SISTEMA DE CONTROL INTERNO

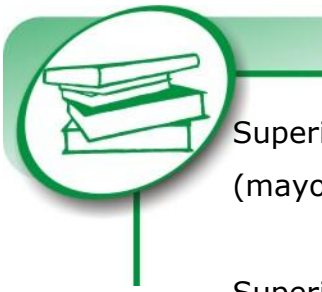
1. SISTEMA DE CONTROL INTERNO (SCI)

Ideas rectoras

Las organizaciones de economía solidaria deben establecer unas políticas e implementar planes y programas de control interno, de identificación y gestión de riesgos y de auditoria, con el fin de garantizar el cumplimiento de su objeto, dada la naturaleza de su actividad.

Justificación

En el marco de la normatividad legal y reglamentaria Coomeva, como entidad cooperativa financiera, ha definido como un elemento indispensable el desarrollo y fortalecimiento de su sistema de control interno, adecuándolo a los lineamientos establecidos por la Superintendencia Financiera de Colombia, de tal manera que este sistema contribuya al logro de sus objetivos y fortalezca en particular la apropiada administración de los riesgos a los cuales se ve expuesta en el desarrollo de su actividad.



Referencia bibliográfica

Superintendencia Financiera de Colombia – Circular Externa 014 de 2009 (mayo 19).

Superintendencia Financiera de Colombia – Circular Externa 038 de 2009 (septiembre 29).

El *control interno* significa que la organización implementa un sistema que se actualiza y revisa constantemente con el que se logra eficacia y eficiencia en todas las operaciones, siendo uno de sus fines la prevención y mitigación de la ocurrencia de fraudes o errores, originados tanto al interior como al exterior de la organización.

Conceptos

Eficacia: capacidad de alcanzar las metas y los resultados propuestos.

Eficiencia: capacidad para producir el máximo de resultados con el mínimo de inversión en tiempo y recursos.

En este sentido, se exige orientar a todas las instancias pertinentes, en la implementación de un *Sistema de Control Interno* (SCI) sustentado en la autorregulación y el autocontrol de todos los integrantes de la organización, quienes deben autoevaluar y ejercer pleno dominio sobre la calidad e integridad de su labor. Este sistema de estructuración organizacional garantiza la transparencia y la seguridad en las funciones que se ejercen.

Definición y objetivo

Teoría

Un ***Sistema de Control Interno (SCI)*** es un conjunto de políticas, principios, normas y procedimientos de verificación y evaluación que se establecen para garantizar eficacia, eficiencia, transparencia y seguridad en el actuar de una organización.

El monitoreo permanente del SCI, la revisión y mejora de las acciones de control y la toma de medidas efectivas previenen y mitigan riesgos y fraudes. De esta manera constituye un elemento fundamental del gobierno corporativo.

Objetivos del SCI

- ✓ 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.

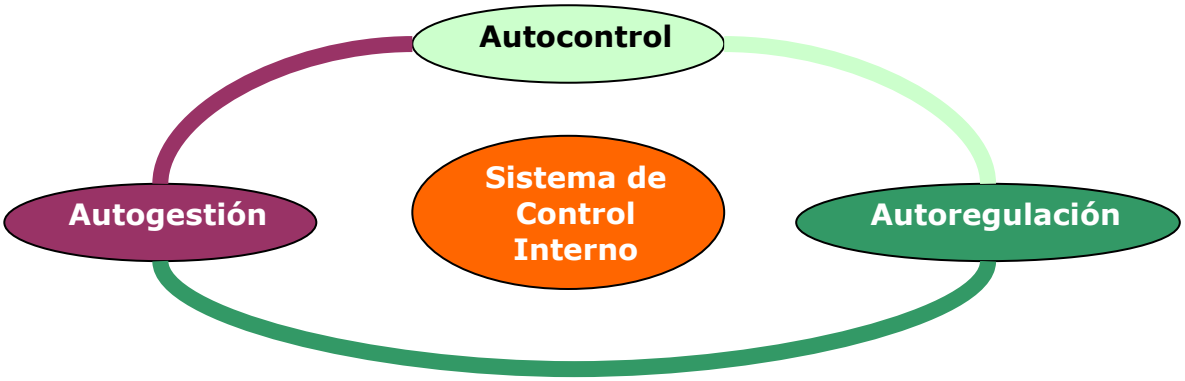
Principios de un SCI

Ideas rectoras

Los principios del SCI garantizan su efectividad de acuerdo con la naturaleza de las operaciones, funciones y características de la organización.

La implementación de programas relacionados con el *Sistema de Control Interno* de Coomeva, su revisión, actualización y mejora, debe cubrir todas las empresas, unidades de negocio, sucursales y agencias de la entidad. Así, los principios que rigen el SCI deben ser aplicados bajo un entorno organizacional de validación al control, la mitigación y prevención de riesgos y fraudes y las labores de auditoría interna y externa.

Estos principios son autocontrol, autorregulación y autogestión.



Valores y principios

Autocontrol: capacidad responsable de todos los funcionarios de la organización, independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos para la mejora de su labor.

Autorregulación: se refiere a la capacidad de la organización para aplicar métodos, normas y procedimientos que permitan el desarrollo, implementación y mejoramiento del *Sistema de Control Interno (SCI)* dentro del marco normativo legal.

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

Las reglas, parámetros generales y requisitos contemplados en el SCI de Coomeva, han sido ajustados de conformidad con lo señalado en los Artículos 72 y 73 del Decreto 4327 de 2005, de acuerdo con su tamaño, la naturaleza de sus actividades y la complejidad de sus operaciones, teniendo en cuenta la relación beneficio / costo. El Consejo de Administración analizó y verificó este punto teniendo en cuenta su conocimiento de la misma, del sector económico al que pertenece y de los riesgos que enfrenta, teniendo en cuenta que el costo de las medidas adoptadas no excede el beneficio que de ellas se deriva.

2. ESTRUCTURA DEL SISTEMA DE CONTROL INTERNO (SCI)

La aplicación de procesos operativos apropiados exige unos elementos para la consolidación de la estructura del *Sistema de Control interno (SCI)* que son:

1. Ambiente de control
2. Sistema de administración y gestión de riesgos
3. Actividades de control
4. Sistema de información y comunicación
5. Monitoreo
6. Evaluaciones independientes

Veamos cada uno de ellos.

1) Ambiente de control

Se corresponde con la cultura organizacional que fomenta en una organización principios, valores y conductas orientadas hacia el control y el sentido de

integridad. Personal competente y un adecuado ambiente organizacional garantizan que en las entidades se implemente, evalúe y mejore permanentemente el SCI.

Herramienta

En Coomeva este *ambiente de control*, esta cultura organizacional, orientada a la integridad y la transparencia, se ha impulsado a través de los Estatutos, el Código de Buen Gobierno Corporativo, el Código de Ética y entes de control como son: el Comité de Auditoría Corporativa y la Junta de Vigilancia, entre otras instancias.

La entidad debe contar también con estándares documentados de las competencias, habilidades, aptitudes e idoneidad de sus funcionarios y dirigentes. Así mismo, debe determinar las políticas y prácticas de gestión humana que aplicará al realizar los procesos de selección, inducción, capacitación, remuneración y evaluación del desempeño de sus colaboradores, prácticas que son implementadas para lograr un efectivo control interno.

Método

La base de ese adecuado *ambiente de control* requiere:

- ✓ definir claramente los niveles de autoridad y responsabilidad, precisando el alcance y límite de los mismos,
- ✓ forjar los conocimientos, habilidades y conductas necesarias para el desempeño de las funciones de los colaboradores, organismos de administración y entes de control y
- ✓ determinar una estructura organizacional que soporte el SCI.

2) Sistema de administración y gestión de riesgos

Preservar la eficacia, eficiencia y efectividad de la gestión y capacidad operativa de una organización, así como salvaguardar los recursos, obliga a aplicar un sistema de administración de riesgos que permita minimizar costos y daños ocasionados por los eventos que, en el caso de Coomeva, comporta la operación administrativa y financiera.

Autoevaluar los riesgos existentes en los procesos, identificándolos y priorizándolos, a través de un ejercicio de valoración, teniendo en cuenta los factores propios del entorno y la naturaleza de la actividad, se convierten en soporte de este sistema.

Método

El análisis del contexto estratégico, la determinación de métodos para el monitoreo y tratamiento de riesgos y la mitigación de su impacto, son algunas de las exigencias para el buen funcionamiento de este sistema de administración y gestión.

Análisis de riesgos

El análisis de los riesgos en economía representa la estimación de los riesgos implícitos en una actividad. Todas las decisiones que se toman implican un cierto grado de incertidumbre. Los elementos esenciales para efectuar un mapa de riesgos son: la identificación de los posibles riesgos, lo que implica su cuantificación y la evaluación de éstos.

