

CIRCULAR BASICA CONTABLE Y FINANCIERA

CAPITULO IV SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO – SARO

1. CONSIDERACIONES GENERALES

Este capítulo contiene las reglas y parámetros mínimos a seguir para gestionar el Sistema de Administración del Riesgo Operativo -SARO- que deben implementar las organizaciones solidarias vigiladas, que les permita identificar, medir, controlar y monitorear eficazmente el riesgo operativo al cual se exponen.

Dicho sistema deberá permitir a las organizaciones la adopción de decisiones oportunas para la adecuada mitigación de eventos que genera el riesgo operativo.

El Consejo de Administración y la Alta Gerencia deberán implementar las reglas y parámetros para gestionar su SARO atendiendo las características de la organización solidaria, tales como su tamaño, el tipo de productos y servicios ofrecidos, y el volumen y la complejidad de sus operaciones.

El SARO que adopten las organizaciones está sujeto a la supervisión permanente e integral de la Superintendencia de esta Economía, en los términos previstos en el presente capítulo.

2. AMBITO DE APLICACIÓN

Las instrucciones y procedimientos mínimos contenidos en el presente capítulo, para implementar un Sistema de Administración del Riesgo Operativo (SARO), deben ser aplicadas por las cooperativas de ahorro y crédito, multiactivas e integrales con sección de ahorro y crédito vigiladas.

La Superintendencia podrá extender la obligación de aplicar lo dispuesto en este capítulo a otras organizaciones solidarias vigiladas en razón a su tamaño, actividades desarrolladas e impacto en el sector solidario.

Aquellas organizaciones solidarias que proactivamente deseen adoptar principios o modelos contenidos en otras normas lo pueden realizar siempre y cuando se asegure el cumplimiento de lo dispuesto en el presente capítulo.

3. DEFINICIONES

Las siguientes definiciones se tendrán en cuenta para los fines del presente capítulo y del **Anexo 1**.

3.1. RIESGO OPERATIVO

CIRCULAR BASICA CONTABLE Y FINANCIERA

En el contexto del SARO, se entenderá por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas, ausencias o inadecuaciones en:

- a. los procesos,
- b. el recurso humano,
- c. la tecnología,
- d. la infraestructura física; o
- e. por la ocurrencia de acontecimientos externos.

El Riesgo Operativo está asociado al riesgo legal y al riesgo reputacional.

3.2. RIESGO LEGAL

Es la posibilidad de pérdida en que incurre una organización solidaria al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones, obligaciones contractuales, fallas en los contratos y transacciones.

El riesgo legal surge también como consecuencia de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

3.3. RIESGO REPUTACIONAL

Es la posibilidad de pérdida en que incurre una organización por desprestigio, mala imagen, publicidad negativa, cierta o no relacionadas con sus prácticas de negocios, que puede causar el retiro de sus asociados, disminución de ingresos o el inicio de procesos judiciales.

3.4. EVENTO DEL RIESGO OPERATIVO

Los eventos de riesgo operativo son situaciones que generan impactos no deseados en las organizaciones solidarias asociados al riesgo operativo.

3.5. PÉRDIDAS

Es la cuantificación económica de la ocurrencia de un evento de riesgo operativo, así como los gastos derivados de su atención.

3.6. FACTORES DE RIESGO OPERATIVO

Se entiende por factores de riesgo las principales situaciones generadoras de riesgos operativos que pueden o no generar pérdidas. Son factores de riesgo: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Dichos factores se deben clasificar en internos o externos, según se indica a continuación.

3.6.1. Factores internos

CIRCULAR BASICA CONTABLE Y FINANCIERA

Se entiende por factores de riesgos internos, aquellas situaciones generadoras de eventos de riesgo operativo al interior de la organización solidaria relacionados con: el recurso humano, los procesos, la tecnología y la infraestructura física.

3.6.1.1. Recurso humano

Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la organización.

- a. Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente.
- b. La vinculación indirecta hace referencia a aquellas personas que tienen con la organización una relación jurídica de prestación de servicios, diferente a aquella que se origina en un contrato de trabajo.

