y monitoreo.

Le corresponde a la auditoría interna u órgano que haga sus veces cumplir con las siguientes funciones:

4.5.5.1. Evaluar la efectividad del SCI en las áreas y procesos de las EV, teniendo en cuenta las políticas definidas por la JD u órgano que haga sus veces.

4.5.5.2. Evaluar el cumplimiento de las recomendaciones de la JD u órgano que haga sus veces, los comités de apoyo y la Revisoría Fiscal, con el fin de verificar si fueron implementadas bajo la dirección de la AG.

4.5.5.3. Evaluar el funcionamiento de los controles establecidos por la EV, de acuerdo con lo previsto en el plan de auditoría interna.

4.5.5.4. Evaluar las actividades tercerizadas por la EV, verificando que se cumplan las disposiciones aplicables y los lineamientos internos en esta materia, de acuerdo con lo previsto en el plan anual de auditoría.

4.5.5.5. Verificar que las decisiones adoptadas por los órganos de gobierno atiendan lo previsto en las disposiciones normativas y en los lineamientos internos aplicables.

4.5.5.6. Hacer las recomendaciones a las áreas competentes para mejorar el proceso de gobierno corporativo.

4.5.5.7. Dar su opinión en las investigaciones que se adelanten al interior de la EV cuando sea solicitada en asuntos relativos a posibles conflictos de interés.

5. MODELO DE LAS TRES LÍNEAS

El modelo de las tres líneas propuesto por el IIA promueve la creación de estructuras de gobierno y procesos que contribuyen a la materialización de los objetivos estratégicos de las EV y facilitan la gestión de los riesgos.

Las EV deben tener en cuenta el referido modelo en la asignación de funciones a todo su personal y en la definición de las líneas de rendición de cuentas.

5.1. Asignación de funciones

Independientemente de la estructura que defina cada EV para el diseño de su SCI, las EV deben asignar responsabilidades a su personal, teniendo en cuenta las funciones generales que establece el modelo de las tres líneas, de tal manera que se definan claramente los roles y responsabilidades de cada una de ellas, así como la forma en que se interrelacionan, conforme se establece a continuación:

5.1.1. Primera línea

Las EV deben contar con funcionarios encargados de identificar los riesgos asociados a las actividades que ejecuta la EV en el desarrollo de su operación e implementar los controles necesarios.

5.1.2. Segunda Línea

Las EV deben contar con funcionarios encargados de evaluar la gestión de riesgos, apoyar la identificación de los controles para la mitigación de los riesgos, verificar la correcta aplicación de los controles y aportar su conocimiento especializado para el direccionamiento de la EV.

5.1.3. Tercera Línea

Las EV deben contar con funcionarios encargados de ejecutar actividades de aseguramiento y asesoría independiente. En aquellas EV que cuenten con un área de auditoría interna u órgano que haga sus veces, las funciones de tercera línea serán desempeñadas por esta área, de acuerdo con lo previsto en el subnumeral 4.5. del presente Capítulo.

5.2. Líneas de rendición de cuentas

Las EV deben definir líneas de rendición de cuentas internas y externas, entendidas como las instancias y los canales a través de los cuales se informa el cumplimiento de las funciones de control interno. En ese sentido, tanto la primera como la segunda línea responden por la observancia de sus responsabilidades ante la AG. Por su parte, la tercera línea debe responder por la observancia de sus responsabilidades ante la JD u órgano que haga sus veces y ante el Comité de Auditoría.