La identificación depende, en gran medida, de la información disponible y la valoración del analista que debe ponderar:

- La probabilidad de ocurrencia de los riesgos.
- El cálculo de los riesgos máximo y mínimo.
- La valoración del riesgo real como posibilidad de que se produzca el resultado previsto.

- La determinación del grado de control que se ejerce sobre dichos riesgos.

Teoría

La calidad y mejora de la información para la toma de decisiones que posee una organización puede aumentar si se dedican fondos para el análisis y la investigación. En este sentido, el análisis de los riesgos así como de los *sistemas de control interno* no son operaciones estáticas. La gestión y análisis de los riesgos debe revisarse cuando se dispone o se obtiene información adicional o cuando las circunstancias varían.

Hay tres aspectos importantes en el análisis de riesgos: los factores de riesgo, el perfil de riesgo y los indicadores de riesgo.

Factores de riesgo: Fuentes generadoras de eventos, dichos factores de riesgo pueden ser:

- ✓ Internos: Recursos humanos; procesos; tecnología, infraestructura.
- ✓ Externos: Eventos asociados a la fuerza de la naturaleza o los ocasionados por terceros que escapan en cuanto a su causa y origen al control de la organización.

Perfil de riesgo: Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.
Indicadores de riesgo: sus características se presentan en la siguiente tabla:

Indicadores de riesgo	***Características***
Riesgo de Mercado	Posibilidad de que se produzca una pérdida debido a un movimiento adverso de las variables de mercado que determinan el valor de la cooperativa, tales como tipo de interés, tipo de cambio, cotización de las acciones y precios de los activos en general.
Riesgo de Liquidez	Posibilidad de que la entidad incurra en pérdidas excesivas por la venta de activos a descuentos inusuales y significativos o deba obtener fondos a precios por fuera de las condiciones normales de mercado, con el fin de disponer rápidamente de los recursos necesarios para cumplir con sus obligaciones contractuales.
Riesgo de Crédito	Posibilidad de que se incurra en pérdidas y se disminuya el valor de los activos, como consecuencia de que un deudor o contraparte incumpla sus obligaciones.
Riesgo Operacional	Posibilidad de que se produzca una pérdida financiera, debido a acontecimientos inesperados en el entorno operativo y tecnológico de la entidad. Deficiencias en el control interno, procedimientos inadecuados, errores humanos, fraudes y fallos en los sistemas informáticos son algunos de los riesgos operativos en los que puede incurrir una organización.
Riesgo Operativo	Supone la posibilidad de incurrir en pérdidas por deficiencias, o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Este tipo de riesgo incluye también el riesgo legal y reputacional.
Riesgo Jurídico	Supone una pérdida debido a que una operación no pueda ejecutarse por no existir una formalización clara o por no ajustarse al marco legal establecido. También se considera dentro de este riesgo los eventos que se produzcan por cambios o incumplimiento de la normatividad y la legislación que afecten negativamente los recursos de la entidad.

Indicadores de riesgo	***Características***
Riesgo de Negocio	Posibilidad de incurrir en pérdidas o dejar de percibir ganancias debido a movimientos negativos en el volumen de negocios, el volumen de ingresos o los márgenes esperados.
Riesgo del Asociado	Posibilidad de que los asociados se retiren de la entidad.
Riesgo Reputacional	Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto a sus prácticas que cause pérdida de clientes, disminución de ingresos o que comporte procesos judiciales.
Riesgo Residual	Nivel resultante del riesgo después de aplicar los controles. Es el riesgo que queda, una vez se han instrumentado los controles pertinentes. Exige un permanente monitoreo para observar su evolución.
Riesgo Inherente	Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Eventos de riesgo operativo

Un evento es un incidente o situación que ocurre en un lugar particular, durante un intervalo de tiempo determinado. Los eventos de pérdida son aquellos incidentes que generan pérdidas por riesgo operativo a las entidades y que repercuten sobre las relaciones laborales y los clientes. Este tipo de eventos se clasifican en:

Eventos de riesgo operativo	***Características***
Fraude interno	Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad o incumplir normas o leyes. Fraude en el que está implicado un colaborador o administrador de la organización.

Eventos de riesgo operativo	***Características***
Fraude externo	Actos realizados por una persona externa a la entidad, que buscan defraudar o apropiarse indebidamente de activos o incumplir normas o leyes.
Daños a activos físicos	Pérdidas derivadas de daños o perjuicios a activos físicos de la entidad.
Fallas tecnológicas	Pérdidas derivadas de incidentes por fallas informáticas o tecnológicas.
Fallas en la ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de los procesos.

Método

Un análisis de riesgos requiere estudiar los siguientes aspectos:

- ✓ *Identificación de causas: ¿*por qué se puede presentar un evento o incidente?

- ✓ *Consecuencias:* efectos en caso de presentarse un evento.

- ✓ *Probabilidad:* Medida de oportunidad de la ocurrencia de un evento. Para valorizar la probabilidad se calificará así: Alta = 5; Media = 3 y Baja = 1.

- ✓ *Impacto:* Se califica como Leve = 5; Moderado = 10 y Catastrófico = 20. Las unidades de medida para el impacto, se califican teniendo en cuenta sus efectos económicos, reputacionales y legales.

- ✓ Una vez se realice la medición de la probabilidad y el impacto para los riesgos de cada proceso, se debe realizar la medición consolidada, determinando el perfil de Riesgo Inherente.

- ✓ *Valoración:* Según el resultado numérico, el riesgo puede ser catalogado como: Inaceptable, Importante, Moderado y Tolerable.

- ✓ Controles*:* Identificación y puesta en marcha de las acciones y los controles que se tienen para prevenir un riesgo, y si fuera el caso, enunciar los que deben implementarse de manera adicional o sustitutiva, así como definir los responsables. Para mitigar el riesgo en forma efectiva las medidas de control deben considerar el costo de su implementación, frente al impacto esperado, con base en la probabilidad de ocurrencia de cada riesgo. Del mismo modo, se deben identificar los factores limitantes que puedan impedir el desarrollo de las acciones de mitigación.

- ✓ Implementados los controles se debe revisar la medición de la probabilidad y el impacto en las áreas responsables y los procesos modificados, determinando el perfil del Riesgo Residual y el nuevo perfil de riesgo consolidado.

- ✓ Estos son algunos de los aspectos que permiten identificar, hacer seguimiento y monitorear un riesgo operativo:

    - Riesgo al que se hace referencia
    - Fecha de inicio del evento
    - Fecha de finalización del evento
    - Fecha del descubrimiento
    - Fecha en que se registra contablemente la pérdida por el evento

- Cuantía de la pérdida
- Cuantía total recuperada por acción directa de la Entidad (incluye cuantías recuperadas por seguros)
- Cuantía recuperada por seguros
- Clase de evento (fraude interno, fraude externo, clientes, daños a activos físicos, fallas tecnológicas, ejecución, administración de procesos)
- Producto o servicio afectado
- Proceso afectado
- Tipo de pérdida
- Descripción detallada del evento

Gestión de riesgos

Existen además normas e instrucciones especiales en materia de gestión de ciertos riesgos, aplicables en virtud del objeto social de cada entidad. Algunas de las denominaciones de estos riesgos son:

Gestión de riesgos de mercado ***– SARM***

Medición y toma de decisiones sobre la exposición al riesgo de mercado. Coomeva emplea el Modelo Estándar sugerido por la Superintendencia Financiera de Colombia. La exposición a este tipo de riesgo representa en la Cooperativa un porcentaje del valor del portafolio.

Método

Con el objetivo de diversificar la exposición al riesgo de mercado el Consejo de Administración aprueba inversiones en bonos para el portafolio de inversiones del Fondo de Solidaridad dada su naturaleza de largo plazo.