3.6.1.2. Procesos

Es el conjunto de acciones o actividades sistemáticas y repetitivas por las que unas entradas (inputs) se convierten en un producto o servicio final (outputs).

3.6.1.3. Tecnología

Es el conjunto de herramientas empleadas para soportar los procesos de la organización solidaria, que incluye: hardware, software y telecomunicaciones.

3.6.1.4. Infraestructura Física

Es el conjunto de elementos de apoyo para el funcionamiento de una organización que incluye entre otros los siguientes: edificios, espacios de trabajo, almacenamiento y transporte.

3.6.2. Factores externos

Son situaciones asociadas a la fuerza de la naturaleza, u ocasionadas por proveedores o terceros, que escapan en cuanto a su causa y origen al control de la organización.

3.7. CLASIFICACIÓN DE LOS RIESGOS OPERATIVOS

Para los efectos del presente capítulo los riesgos operativos se clasifican de la siguiente manera:

3.7.1. Fraude Interno

Hace referencia a actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la organización, o incumplir normas o leyes, en los que está

CIRCULAR BASICA CONTABLE Y FINANCIERA

implicado, al menos, un empleado, tercero contratado o administrador de la organización.

3.7.2. Fraude Externo

Corresponde a actos realizados por un externo a la organización, que busca defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

3.7.3. Relaciones laborales incompatibles

Hace referencia a actos que son incompatibles con la legislación laboral y con los acuerdos internos de trabajo.

3.7.4. Asociados o clientes

Se relaciona con fallas negligentes o involuntarias de las obligaciones de la organización frente a los asociados o clientes, que impiden cumplir una obligación contraída con estos, o fallas de la naturaleza o diseño de un producto o servicio.

3.7.5. Daños a activos físicos

Hace referencia a pérdidas derivadas de daños o perjuicios a activos físicos de la organización.

3.7.6. Fallas tecnológicas

Se relaciona con pérdidas derivadas de incidentes por fallas tecnológicas.

3.7.7. Ejecución y administración de procesos

Tiene que ver con las pérdidas derivadas de errores en la ejecución y administración de los procesos.

3.8. CADENA DE VALOR DE UNA ORGANIZACIÓN SOLIDARIA

La cadena de valor es un concepto que hace referencia al conjunto de procesos encadenados que estratégicamente son fundamentales para entender y gestionar las ventajas competitivas de una organización solidaria. Se dividen en tres conjuntos de procesos: estratégicos, misionales, y de apoyo y control.

3.8.1. Procesos estratégicos

Son los que permiten definir y desplegar las estrategias y objetivos de la organización. Es decir, aquellos procesos que definen el direccionamiento del “negocio” de la organización; como, por ejemplo: marketing estratégico y estudios de mercado, planificación y seguimiento de objetivos, revisión del sistema, evaluación de la satisfacción de los asociados, etc.

CIRCULAR BASICA CONTABLE Y FINANCIERA

3.8.2. Procesos misionales

Son aquellos procesos que añaden valor al asociado o inciden directamente en su satisfacción o insatisfacción. Son procesos claves que intervienen en la misión de la organización y en el cumplimiento del objeto social.

3.8.3. Procesos de apoyo y control

Los procesos de apoyo son los que suministran los recursos necesarios para el buen desempeño de las operaciones del negocio, como son: financieros, humanos, tecnológicos, jurídicos, físicos e intangibles, entre otros y en los procesos de control se tiene la gestión de riesgos, control interno, etc.

3.9. SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO - SARO

Corresponde al conjunto de etapas y elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las organizaciones solidarias vigiladas identifican, miden, controlan y monitorean el riesgo operativo.

3.10. RIESGO INHERENTE

Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

3.11. RIESGO RESIDUAL

Nivel resultante del riesgo después de aplicar los controles al riesgo inherente.