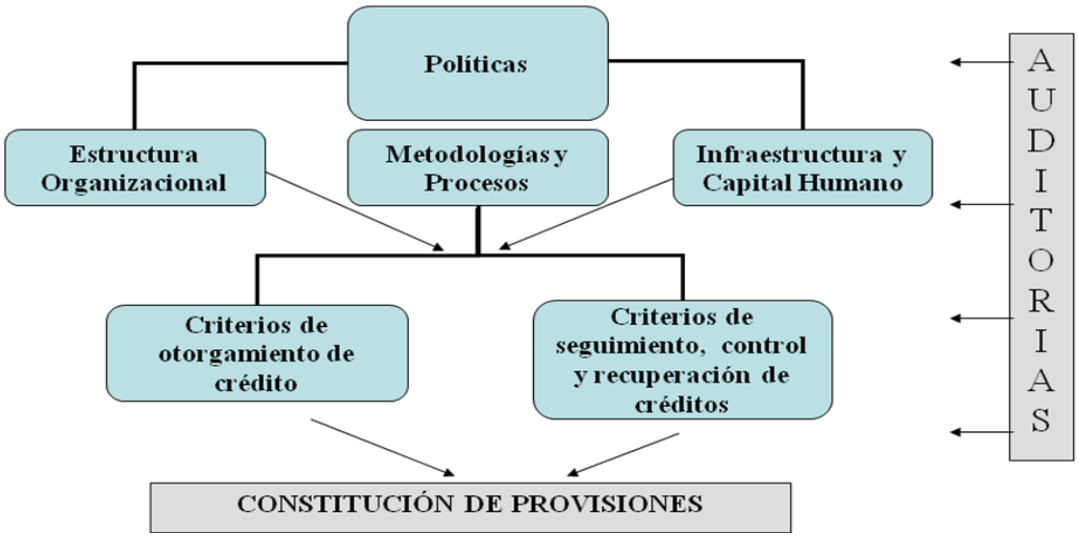
Gestión de riesgo de crédito ***–SARC***

La política de Coomeva Cooperativa Financiera en la concesión de crédito se fundamenta en el análisis de la situación del cliente: capacidad de pago del deudor y sus co-deudores, así como el flujo de caja del proyecto, de conformidad con información financiera actualizada y documentada; servicio de la deuda, cumplimiento de los términos pactados; información proveniente de centrales de riesgo, consolidadas con el sistema, y de las demás fuentes de información comercial de las cuales dispone la institución. También se considera la información relacionada con el conglomerado económico, las reglas de alineamiento con respecto a otros créditos del cliente y las provisiones.

La calificación por riesgo del deudor es establecida por una escala así:

"a" riesgo normal: vencimientos hasta 2 meses
"b" riesgo aceptable: vencimientos superiores a 2 meses y hasta 5 meses
"c" riesgo apreciable: vencimientos superiores a 5 meses y hasta 12 meses
"d" riesgo Signifcativo: vencimientos superiores a 12 meses y hasta 18 meses
"e" riesgo de incobrabilidad: vencimientos de más de 18 meses

El Sistema de Administración de Riesgo Crediticio - *SARC*



Método

Este proceso corresponde igualmente a la aplicación de medidas que permitan el conocimiento pleno del deudor actual y potencial, capacidad y fuentes de pago, solvencia, garantías ofrecidas, condiciones financieras del préstamo y externalidades a las que el deudor puede estar expuesto.

Gestión de riesgo operativo ***–SARO***

La gestión de este riesgo consiste en implementar un programa de identificación, evaluación, documentación y actividades que permitan prevenir el riesgo relacionado con errores operativos.

Método

Diseñar acciones correctivas y de contingencia, a partir de los hallazgos en este sistema de administración y gestión, permite integrar las políticas del personal de Tesorería y de la plataforma tecnológica, que son los que soportan la operación y documentación de todos los procedimientos en Coomeva.

De este modo, el Consejo de Administración de la Cooperativa ha definido políticas, procedimientos y controles dentro del Sistema de administración de riesgo de las operaciones de Tesorería como son:

- Control de límites por negociabilidad de las inversiones
- Control a la exposición por riesgo de mercado para cada uno de los portafolios de inversión
- Control al límite de operación diaria, por emisor y/o contraparte
- Control a la concentración por emisor para cada uno de los portafolios
- Control a los niveles de liquidez a corto, mediano y largo plazo

Método

Uno de los miembros del Consejo de Administración es miembro del Comité Corporativo de Inversiones y Riesgos Financieros. Comité encargado de analizar, evaluar y presentar ante el Consejo de Administración resultados de la gestión de los riesgos inherentes a las operaciones de Tesorería.

El Comité y el Consejo de Administración cuentan además con el apoyo del Comité de Tesorería, el Comité Financiero Corporativo y el Comité de Auditoria.

Gestión de riesgo de liquidez ***–SARL***

El riesgo de liquidez se refiere a las perdidas en las que puede incurrir una organización. La administración y el control de la liquidez de corto, mediano y largo plazo tiene establecidos unos procedimientos y controles estandarizados que son monitoreados, en Coomeva, por el Comité de Tesorería, para asegurar la relación entre las entradas y salidas de los recursos financieros y para soportar la operación.

Ejemplo

El Sistema de Administración de Riesgo de las operaciones de Tesorería a través de su estructura de Front Ofce (negociación), Middle (controles) y Back Ofce (cierre, cumplimiento y contabilización) le ha permitido a Coomeva monitorear el nivel de exposición a los diferentes riesgos y posicionarla como una organización con un nivel menor de riesgo de liquidez.

Gestión de riesgo de lavado de activos y de financiación del terrorismo ***– SARLAFT***

El lavado de activos y la financiación del terrorismo representan una amenaza para la estabilidad del sistema financiero y la integridad de los mercados por su carácter global y las redes utilizadas para el manejo de tales recursos. Tal circunstancia destaca la importancia actual del control de este tipo de riesgo.

Ejemplo

Prevenir la legalización de activos provenientes de actividades delictivas o la canalización de recursos para o procedentes de actividades terroristas recae en Coomeva sobre la Unidad de Tecnología e Informática. Mediante un aplicativo se consultan las listas de lavado de activos y financiación del terrorismo. Esta acción de control, de este tipo de riesgo, se encuentra basada en el procedimiento SS-DC-013.

Identificar las amenazas que enfrenta la entidad y las fuentes de las mismas hace parte de la gestión y administración de este riesgo de lavado de activos y financiación del terrorismo, en el que hay que continuar capacitando el personal para lograr instaurar una cultura de la prevención.

Es una labor importante detectar y reportar las operaciones que se pretendan realizar o se hayan realizado aparentemente de forma legal, y medir la probabilidad de ocurrencia de estos riesgos y su impacto sobre los recursos económicos, financieros y humanos de la entidad, así como sobre su credibilidad y buen nombre.

Mensaje

Solo el análisis razonable y objetivo sobre los eventos ocurridos, la valoración de los controles existentes y la medición de su ocurrencia y efectividad podrán garantizar la prevención y mitigación del impacto de un determinado tipo de riesgo dentro del funcionamiento general del Sistema.

Gestión de riesgo de garantías ***–SARG***

Las garantías que respaldan la operación son necesarias para calcular las pérdidas esperadas en el evento de no pago y, por consiguiente, para determinar el nivel de provisiones. Las garantías deben ser idóneas y sobre un valor establecido, con base en criterios técnicos y objetivos, que ofrezcan un respaldo jurídicamente eficaz al pago de la obligación. Para evaluar el respaldo ofrecido y la posibilidad de realización de cada garantía se debe tener en cuenta su naturaleza, idoneidad, liquidez, valor y cobertura.

Idea

Una garantía admisible se rige por la eficacia jurídica que ofrezca, de tal forma que se de un respaldo jurídico al pago de la obligación. En consecuencia, debe tenerse presente que, constituye requisito indispensable dentro del contrato, la limitación de disposición del objeto de la garantía, a efectos de poder hacer efectivos los derechos de persecución y preferencia.

Con el propósito de dar cumplimiento a las normas, los establecimientos de crédito deben efectuar un avaluó previa constitución de la garantía. Dicho avalúo deberá estar acompañado de una explicación sobre los criterios técnicos aplicados en su elaboración.

Las garantías no admisibles tienen que ver con criterios que no permiten verificar su suficiencia y eficacia, tales garantías no pueden ser aceptadas en el otorgamiento de aquellos créditos que, por ejemplo, superen los límites de los cupos individuales.

Recuerde

Las políticas y los criterios establecidos para la identificación, medición, control, evaluación y administración de riesgos deben estar de conformidad con las normas vigentes expedidas por la Superintendencia de Economía Solidaria y la Superintendencia Financiera de Colombia.

La Superintendencia de Economía Solidaria puede revisar en cualquier momento las clasificaciones y valoraciones que efectúe cada organización solidaria vigilada y ordenar las modificaciones pertinentes. Todas las organizaciones solidarias sometidas al control y vigilancia de la Superintendencia de la Economía Solidaria, independientemente que califiquen y realicen la valoración establecida, deberán someterse al régimen de provisiones.

Las provisiones son formas de protección que deben asumir las organizaciones para garantizar su fortaleza y respaldo en cada operación. Por cada ejercicio la organización preserva unos fondos que garantizan el cumplimiento de su objeto y labor.

Ejemplo

Coomeva hace dos tipos de provisiones para la cartera de créditos:

- ✓ Provisión general: porcentaje sobre el total de la cartera bruta de vivienda.
- ✓ Provisión individual: se constituyen provisiones individuales para la protección de los créditos según el nivel de clasificación en las diferentes categorías y según las reglas de alineamiento.

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 y de los entes de control, con relación a riesgos y controles, se cumplan. Las *actividades de control* cubren todos los niveles y funciones y son actividades obligatorias para todas las áreas, operaciones y procesos de la entidad:

- ✓ *Revisiones de alto nivel*: son los análisis de los informes y presentaciones solicitados por los miembros del Consejo de Administración, el Comité de Auditoria Corporativa y los encargados de Auditoría interna y externa. Estas revisiones se realizan con el fin de monitorear el progreso de la entidad, detectar problemas, identificar deficiencias de control, errores en los informes financieros o actividades fraudulentas, para poder adoptar los correctivos necesarios.