3.12. PLAN DE CONTINUIDAD DEL NEGOCIO

Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

3.13. PLAN DE CONTINGENCIA

Es el conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

4. ETAPAS DE LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Es deber de las organizaciones revisar periódicamente las etapas y elementos del SARO a fin de realizar los ajustes que consideren necesarios para su efectivo, eficiente y oportuno funcionamiento, de forma tal que atiendan en todo momento las condiciones particulares de la organización y las del sector en general.

CIRCULAR BASICA CONTABLE Y FINANCIERA

En la administración del riesgo operativo se deben desarrollar las siguientes etapas: identificación, medición, control y monitoreo.

4.1. IDENTIFICACIÓN

En desarrollo del SARO se deben identificar los riesgos operativos y las causas a que se ven expuestas, teniendo en cuenta los factores de riesgo definidos en el presente capítulo, como etapa base para la gestión de este riesgo.

Por ello, la administración debe darle a esta etapa la importancia, tiempo y recursos que sean necesarios.

La etapa de identificación debe realizarse de manera previa a la implementación o modificación de cualquier proceso, así como en los casos de fusión, incorporación, cesión de activos y pasivos, entre otros.

Para identificar los riesgos operativos y sus causas, la organización solidaria debe, como mínimo, tener en cuenta los siguientes aspectos:

4.1.1. Identificar y documentar la totalidad de los procesos.

La organización debe mantener actualizado el manual de los procesos definidos en su cadena de valor: estratégicos, misionales, y de apoyo y control.

Para asegurar la adecuada actualización de cada uno de los procesos se debe tener en cuenta como mínimo lo siguiente:

- a. La responsabilidad de la actualización debe estar en cabeza del líder o gestor del proceso.
- b. Que participen funcionarios expertos y/o claves para el proceso, o si la organización los considera pertinente, se podrá apoyar con personal externo.
- c. Que el área de auditoría, control interno, o quién haga sus veces, realice pruebas de auditoría sobre el cumplimiento o no del manual del proceso.

4.1.2. Establecer una metodología para identificar el riesgo operativo

Se debe establecer una metodología formal para identificar los riesgos operativos y sus causas, que se puedan materializar en los procesos definidos en su cadena de valor.

Para tal efecto, la organización solidaria podrá considerar los siguientes aspectos:

4.1.2.1. Designar un grupo de funcionarios para el proceso

De acuerdo con el tamaño de la organización, su estructura y características particulares conformar un equipo de trabajo del cual hagan parte como mínimo el líder o gestor de proceso, el responsable de riesgos y demás personas que por su conocimiento y

CIRCULAR BASICA CONTABLE Y FINANCIERA

experiencia puedan aportar en esta etapa.

4.1.2.2. Actividades previas a las reuniones de trabajo

El responsable del área de riesgo o quien haga sus veces, debe coordinar la consecución, análisis y resumen de toda la información que sea útil al grupo de trabajo para identificar los riesgos operativos de cada proceso, tales como:

- a. Un resumen del proceso, que contenga la descripción de: las entradas (inputs) y sus proveedores, procedimientos principales, descripción de las salidas (outputs) y sus clientes internos y/o externos.
- b. Un resumen de los eventos de riesgo operativo que se hayan documentado en la organización o en el sector.
- c. La matriz de riesgo operativo del proceso, en el caso que la organización solidaria ya cuenta con ella.
- d. Informes de entes de control, internos o externos, relacionados con fallas o debilidades evidenciadas en el proceso en cuestión, o informes derivados de las peticiones, quejas y reclamos recibidos.
- e. Cualquier otro tipo de información que se considere relevante.

4.1.3. Definir la matriz consolidada de riesgo operativo

Para los procesos de la cadena de valor, se debe establecer una matriz consolidada de riesgo operativo. El procedimiento para realizar este trabajo será el que defina la organización; en todo caso, el procedimiento deberá tratar como mínimo lo siguiente:

- a. Las actividades a desarrollar para actualizar (si ya existe) o definir la matriz de riesgo operativo de cada uno de los procesos de la cadena de valor.
- b. Documentar la forma cómo se definieron los riesgos operativos del proceso. Lo anterior por medio de acta(s) o resumen(es) escrito(s) y validado(s) o firmado(s) por el líder o gestor del proceso y el funcionario responsable de riesgos o quien haga sus veces.
- c. Las matrices de riesgo operativo identificadas de cada uno de los procesos, se deben consolidar en una sola matriz.
- d. La validación de la matriz de riesgo consolidada por parte del área o funcionario responsable.
- e. Una vez consolidada la matriz de riesgos deberán generar el perfil de riesgo inherente y residual.