- ✓ *Controles generales:* rigen para todas las aplicaciones de los sistemas y los procesos y son los que aseguran la continuidad y la operación adecuada. Dentro de éstos se incluyen aquellos que se hacen sobre la administración de tecnología de información, su infraestructura, administración de seguridad y la adquisición, desarrollo y mantenimiento de software.

- ✓ *Controles de aplicación:* controles que se centran en la suficiencia, exactitud, autorización y validez de la captura y procesamiento de datos. Estos controles permiten que los datos de las aplicaciones de soporte estén disponibles y que los errores de interface se detecten y puedan corregirse rápidamente.

- ✓ *Limitaciones de acceso*: de acuerdo con el nivel de riesgo, asociado a las distintas áreas de la organización, se debe limitar el acceso y la circulación.

- ✓ *Supervisión de visitantes:* 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.

- ✓ *Controles físicos adicionales*: Son todos aquellos controles que resulten necesarios para garantizar la seguridad de las personas, datos y equipos.

- ✓ *Indicadores de rendimiento y segregación de funciones:* se refiere a todas aquellas variables y toma de medidas que determinan la eficacia y eficiencia del personal y de una determinada actividad, operación o función.

- ✓ *Acuerdos de confidencialidad:* las organizaciones financieras se rigen por la reserva bancaria y por la importancia en la salvaguarda de la información de sus clientes y usuarios. La confidencialidad en la información y en los datos debe ser garantizada dentro de un *Sistema de control interno* y debe hacer parte del inventario de riesgos y vulnerabilidades de una organización.

- ✓ *Procedimientos de control:* son todas aquellas actividades que al ser parte de un *Sistema de control interno* garantizan una supervisión y monitoreo permanente, continuo y efectivo.

- ✓ *Difusión de las actividades de control:* todas las actividades de control deben ser dadas a conocer a todos los miembros y funcionarios de la organización.

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

Las actividades de control implican, por lo tanto, una política que debe establecer los procedimientos para la determinación y prevención de los riesgos potenciales

y reales, errores, fraudes y otras situaciones que afecten o puedan llegar a afectar la estabilidad y el prestigio de la entidad.

4) Sistema de información y comunicación

La operación de las organizaciones depende hoy, en gran medida, de sus sistemas de información. En este sentido, es necesario adoptar controles que garanticen la seguridad en el acceso (confidencialidad, integridad y disponibilidad), calidad (efectividad, eficiencia, y confiabilidad) y cumplimiento de la información generada. El sistema debe ser además oportuno y funcional en el suministro de la procedencia de la fuente de información y de determinados datos al personal autorizado.

Los sistemas de información y comunicación son la base para identificar, intercambiar información y tomar decisiones que permitan a los funcionarios cumplir con su labor y a los usuarios contar con elementos de juicio suficientes para la utilidad y demanda de beneficios y servicios, según la naturaleza de la entidad.

Los sistemas de información y comunicación deben garantizar la aplicación de los criterios de seguridad y transparencia (copias de respaldo y custodia), calidad (almacenamiento y conservación) y cumplimiento, para lo cual deberán establecerse controles generales y específicos para la entrada de la información, su procesamiento y salida, atendiendo el nivel de importancia y riesgo.

Método

Diseñar procedimientos para detectar, reportar y corregir los errores, deficiencias y las irregularidades que puedan presentarse y establecer estrategias que permitan retener o reproducir los documentos originales, para facilitar la reconstrucción de los datos, así como para satisfacer requerimientos legales, son algunas de las *actividades de control* que garantizan la efectividad del *Sistema de información y comunicación.*

Es necesario también evitar la filtración, difusión inapropiada y la tergiversación de la información. La entidad debe mantener, en este sentido, una comunicación eficaz, suficiente y veraz que fluya en todas las direcciones y áreas de la organización. Cada colaborador debe conocer el papel que desempeña dentro de la entidad y dentro del SCI y la forma como las actividades a su cargo están relacionadas con el resto de la estructura organizacional y con los usuarios externos.

Los canales de comunicación, los responsables en el manejo de la información y de la comunicación, la frecuencia de la información y la comunicación, la identificación de los respectivos destinatarios y los controles al Sistema de información y comunicación son algunos de los requerimientos para una adecuada cultura organizacional de control y de relación con los clientes.

Herramienta

Coomeva tiene un compromiso de transparencia, eficiencia y rendición de cuentas con sus asociados y con el mercado, por ello ha establecido en su portal de Internet, un enlace sobre las funciones y el actuar del gobierno corporativo, en el que la información se encuentra clasificada así:

Información General: Aquella que es de uso general, no clasificada como reservada.

Información Reservada: Aquella que compete exclusivamente a los miembros del Consejo de Administración, al Gerente General Corporativo y a sus inmediatos colaboradores. En esta categoría están incluidas las comunicaciones que contemplan riesgo para la entidad o involucran estrategias de negociación o competitividad.
La información se revela de manera precisa y de modo regular, acerca de todas las cuestiones materiales referentes a la Cooperativa, con excepción de la información confidencial o de aquella que ponga en riesgo los negocios o los derechos de terceros.

Herramienta

La Entidad suministrará en su página Web información general, actualizada y elaborada siguiendo principios, criterios y prácticas profesionales así:

1. Revelación de información contable, financiera y operativa, con periodicidad mínima anual.

2. Informes de gestión, con periodicidad mínima trimestral.

3. Las decisiones de inversión, financiación, garantía o contratación a favor de empresas proveedoras de Coomeva o de sus subordinadas, incluyendo: justificación, objetivos, rendimiento esperado, valores en riesgo, y factores de incertidumbre.

Otras fuentes y modos de circulación de información son:

Cámara de Comercio: Dentro del mes siguiente a la fecha en la cual son aprobados por la Asamblea General de Delegados, se deposita copia de los estados financieros, junto con sus notas y el dictamen correspondiente, si fuera el caso, en la Cámara de Comercio del domicilio social.

Delegados y Dirigencia en general: A estas instancias se les suministra información contable, financiera y operativa con periodicidad mensual.

Método

En cumplimiento de la normatividad vigente, Coomeva realiza reportes de información a los entes de control estatal, con la periodicidad establecida en la reglamentación respectiva. Dicha información reposa en archivos públicos y puede accederse a ésta, salvo a la información que esté sometida a reserva, de manera personal o por vía electrónica, de acuerdo con los mecanismos establecidos por dicha autoridad.

Mensaje

Todas las personas vinculadas a Coomeva están obligadas a utilizar la información a la cual tengan acceso, en virtud de sus funciones, o relación contractual, exclusivamente para el ejercicio de las mismas, con plena observancia del procedimiento establecido para la revelación de información a terceros.

Herramienta

Coomeva cuenta además con un sistema de información electrónico, que los asociados y las demás personas interesadas en su actividad pueden consultar. Toda persona vinculada a la entidad deberá tener especial cautela en el manejo de la información catalogada como reservada, sobre todo aquellos asuntos que tengan relación con su ventaja competitiva, su estrategia corporativa, su competencia, precios y campañas.

5) Monitoreo

Proceso que se lleva a cabo para verificar la calidad de desempeño del *Sistema de control interno*. El monitoreo se efectúa por medio de la supervisión continua que realizan los jefes o líderes de cada área o proceso, como parte constitutiva de su responsabilidad, dentro del ámbito de competencia de cada uno.

Del mismo modo, este proceso de supervisión recae también sobre el Área de Auditoría interna, el Comité de Auditoría Corporativa y sobre la alta dirección de la organización. El SCI no es un sistema estático, es un ente dinámico que se debe ajustar, de forma permanente, a las nuevas situaciones del entorno; de ahí la necesidad del monitoreo continuo y la toma de correctivos.

Herramienta

Implantar controles automáticos y alarmas tanto en los sistemas automatizados como en los manuales que evalúen la calidad y el desempeño del sistema son los que permiten determinar las acciones de mejoramiento necesarias. El monitoreo debe, por tanto, poder hacerse en tiempo real en el curso de las operaciones.

Las evaluaciones permanentes y separadas permiten igualmente determinar si el control interno está presente y si funciona en forma adecuada en el tiempo. Así las deficiencias pueden ser identificadas y comunicadas de manera oportuna a las partes responsables para la toma de acciones correctivas.

6) Evaluaciones independientes

Los procedimientos de seguimiento permanente, así como la autoevaluación de cada área, proporcionan una retroalimentación importante. No obstante, es necesario realizar adicionalmente evaluaciones que se centren directamente sobre la efectividad del SCI, las cuales deben ser realizadas por personas totalmente independientes al proceso, como requisito indispensable para garantizar su imparcialidad y objetividad. Estas evaluaciones independientes las realizan los auditores internos y el revisor fiscal. La administración, si lo considera conveniente, puede como práctica de *buen gobierno corporativo* contratar auditores externos para revisar la efectividad del *Sistema de control interno*.

3. ÁREAS ESPECIALES DENTRO DEL SCI

El SCI debe abarcar todas las áreas de la organización, aplicando para cada una, según su carácter, los objetivos, principios, elementos y actividades de control, información y comunicación que les corresponda, dada su función.

No obstante, las áreas especiales sobre las cuales recae fundamentalmente el control en Coomeva son: el Área contable, el Área de Tecnología e informática, el Comité de Auditoría Corporativa y la Junta de Vigilancia.

1) Control interno a la gestión contable

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

Confiable se refiere a la manera como se cumplen plenamente normas, principios y reglamentos. Un eficiente SCI contable debe supervisar el que se genere información financiera oportuna, razonable y veraz. El diseño e implementación del *control interno* para la *gestión contable* es responsabilidad de la administración, así como la correcta preparación y presentación de los estados financieros y sus correspondientes notas.

Del mismo modo, los representantes legales serán los responsables de la implementación y mantenimiento de los controles adecuados sobre la información financiera, para lo cual deberán diseñar *procedimientos de control.*

Idea

Calidad, suficiencia y oportunidad en la información financiera y verificar la operatividad de los controles establecidos al interior de la organización, para poder tomar medidas correctivas y minimizar riesgos, hace parte de la necesaria evaluación del desempeño de los sistemas de revelación y control, por parte del Área contable de una organización y de los entes de control, tanto internos como externos.

Sobre el Representante Legal

El Representante Legal es también responsable 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 organización registrar, procesar, resumir y presentar adecuadamente la información financiera. A este rol le corresponde igualmente reportar los casos de fraude que hayan podido afectar la calidad de la información financiera, así como cambios en la metodología de evaluación de este tipo de información.

Ideas rectoras

Un apropiado *Sistema de control interno contable* garantiza que los estados financieros que se presentan a la Asamblea, a los entes de supervisión, fiscalización y control y, que son objeto de publicación, reflejen de forma fidedigna la realidad económica de una entidad. De este modo, deben ejecutarse procedimientos de verificación idóneos, que le permitan al Representante Legal contar con elementos de juicio suficientes que orienten y complementen el papel de la Revisoría Fiscal.

La evaluación del revisor fiscal debe realizarse así en el contexto del alcance de las funciones que le asigna la ley. Verificar que los referidos sistemas coadyuvan a que la administración garantice el adecuado cumplimiento de las normas vigentes y poner oportunamente en conocimiento del Representante Legal y del Comité de Auditoria y de la Auditoría Interna, según corresponda, las inconsistencias y fallas detectadas en cada uno de los Sistemas de Administración de Riesgos, es complemento de su actuar. En caso que sus observaciones o recomendaciones no sean adecuadamente atendidas por la administración o

cuando la gravedad de las deficiencias encontradas lo amerite, el revisor deberá informar sobre tales circunstancias a la Superintendencia.

Políticas y procedimientos contables

Las *actividades de control contable* implican dos componentes: una política contable, que establece lo que debe hacerse y unos procedimientos para llevarla a cabo. La administración debe tomar 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.

Idea

De ahí que resulte indispensable que las entidades implementen la ejecución de políticas contables a toda la organización, en todos los niveles y en todas las funciones que intervienen en este proceso contable.

Algunos de los procedimientos obligatorios para un adecuado *Sistema de control interno contable son:*

- Supervisión de los procesos contables.
- Evaluaciones y supervisión de los aplicativos, accesos a la información y archivos, utilizados en los procesos contables.
- Presentación de informes de seguimiento.
- Validaciones a la calidad de la información, revisando que las transacciones u operaciones sean veraces y estén adecuadamente calculadas y valoradas aplicando principios de medición y reconocimiento.
- Comparaciones, inventarios y análisis de los activos de la entidad, realizadas a través de fuentes internas y externas.

- Supervisión de los Sistemas de Información.
- Asumir controles generales.
- Autorización apropiada de las transacciones por los órganos de dirección y administración.
- Autorización y control de documentos
- Autorizaciones y establecimiento de límites

Controles sobre los Sistemas de información contable

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

En este sentido, las *actividades de control* a los Sistemas de información son:

- Controles generales

  Rigen para todas las aplicaciones de los sistemas de información y ayudan a asegurar su continuidad y operación adecuada. Dentro de éstos se incluyen aquellos que se hacen sobre la administración de las tecnología de información, su infraestructura, administración de seguridad y adquisición, desarrollo y mantenimiento de software.

- Controles de aplicación

  Se centran directamente en la suficiencia, exactitud, autorización y validez de la captura y procesamiento de los datos, aseguran que los datos que se capturan estén disponibles y que los errores de interface se detecten rápidamente.

Análisis de vulnerabilidades de la información

Las entidades deben implementar y monitorear un sistema de análisis de vulnerabilidades informáticas que cumpla, según la Superintendencia Financiera de Colombia, con los siguientes requisitos:

- Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática

- Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas.

- Las entidades deberán tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.

- Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

- Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilitis and Exposures) y actualizadas a la fecha de su utilización.

- Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org)

2) Normas de Control interno para la gestión de tecnología:

La tecnología es imprescindible para el cumplimiento de los objetivos y la prestación de los servicios de entidades que, según su naturaleza, deben velar porque las operaciones se den en condiciones de seguridad, calidad y efectividad.

Mensaje

El diseño del SCI para la *Gestión de tecnología* debe velar y responder a las políticas, necesidades y expectativas de la entidad, así como a las exigencias normativas.

Así el sistema debe ser objeto de evaluación y 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, por lo tanto, deben establecer, desarrollar, documentar y comunicar políticas de tecnología y definir los recursos, procesos, procedimientos, metodologías y controles necesarios.

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

- Diseño de un Plan estratégico de tecnología
- Dotar de una adecuada infraestructura tecnológica
- Cumplimiento de los requerimientos legales para derechos de autor, privacidad y comercio electrónico
- Procedimientos para la administración de la calidad y la seguridad de los sistemas
- Adquisición y mantenimiento de software de aplicación

- Instalación y acreditación de sistemas
- Establecer la administración de cambios, servicios internos, externos y a terceros, desempeño, capacidad y disponibilidad de la infraestructura tecnológica y los datos
- Educación y entrenamiento de usuarios
- Documentación
- Administración de riesgos operativos –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

Plan Estratégico de Tecnología

Las entidades deberán realizar un proceso de planeación estratégica de tecnología, cada cierto tiempo, con el propósito de lograr el cumplimiento de los objetivos de la organización a través de las posibilidades y oportunidades que brinda la tecnología en el mundo actual.

El plan estratégico de tecnología debe estar alineado con el plan estratégico institucional y en éste se debe contemplar:

- Análisis de cómo soporta la tecnología los objetivos de cada operación
- Evaluación de la tecnología actual y las posibilidades de otras aplicaciones
- Estudios de mercado y factibilidad de alternativas tecnológicas que respondan a las necesidades de la organización
- Planes operacionales estableciendo metas claras y concretas

Administración de la Calidad

Con el objeto de satisfacer las necesidades de clientes (internos y externos), debe llevarse a cabo la planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad de tecnología. La calidad y la tecnología se garantizan mediante:

- Programas para establecer una cultura de calidad de la tecnología en toda la entidad
- Planes concretos de calidad de la tecnología
- Nombramiento de responsables del aseguramiento de la calidad
- Prácticas de control de calidad
- Metodología para el ciclo de vida de desarrollo de los sistemas
- Metodología de prueba y documentación de los programas y sistemas
- Diseño de informes de aseguramiento de la calidad
- Capacitación de usuarios finales y del personal de aseguramiento de la calidad
- Desarrollo de una base de conocimiento de aseguramiento de la calidad

Recuerde

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

Administración de Cambios

Con el fin de minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, se deberá diseñar un sistema de administración de cambios

que permita el análisis, implementación y seguimiento de las transformaciones requeridas a través de la infraestructura de tecnología que posea la organización.

Un sistema de administración de cambios debe contemplar los siguientes aspectos:

- Identificación clara del cambio a realizar en la infraestructura
- Categorización, priorización y procedimientos de emergencia a llevar a cabo durante el cambio
- Evaluación del impacto que ocasiona el cambio en la infraestructura.
- Procedimiento de autorización de los cambios
- Procedimiento de administración de las versiones
- Políticas de distribución del software
- Obtención de herramientas automatizadas para realizar los cambios
- Procedimientos para la administración de la configuración
- Rediseño de los procesos del negocio que se vean impactados por el cambio en la infraestructura

Seguridad de los Sistemas

Con el objeto de salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, corresponde a las entidades establecer controles de acceso que aseguren que los sistemas, datos y programas están restringidos y deberán ser usados por personal autorizado, para lo cual se deberá contar con procedimientos y recursos como:

- Autorización, autenticación y control de acceso
- Identificación de usuarios y perfiles de autorización a la información y la tecnología
- Manejo de incidentes, información y seguimiento

- Prevención y detección de código malicioso, virus, entre otros
- Entrenamiento de usuarios
- Administración centralizada de la seguridad

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 tecnología.