CIRCULAR BASICA CONTABLE Y FINANCIERA

La matriz de riesgo operativo consolidada de la organización solidaria debe contener, como mínimo, la información que se define a continuación:

4.1.3.1. Referencia del riesgo operativo

Se debe codificar cada uno de los riesgos operativos identificados según el proceso al que pertenece.

4.1.3.2. Nombre del riesgo operativo

Se debe dar un nombre “preciso” al riesgo operativo. De acuerdo con la definición de riesgo operativo, dada en el numeral 3.1 del presente capítulo, se debe especificar la deficiencia, falla o inadecuación de un factor de riesgo de entradas y/o procedimientos del proceso que lleve a no cumplir con la calidad, cantidad o tiempo de entrega de una de las salidas (outputs) definidas.

4.1.3.3. Descripción del riesgo operativo

Se debe describir, lo más completo posible, la forma en que se considera podría presentarse un evento derivado del riesgo operativo.

Como ejemplos de estos eventos se pueden citar normas o políticas que se puedan incumplir, o cualquier otra información que contribuya a especificar la importancia del riesgo operativo para el(los) proceso(s) de la organización solidaria.

4.1.3.4. Causas del riesgo operativo

Se deben establecer cuáles son las causas que incrementan la posibilidad de ocurrencia del riesgo operativo y que impliquen la implementación de controles con el fin de disminuir su probabilidad de ocurrencia.

Con el propósito de identificar las causas principales de un riesgo operativo, los integrantes del grupo de expertos deben orientar el análisis especialmente sobre las causas que lo originan al interior o al exterior de la organización y que pueden controlarse. Por ello, es esencial realizar una descripción completa de la causa.

La causa identificada debe tener asociado e implementado su(s) control(es) de mitigación.

4.1.3.5. Consecuencias de riesgo operativo

Para cada riesgo operativo identificado, se debe establecer las principales consecuencias, en que puede verse inmersa la organización solidaria si llega a materializarse el riesgo en cuestión.

Los efectos de la materialización de un riesgo operativo suelen estar asociados, en su gran mayoría, en el corto plazo, con pérdidas económicas e impacto en la imagen o riesgo

CIRCULAR BASICA CONTABLE Y FINANCIERA

reputacional. También existen consecuencias de otro tipo, como pérdida de mercado, pérdida de activos físicos, pérdida de información (de acuerdo con los lineamientos presentados en el numeral 4.3.4 del presente capítulo), reprocesos, demandas legales, glosas o multas, entre otras, que en el mediano o largo plazo también pueden causar pérdidas económicas.

La organización solidaria, debe implementar controles a los posibles impactos, los cuales deben ser eficientes y eficaces.

4.1.3.6. Clasificación

La organización solidaria debe clasificar cada riesgo operativo por factor de riesgo, atendiendo los niveles de clasificación definidos en el **Anexo 1** del presente capítulo.

4.1.3.7. Procesos

La organización debe listar los procesos en los cuales el riesgo operativo se puede materializar.

4.1.3.8. Productos o servicios

Se requiere listar los productos o servicios de la organización solidaria que se pueden ver afectados directamente si se materializa el riesgo. Esta columna puede estar vacía, en razón a que no todo riesgo operativo tiene que estar asociado directamente a un producto o servicio.

4.2. MEDICIÓN

Una vez concluida la etapa de identificación, se debe medir la probabilidad de ocurrencia de los riesgos operativos y su impacto en caso de materializarse. Esta medición podrá ser cualitativa y, cuando se cuente con datos históricos, cuantitativa. Para la determinación de la probabilidad se debe considerar un horizonte de tiempo de un año.