Método

Establecer controles de entrada, procesamiento y salida para garantizar la autenticidad e integridad de los datos, verificar la exactitud, suficiencia y validez de éstos en las transacciones, generados por personas, por sistemas o entradas de interface y preservar la segregación de funciones son algunos de los procedimientos para la adecuada y eficiente *administración de los datos* en una organización.

Los procedimientos deberán incluir también controles de actualización adecuados y controles de actualización de archivos maestros. La validación, autenticación y edición de los datos se tienen que llevar a cabo tan cerca del punto de origen como sea posible, según formulaciones de la normatividad vigente.

Del mismo modo, 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 y garantizar que los datos marcados como eliminados no puedan ser recuperados por cualquier individuo interno o tercero, ajeno a la

entidad, establecen esa necesaria seguridad sobre la reserva bancaria de la información.

Definir e implementar procedimientos apropiados y prácticas para transacciones electrónicas que sean sensitivas y críticas para la organización, velando por su integridad y autenticidad y establecer controles para garantizar la integración y consistencia de las plataformas, hace parte de ese sustento riguroso de un sistema de información tecnológica que sabe administrar los datos eficientemente.

4. DOCUMENTOS QUE DEBEN SUSTENTAR UN SCI

La Superintendencia Financiera de Colombia podrá exigir a través de la supervisión in situ o extra situ, manuales, formatos, procedimientos y demás documentos e información que estime pertinente, en el ejercicio de sus atribuciones legales. Los documentos mínimos que, según la normatividad, sustentan un SCI son:

1. Planes y programas definidos por la entidad para el logro de sus objetivos, incluyendo las correspondientes acciones, responsables y cronogramas, lo cual comprende, entre otros, el plan estratégico de tecnología.

2. Código de Conducta o su equivalente y documento mediante el cual éste se adopte oficialmente.

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

4. Metodología y herramientas definidas por la organización para hacer la evaluación con respecto a la aplicación de los principios de autocontrol, autorregulación y autogestión, a nivel general, por áreas o procesos, según resulte pertinente.

5. Mapa de procesos y mapa de los riesgos relevantes, 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.

6. Política para manejo de riesgos definida por el Consejo de Administración y la metodología e instrumentos para la gestión de riesgos en la entidad, incluyendo la definición de los comités u órganos responsables.

7. 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.

8. Documento que soporte la comunicación a todos los funcionarios de la entidad del mapa de riesgos y de las políticas y metodologías implementadas.

9. 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.

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

11. Plan anual de auditoría interna.

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

13. 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.

14. En relación con el consumidor financiero deben establecerse:
    a. Políticas de servicio.
    b. Políticas de transparencia e integridad en las relaciones (información veraz y fiable acerca de productos y tarifas, y mecanismos y sistemas de atención seguros y eficientes).
    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.

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

16. Programas o planes de mejoramiento.

5. RESPONSABILIDADES DENTRO DEL SISTEMA DE CONTROL INTERNO (SCI)

1) Órganos internos

La organización de Coomeva se da en tres órdenes fundamentales: Nacional, Regional y Zonal y bajo esta estructuración funciona mediante sucursales, agencias y oficinas. La Asamblea General de Delegados es el máximo órgano de autoridad y administración de la Cooperativa y sus decisiones son de obligatorio cumplimiento. La Asamblea examina los informes de los órganos de administración y vigilancia.

Consejo de Administración

En este sentido y con el fin de ordenar y vigilar que los procedimientos de *control interno* se efectúen en todas y cada una de las actividades, el Consejo de administración, bajo las directrices de la Asamblea, opera en esta materia, a través del Comité de Auditoría Corporativo. Este ente tiene por objeto realizar la evaluación integral del *Sistema de control interno* (SCI) y planificar su funcionamiento y mejoramiento continuo.

El Consejo de Administración es un órgano permanente de administración de Coomeva; está subordinado a las directrices y políticas de la Asamblea General y es responsable ante los asociados por el buen funcionamiento de la entidad.

Por ser los principales gestores del gobierno corporativo, el Consejo de Administración debe realizar su gestión con profesionalismo, integridad, competencia e independencia, dedicando el tiempo necesario.

Definir y aprobar las estrategias y políticas generales relacionadas con el SCI, basado en las recomendaciones del Comité de Auditoría Corporativa y la Revisoría Fiscal, le permitirán evaluar con profundidad los riesgos relacionados con los instrumentos de inversión y apoyar la labor de los órganos de fiscalización y control.

Ser transparentes en su gestión, procurando tener un buen conocimiento de los riesgos que involucran los servicios y productos que ofrece la organización, son la garantía necesaria para el correcto funcionamiento financiero y social de una organización.

Del mismo modo, conocer los informes relevantes respecto a la efectividad del SCI que sean presentados por los diferentes órganos de control o supervisión e impartir las órdenes necesarias para que se adopten recomendaciones y correctivos y planear el redireccionamiento estratégico, que pueda exigir la organización, son también funciones del Consejo, quien en Coomeva delega la gestión administrativa y operativa en el Gerente General Corporativo.

Método

Efectuar seguimiento a través de informes periódicos que presente el Comité de Auditoría Corporativa, sobre la gestión de riesgos en la entidad y las medidas adoptadas para el control o mitigación de éstos, por lo menos cada seis (6) meses, o con una frecuencia mayor si resulta procedente, permitirá que la organización y este organismo de administración y control cumplan su rol ante los Asociados y la Asamblea General.

Comité de Auditoría Corporativa

Documento de Coomeva

COOMEVA – Consejo de Administración. Acuerdo No. 343 (AC-AI-ET-2009.343). Cali, 11 de septiembre de 2009.

Este ente de Control, el "Comité de Auditoría Corporativa" en Coomeva se encuentra conformado por siete (7) miembros. Tres (3) miembros son del Consejo de Administración, un (1) miembro de la Junta de Vigilancia y tres (3) miembros son independientes y no podrán ser colaboradores, directivos, consultores o dirigentes de organizaciones con las cuales la cooperativa tenga relación. La designación es por un período de tres (3) años pero el Consejo de Administración podrá realizar cambios en la conformación cuando lo considere pertinente.

El Auditor Corporativo y el Revisor Fiscal asistirán a las reuniones a las cuales podrá ser citado cualquier funcionario de la organización. El Gerente General Corporativo y el Gerente Financiero Corporativo podrán asistir también a las reuniones mencionadas pero sin voz ni voto.

El objeto del Comité de Auditoria Corporativa es brindar apoyo al Consejo de Administración para realizar la permanente evaluación integral del *Sistema de Control Interno*, vigilar el cumplimiento de leyes y regulaciones sobre control, gestión de riesgos y auditoría y velar por la gestión operativa, la transparencia y la exactitud de la información financiera.

Otras funciones de este Comité son:

- ✓ Aprobar y ajustar la estructura, procedimientos y metodologías para el adecuado funcionamiento del SCI, señalar responsabilidades a cargos y áreas respecto a la administración del SCI y la gestión de riegos. Del mismo modo, evaluar y establecer si los procedimientos para el *control interno* son los necesarios y si se protegen los activos de la entidad y las transacciones se autorizan y registran de manera conveniente.

- ✓ La administración, los diferentes cargos y áreas deberán suministrar la información requerida por los órganos de control y el Comité de Auditoría Corporativa deberá velar e implementar programas, en este sentido, para prevenir y detectar errores, fraude o mala conducta en la operación.

- ✓ La información financiera deberá ajustarse a las normas legales y el Comité de Auditoría Corporativa tendrá, por lo tanto, que estudiar los Estados financieros teniendo en cuenta los dictámenes y observaciones de los entes de control tanto internos como externos.

- ✓ Supervisar las funciones y actividades de auditoría interna y verificar que se cumple con las necesidades de control de la entidad y hacer el seguimiento a los niveles de riesgo y sus implicaciones, es otra función del Comité, que deberá hacerse mínimo cada tres meses. También se debe analizar el funcionamiento de los sistemas de información, su confiabilidad e integridad y estudiar y presentar los candidatos a la Revisoría Fiscal, al Consejo de Administración.

- ✓ Las políticas para la implementación, ajuste, mejoramiento del SCI y la gestión de riegos y auditoría son responsabilidad del Comité de Auditoría Corporativa que deberá rendir informe en materia de *control interno* al

Consejo de Administración y éste, a su vez, a la Asamblea. Evaluar la independencia de la auditoria externa y la efectividad de sus procesos cuando corresponda posibilita que la evaluación y el monitoreo puedan ser garantizados.

Mensaje

Las deficiencias materiales detectadas, las recomendaciones y medidas adoptadas, las observaciones formuladas por los órganos de supervisión y vigilancia y las sanciones impuestas que, pudieran afectar el funcionamiento de la entidad, los Estados financieros y/o los indicadores de gestión, deberán ser presentados por el Comité de Auditoría Corporativa al Consejo de Administración y al Representante Legal.

Servir de apoyo a la Superintendencia de la Economía Solidaria y a la Revisoría Fiscal, evaluando constantemente los procedimientos establecidos y confirmar o reprobar el concepto de la Revisoría Fiscal frente al informe de suficiencia y adecuación de las medidas de Control Interno de la entidad, que se deben presentar a la Asamblea, son del mismo modo, objeto de su labor. El Comité de Auditoria Corporativo sólo hará recomendaciones al Consejo de Administración y no tomará decisiones por su propia cuenta.

Representante Legal

El Gerente General Corporativo es el representante legal de Coomeva, el ejecutor del Plan de Desarrollo y de las decisiones del Consejo de Administración y es el superior jerárquico y coordinador del personal administrativo.

Elegido por el Consejo de Administración, el Gerente General Corporativo debe velar por que los bienes y valores de la entidad estén adecuadamente protegidos, y porque la contabilidad se encuentre al día, conforme con las disposiciones legales y estatutarias.

Coordinar, orientar y dirigir las Empresas donde Coomeva tiene participación, de tal forma que se garantice la unidad de propósitos, dirección y control y garantizar que los asociados reciban información oportuna sobre los servicios y beneficios son también otras de sus funciones.

Concepto

Implementar estrategias y políticas aprobadas por el Consejo de Administración en relación con el SCI, comunicar las políticas y decisiones adoptadas en materia de *control interno*, *gestión de riesgos y auditoría*, poner en funcionamiento la estructura, procedimientos y metodologías inherentes al *control interno*, garantizando una adecuada segregación de funciones y asignación de responsabilidades e implementar los diferentes informes, protocolos de comunicación, sistemas de información y demás determinaciones de los entes de control, tanto internos como externos, permitirá blindar la organización de todos aquellos errores y riegos de operación.

En materia de control interno el Representante Legal es la instancia también responsable de:

Definir políticas y un programa antifraude, para mitigar los riesgos y crear y promover una 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 el establecimiento y aprobación de canales de comunicación, a todos los niveles, posibilitará que el

personal comprenda la importancia del control interno, las responsabilidades dentro del sistema y el necesario y permanente monitoreo.

Es igualmente importante que el representante Legal proporcione los recursos que se requieran para el adecuado funcionamiento del SCI, de conformidad con lo autorizado por el Consejo de Administración, y que pueda establecer mecanismos para la recepción de denuncias que faciliten, a quienes detecten eventuales irregularidades, ponerlas en conocimiento de los órganos competentes.

Su informe de gestión deberá en un aparte independiente evaluar el desempeño del SCI que incluya las entidades subordinadas (filiales, sucursales, otras zonas regionales y oficinas).

Método

El Representante Legal es el responsable de dirigir la implementación de los procedimientos de control y revelación, verificar su operatividad al interior de la entidad y su adecuado funcionamiento, para lo cual debe demostrar la ejecución de los controles que corresponden; de tal forma que deberá dejar constancia documental de sus actuaciones mediante memorandos, cartas, actas de reuniones y mediante los documentos que resulten pertinentes para el efecto.

Auditoría interna

Actividad que se fundamenta en criterios de independencia y objetividad para el aseguramiento y consulta de información que agregue valor y mejore 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.

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 labor con el cuidado y la pericia que se espera de un especialista prudente y competente.

Método

Para desarrollar, mantener y asegurar la calidad y mejora, la Auditoría Interna debe cubrir todos los aspectos de la actividad y de la calidad de una organización y deberá continuamente revisar su eficacia. El programa de calidad incluye evaluaciones de calidad externas e internas periódicas y supervisión interna continua.

En este sentido, cada parte del programa debe estar diseñada para añadir valor y mejorar las operaciones que aseguren que la Auditoría Interna cumple con las normas aplicables a esta actividad y al Código de Ética de los auditores. Cuando el incumplimiento afecte el alcance general o el funcionamiento de la actividad de Auditoría Interna debe declararse esta situación al Consejo de administración.

Para cumplir con su actuar la Auditoría Interna debe realizar las siguientes actividades de control:

Planificación. Debe establecer 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.

Comunicación y aprobación. Comunicar los planes y requerimientos de recursos de la actividad de auditoría interna, incluyendo los cambios provisorios significativos al Comité de Auditoría Corporativa y al Representante Legal, para la adecuada revisión y aprobación. El Auditor Interno también debe comunicar cualquier limitación de recursos.

Administración de recursos. Determinar los recursos que la auditoría interna necesita para el adecuado ejercicio de su labor y solicitarlos al Consejo de Administración y/o al Comité de Auditoría Corporativa.

Políticas, procedimientos y coordinación. Establecer políticas y procedimientos para guiar la actividad de auditoría. Igualmente, debe compartir información y coordinar actividades con los otros órganos de control para lograr una cobertura adecuada y minimizar la duplicación de esfuerzos.

Informes y seguimiento. Los informes emitidos deben ser precisos, objetivos, claros, constructivos, completos y oportunos y deberán estar debidamente soportados en evidencias suficientes. Realizar seguimiento a las acciones tomadas por la administración frente a estas comunicaciones es también una actividad vital de control de esta área de la organización.

2) Órganos externos

Revisoría Fiscal

El control fiscal y contable de Coomeva se encuentra a cargo de un Revisor Fiscal, con su respectivo suplente, elegidos por la Asamblea General para un período de tres (3) años, pudiendo ser reelegido para ejercer como máximo hasta un período adicional de manera consecutiva.

La Asamblea podrá en cualquier momento remover la Revisoría Fiscal, caso en el cual el período del nuevo revisor y su suplente, se extenderá hasta completar el período para el que habían sido elegidos los removidos.

La firma designada para la revisoría fiscal que fuere elegida para dicho cargo deberá asignar personas naturales diferentes para cada una de las empresas y no podrán ser Revisores Fiscales los asociados, los socios de las empresas ligadas a la entidad ni los colaboradores.

El control ejercido por la Revisoría Fiscal, tiene como objetivo principal, además de lo que establece la ley, velar por que el patrimonio de la Cooperativa esté debidamente protegido, conservado y utilizado, que los actos administrativos se ajusten al objeto social y a las normas legales, estatutarias y reglamentarias y que los registros contables de todas las operaciones se ajusten a la realidad y se realicen de acuerdo con la normatividad vigente.

De esta forma, controlar que las operaciones que se celebren estén conforme a las disposiciones legales, las prescripciones de los Estatutos de Coomeva y las determinaciones de la Asamblea General, del Consejo de Administración y de la gerencia general, son labor de la Revisoría Fiscal.

Velar por que la contabilidad se lleve con exactitud y en forma actualizada y que los soportes y comprobantes se conserven adecuadamente y dar oportuna cuenta, por escrito, al Gerente General Corporativo, al Consejo de Administración, a la Junta de Vigilancia y a la Asamblea, según el caso, de las irregularidades contables de operación existentes en el funcionamiento, es la exigencia, al igual que impartir las instrucciones para practicar las inspecciones y solicitar los informes que sean necesarios para poder establecer un control permanente sobre el patrimonio de la organización.

Efectuar el examen financiero y económico de la Cooperativa, hacer los análisis de cuentas semestralmente y presentarlos, con sus recomendaciones, al Gerente General Corporativo y al Consejo de Administración y rendir a la Asamblea un informe pormenorizado de sus actividades, certificando lo presentado, garantizan que ante la ley y los beneficiarios se cumpla el objeto social. Es también importante que la Revisoría Fiscal inspeccione los bienes de la entidad y procure que se tomen, oportunamente, medidas de conservación y seguridad.

Mensaje

Colaborar con las entidades gubernamentales que ejerzan la inspección y vigilancia y rendir los informes a que haya lugar o le sean solicitados y cumplir con las demás funciones que señale la Ley, el Estatuto de Coomeva y las que, siendo compatibles con su cargo, le encomiende la Asamblea o Consejo de Administración son responsabilidades de la Revisoría Fiscal.

De este modo, el sistema de control en Coomeva está integrado por el control interno y el externo.

Otros órganos de control

Sin perjuicio del control externo que ejerce el Estado, Coomeva está sometida al control social interno de sus propios asociados, a través de la Junta de Vigilancia cuyo ámbito de acción es diferente al que le corresponde a la Auditoria Interna o a la Revisoría Fiscal.

El control interno empresarial recae también en la cooperativa sobre sus administradores y funcionarios. Control interno que se refiere al control de los resultados sociales y los procedimientos para el logro de dichos resultados, así como a los derechos y obligaciones de los asociados.