La metodología de medición o valoración propuesta para los riesgos operativos, permite determinar:

- a. La probabilidad de ocurrencia, que se refiere a la probabilidad de que fuentes potenciales de riesgos lleguen realmente a manifestarse, y
- b. El impacto que pueda generar sobre la organización solidaria, la materialización del riesgo operativo analizado. Esta variable hace referencia a los efectos adversos sobre la organización, es decir, lo que ésta podría perder y/o lo que podría salir mal.

Para tal efecto se deben tener en cuenta las siguientes escalas para la medición del riesgo:

4.2.1. Nivel de calificación de la variable “Probabilidad de Ocurrencia”

CIRCULAR BASICA CONTABLE Y FINANCIERA

Nivel	Descriptor	Definición	Criterios (a definir por la Organización Solidaria)
1	Inusual	Puede ocurrir sólo en circunstancias excepcionales	
2	Improbable	Es difícil que ocurra	
3	Posible	Podría ocurrir en algún momento	
4	Probable	Probablemente ocurrirá en la mayoría de las circunstancias	
5	Casi Certeza	Se espera que ocurra en la mayoría de las circunstancias	

Las organizaciones deben definir en la columna “criterio”, el porcentaje de probabilidad de ocurrencia para cada uno de los cinco niveles establecidos, teniendo como referencia el número de veces que ejecuta la actividad en el año.

4.2.2. Nivel de calificación de la variable “Impacto”

Nivel	Descriptor	Definición	Criterios (a definir por la Organización Solidaria)
1	Bajo	No genera perjuicios	
2	Menor	Pocos perjuicios que se controlan, local e inmediatamente	
3	Moderado	Perjuicios que se controlan localmente y/o con asistencia externa y que pueden generar riesgos asociados	
4	Mayor	Perjuicios extensivos que generan pérdida en la capacidad de producción y que generan riesgos asociados importantes	
5	Catastrófico	Perjuicios que generan importantes problemas de funcionamiento, pérdidas financieras, legales y de reputación	

CIRCULAR BASICA CONTABLE Y FINANCIERA

La Organización Solidaria podrá complementar las definiciones para cada uno de los cinco niveles de calificación, para lo cual puede tomar información cualitativa (experta) o cuantitativa. A continuación, se presenta, a manera de ejemplo, una lista de variables o aspectos que se puede tomar como referencia para la definición de cada uno de los niveles:

- a. Tamaño (en valor o porcentaje) de pérdidas en relación con el presupuesto anual de ingresos.
- b. Incremento del riesgo reputacional, asociado a un aumento en el porcentaje de las quejas o reclamos.
- c. Incremento de riesgo legal asociado al tipo o cantidad de glosas o de sanciones del supervisor u otros entes de control.
- d. Nivel de pérdidas de información propia o de sus asociados.
- e. Porcentaje de pérdida del mercado objetivo, o asociados.
- f. Tiempo de interrupción o retraso en la operación.
- g. Tamaño del incremento del riesgo integral de la organización.
- h. Otras

Las organizaciones deberán calcular los rangos de pérdida económica para cada uno de los niveles de impacto en la columna “criterios” cuyos valores deberán ser expresados en salarios mínimos legales vigentes SMLV.

4.2.3. Medir el riesgo Inherente

El grupo de funcionarios, definido de acuerdo con lo establecido en el numeral 4.1.2.1. del presente capítulo, calificará la probabilidad de ocurrencia y el impacto inherente de cada uno de los riesgos operativos que fueron identificados en la etapa anterior.

4.3. CONTROL

La organización debe tomar medidas para controlar los riesgos operativos inherentes a los que se ve expuesta, con el fin de disminuir la probabilidad de ocurrencia y el impacto en caso de que se materialicen. Durante esta etapa, la organización solidaria debe, como mínimo, tener en cuenta los siguientes aspectos:

4.3.1. Identificar los controles que pueden mitigar el riesgo operativo

Para establecer el riesgo residual es necesario que la metodología reconozca los controles que se pueden llevar a cabo para mitigar el riesgo en cuestión. La mayor parte de los controles se establecen a partir del análisis de las actividades que conforman los procesos

CIRCULAR BASICA CONTABLE Y FINANCIERA

diseñados. Por lo tanto, es importante que el experto conozca los procesos.