Junta de Vigilancia

La Junta de Vigilancia tiene a su cargo el control social. Dicho control es de naturaleza técnica e interna, es decir que se encuentra a cargo de los propios asociados de la Cooperativa y tiene como objetivo el control de los resultados sociales, los procedimientos para lograrlos y el cumplimiento de los derechos y obligaciones de los asociados.

La Junta es elegida en la Asamblea General por un periodo de tres años está conformada por tres miembros y sus respectivos suplentes y no podrá ser elegida por dos períodos consecutivos. Sus funciones podrán ser delegadas en los Comités de Vigilancia Regionales y Zonales pero dicha delegación se hará bajo su coordinación y sin perjuicio de las responsabilidades que le corresponde a sus miembros titulares.

Concepto

Es labor de la Junta de Vigilancia velar por que los actos de los órganos de administración se ajusten a las prescripciones legales, estatutarias, reglamentarias y a los principios cooperativos. La Junta deberá informar a los órganos de administración, al Revisor Fiscal o a las Superintendencias correspondientes las irregularidades que existan en el funcionamiento de la Cooperativa y presentar recomendaciones sobre las medidas que deben adoptarse.

Certificar la habilidad y cumplimiento de los requisitos estatutarios para ser delegado o ser elegido o nombrado en cargos de dirección o de responsabilidad y conocer, evaluar y resolver íntegramente las quejas que los asociados y usuarios presenten, acerca de posibles incumplimientos de normas legales o internas, que rigen el desarrollo de las operaciones, contratos o servicios que ofrece, presta, o ejecuta la Cooperativa, son también funciones vitales de la Junta de Vigilancia, quien también deberá velar por la calidad en la prestación de los servicios. De este modo, este organismo solicitará los correctivos del caso, por el conducto regular y con la debida oportunidad.

Todas las decisiones de la Junta de Vigilancia deberán adoptarse como cuerpo colegiado, en reuniones debidamente citadas y sus decisiones deberán motivarse y constar por escrito.

Comité de Ética

Es el encargado de velar por el mantenimiento y respeto del conjunto de normas, principios y razones que Coomeva ha establecido como línea directriz para el

desarrollo de su objeto social y que están plasmadas en los Estatutos, el Código de Ética y en el Código de Buen Gobierno.

El Comité de Ética está integrado por tres asociados, con sus respectivos suplentes y certifican su alta calidad moral, profesional e intelectual. De reconocida reputación y hoja de vida intachable los elegidos serán designados para un período de tres (3) años por la Asamblea General, de ternas que presenten los Comités Administrativos Regionales. Sus miembros podrán ser reelegidos hasta por dos (2) períodos consecutivos.

No podrán ser integrantes del Comité de Ética asociados que sean delegados, colaboradores, asesores, corredores o que tengan vínculos comerciales con la Cooperativa o con alguna de las empresas que conforman su grupo empresarial. Tampoco podrán ser integrantes del Comité quienes hayan sido delegados o pertenecido al Consejo de Administración, a la Junta de Vigilancia o a la Comisión Central de Elecciones e Escrutinios, en el año inmediatamente anterior a la respectiva elección.

Velar por la aplicación de las disposiciones del Código de Ética y ejercer el control ético y de conflictos de interés, proponer las modificaciones, ajustes, desarrollos y precisiones al Código y recomendar e informar a la Junta de Vigilancia toda situación, hecho o conducta que deba ser objeto de investigación y de imposición de sanción, son funciones del Comité de Ética.

Abstenerse de usar indebidamente la información reservada y combatir, denunciar y rechazar cualquier acción o actividad al margen de la Ley son responsabilidades acordes con los principios incorporados en las normas de comportamiento ético de Coomeva.

Recuerde

El Grupo Empresarial Coomeva reafirma así su compromiso de desplegar todas las acciones que estén a su alcance para evitar que los servicios financieros que ofrece a los asociados y terceros, se utilicen como medio para ocultar en cualquier forma, dinero o bienes que provengan de actividades ilícitas. (Art. 5. Código de Ética. Marzo de 1998).

Superintendencia de la Economía Solidaria

Coomeva se encuentra sometida a la inspección, vigilancia y control de la Superintendencia de la Economía Solidaria, organismo de carácter técnico, adscrito al Ministerio de Hacienda y Crédito Público.

El desarrollo del objeto social de la Cooperativa, se enmarca dentro de las prescripciones de las Circulares Básica Jurídica y Básica Contable y Financiera expedidas por el citado ente de control, las cuales desglosan la normatividad propia de las entidades cooperativas.

Además de la supervisión de la Superintendencia de la Economía Solidaria, Coomeva es objeto de control por parte de la Superintendencia Financiera de Colombia.

Superintendencia Financiera de Colombia

Con respecto a las transacciones en el Mercado Público de Valores Coomeva cuenta con la debida autorización e inscripción otorgada por esta entidad estatal de control. De igual forma, se encuentra inscrita ante el Depósito Centralizado de Valores, DECEVAL, en calidad de depositante directo.

Auditorías especializadas

Cuando luego de rendidos los informes respectivos y adelantadas las investigaciones, por parte de los entes pertinentes de control de la Cooperativa, un número de Delegados que representen por lo menos la cuarta parte del total de delegados hábiles, o un número de asociados que representen el uno por ciento (1.0%) del total de asociados hábiles, consideren que persisten dudas sobre determinadas actuaciones que hubieren sido objeto de dichos informes e investigaciones, podrán solicitar a la Gerencia General, la realización de auditorias especializadas.

Idea

La solicitud para realizar auditorias especializadas deberá ser presentada por escrito, indicando las razones que las motivan, los hechos y las operaciones a auditar. Los solicitantes en su petición, deberán designar un representante, con quien se surtirá todo el trámite.

En el término de quince (15) días hábiles siguientes a la fecha de recepción de la solicitud, el Gerente General Corporativo deberá dar respuesta a la solicitud de auditoría especializada, indicando la firma seleccionada, fecha de iniciación y duración estimada.

Los resultados de la auditoría especializada deberán darse conocer al Revisor Fiscal, al Consejo de Administración y al Gerente General Corporativo, quienes disponen de diez (10) días hábiles para pronunciarse, indicando las acciones correctivas y preventivas a desarrollar dentro de un plan específico. En caso de existir la posibilidad de transgresiones a las normas legales, se dará traslado a las entidades judiciales e investigadoras correspondientes.

Consultorías

Son actividades de asesoramiento y servicios relacionados con algún aspecto de la entidad, cuya naturaleza y alcance añade valor y permite mejorar los procesos de gobierno, gestión de riesgos y control en una organización, sin que el auditor interno asuma responsabilidades de gestión.

Recuerde

El Sistema de Control Interno Empresarial de Coomeva es un sistema integrado por un esquema de organización y un conjunto de planes, métodos, principios, normas, procedimientos y mecanismos de verificación, adoptados para procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con normas constitucionales, legales, normativas, estatutarias, políticas de la alta dirección, metas y objetivos previstos.

Recuerde

Este *control interno* debe garantizar:

- Efectividad y eficiencia de las operaciones y cumplimiento de los objetivos básicos de la Cooperativa, salvaguardando sus recursos y los de terceros, en los cuales Coomeva tenga participación.
- Suficiencia y confiabilidad de la información financiera y evaluación, gestión y seguimiento de los riegos
- Cumplimiento de la regulación aplicable: leyes, estatutos, reglamentos e instrucciones internas.

Recuerde

A la Auditoría Interna le corresponde adoptar medidas preventivas, de vigilancia, seguridad, evaluación y seguimiento para garantizar el óptimo aprovechamiento de los recursos. Ejercer buenas prácticas corporativas y velar por el cumplimiento de las normas legales, las disposiciones estatutarias y los compromisos asumidos por Coomeva, son también algunas de sus funciones. Este organismo debe además:

1. Prestar asistencia a las diferentes áreas en la identificación y documentación de las matrices normativas y principios éticos aplicables en sus respectivas actividades.
2. Crear, promover y mantener una cultura de cumplimiento permanente, arraigada entre el personal y en todos los niveles tanto internos como externos.
3. Evaluar, revisar y garantizar el *cumplimiento* de las políticas y lineamientos elaborados por el Consejo de Administración.
4. Revisar las conductas de cumplimiento interno y velar por su aplicación.
5. Reportar a la Gerencia General cualquier situación de riesgo que pueda afectar el patrimonio, activos o buen nombre de la Cooperativa, los colaboradores o los asociados

Recuerde

La doble naturaleza, asociativa y empresarial de Coomeva, permite diferenciar los órganos de control que la rigen. La acción de la Revisoría Fiscal, el Comité de Auditoría Corporativa y las auditorías internas, están relacionadas fundamentalmente con las operaciones propias de la actividad empresarial. La acción del órgano de control social interno está relacionada con la asociación y, por tanto, el control social lo ejerce la Junta de Vigilancia.