Otros controles no necesariamente hacen parte de los procesos. Por ejemplo: auditorias, seguros, planes de contingencia, plan de continuidad, plan de emergencia, código de conducta y/o ética, entre otros.

4.3.1.1. Determinar de qué tipo de control se trata

Se debe clasificar el control identificado, para establecer si está mitigando la probabilidad de ocurrencia o el impacto del riesgo operativo, teniendo en cuenta lo siguiente:

- a. Control Preventivo: Es el que actúa sobre las causas del riesgo, con el fin de disminuir la probabilidad de ocurrencia de este.
- b. Control Detectivo: Es una “alarma” que se acciona cuando se descubre una situación anómala o no buscada.
- c. Control Correctivo: Permite corregir la desviación de los resultados en un proceso y prevenir de nuevo su ocurrencia. Este tipo de control toma las acciones necesarias una vez materializado el riesgo y busca mejorar los demás controles, si se determina que su funcionamiento no corresponde a las expectativas por las cuales fueron diseñados.

Los controles preventivos y detectivos, sirven para disminuir la probabilidad de ocurrencia del riesgo, mientras los controles correctivos se utilizan para disminuir su impacto. Es importante adoptar medidas de autocontrol en cada una de las actividades de los procesos.

4.3.1.2. Medir la efectividad del control

Para establecer la efectividad de un control, se deben medir dos variables:

- a. Eficacia. Un control es eficaz, si permite detectar el riesgo y disminuir su probabilidad de ocurrencia o impacto. El control debe actuar de tal forma, que disminuya la calificación del riesgo operativo; si no lo hace, se considera ineficaz.
- b. Eficiencia. Un control es eficiente si hace un uso adecuado de los recursos involucrados en su aplicación, tales como: personal, tecnología, tiempo, dinero, infraestructura, etc.

Un control es efectivo si es eficaz y eficiente. La metodología debe definir una escala para establecer la efectividad de los controles.

4.3.2. Implementar medidas de control

Una vez estimado el riesgo residual la organización debe establecer si acepta o no ese nivel de riesgo:

CIRCULAR BASICA CONTABLE Y FINANCIERA

- a. Si se acepta el riesgo residual, no se implementan nuevas medidas de control.
- b. Si no se acepta el nivel del riesgo residual, se evaluará la posibilidad de mejorar la efectividad del(los) control(es) actual(es) y/o la adopción de nuevas medidas de control.

Para aceptar o no el riesgo residual, es necesario que previamente se haya definido el nivel máximo de aceptación del riesgo residual.

Las organizaciones podrán decidir si transfieren, aceptan o evitan el riesgo en los casos en que esto sea posible. Se debe tener en cuenta que la utilización de ciertas medidas, como la contratación de un seguro o tercerización (outsourcing), puede ser fuente generadora de otros riesgos operativos, los cuales también deben ser administrados por la organización.

4.3.3. Administración de la continuidad del negocio

De acuerdo con su estructura, tamaño, objeto social y actividades de apoyo, las organizaciones solidarias deberán definir un equipo interdisciplinario para administrar el Plan de Continuidad de Negocio, que se encargará de definir, implementar, probar y mantener las acciones necesarias para garantizar la continuidad de las operaciones de la Organización. Dicho plan deberá incluir como mínimo los siguientes elementos:

- a. Definir política de continuidad del negocio.
- b. Desarrollar el análisis de impacto del negocio.
- c. Identificar riesgos de continuidad del negocio.
- d. Definir estrategias de mitigación del riesgo de continuidad.
- e. Evaluar la efectividad (eficacia y eficiencia) de las estrategias de mitigación.
- f. Definir alternativas de operación y regreso a la actividad normal.

Los planes de continuidad del negocio deben cumplir, como mínimo, con los siguientes requisitos:

- a. Cubrir por lo menos, los siguientes aspectos: identificación de los riesgos que pueden afectar la operación, actividades a realizar cuando se presenten fallas, alternativas de operación y para el regreso al funcionamiento normal de la organización.
- b. Haber superado las pruebas necesarias para confirmar su efectividad.
- c. Ser conocidos por todos los interesados.

CIRCULAR BASICA CONTABLE Y FINANCIERA

4.3.4. Administración de la seguridad de la información

De acuerdo con su estructura tecnológica, tamaño y manejo de información, se debe definir, implementar, probar y mantener un proceso para administrar la seguridad de la información del negocio que incluya elementos como:

- a. Definir la política de seguridad de la información.
- b. Identificar los activos de información.
- c. Identificar los riesgos de seguridad de la información.
- d. Definir, implementar y probar un plan de gestión de riesgos de seguridad de la información.

En el **Anexo 2** del presente capítulo se detallan las Instrucciones sobre seguridad y calidad de la información para la prestación de los servicios financieros.

4.4. MONITOREO

La organización debe realizar un monitoreo periódico, mínimo en forma semestral, del perfil de riesgo operativo y de la exposición a pérdidas. Para tal efecto, se deben cumplir, como mínimo, con los siguientes requisitos:

- a. Asegurar que las acciones planeadas para administrar el SARO se ejecuten.
- b. Evaluar la eficiencia de la implementación del SARO, que facilite la rápida detección y corrección de sus deficiencias.
- c. Hacer revisiones sobre la marcha para asegurar que los controles estén funcionando en forma efectiva.
- d. Identificar los riesgos operativos que puedan surgir, o que no fueron detectados antes, mediante la definición de indicadores descriptivos o prospectivos.
- e. Asegurar que el riesgo residual de cada riesgo operativo se encuentre en los niveles de aceptación establecidos por la organización.
- f. La actualización de las etapas de identificación, medición y control, definidas en este capítulo, deben tener una periodicidad acorde con los riesgos operativos potenciales y ocurridos, así como con la frecuencia y naturaleza de los cambios en el entorno operativo de la organización.

5. ELEMENTOS DEL SARO

5.1. POLÍTICAS

Cada una de las etapas y elementos del SARO deben contar con unas políticas claras y efectivamente aplicables, las cuales deben permitir un adecuado funcionamiento del

CIRCULAR BASICA CONTABLE Y FINANCIERA

sistema y traducirse en reglas de conducta y procedimientos que orienten la actuación de la organización. Las políticas que se adopten deben cumplir con los siguientes requisitos mínimos:

- a. La política de gestión de riesgo operativo es responsabilidad del Consejo de Administración y su aplicación de la Gerencia General.
- b. El Consejo de Administración debe definir el nivel máximo de riesgo residual aceptable para cada riesgo identificado.
- c. Toda la organización es responsable de la gestión de los riesgos operativos.
- d. Promover la integración del riesgo operativo a la cultura organizacional, a partir de la divulgación y capacitación en los temas que componen su gestión, y en las herramientas que se emplean para su administración y control.
- e. Establecer el deber de los órganos de administración, de control y de los demás funcionarios, de asegurar el cumplimiento de las normas internas y externas relacionadas con la administración del riesgo operativo.
- f. Permitir la prevención y resolución de conflictos de interés en la recolección de información en las diferentes etapas del sistema, especialmente para el registro de eventos de riesgo operativo.
- g. Desarrollar e implementar el plan de continuidad del negocio.
- h. Desarrollar e implementar el plan de seguridad de la información.

5.2. PROCEDIMIENTOS

La organización debe establecer los procedimientos que se deben aplicar para la adecuada implementación y funcionamiento de las etapas y elementos del SARO, los cuales deben contemplar, como mínimo, los siguientes requisitos:

- a. Instrumentar las diferentes etapas y elementos.
- b. Identificar los cambios y la evolución de los controles, así como del perfil de riesgo.
- c. Implementar las actividades para asegurar el registro de los eventos por riesgos operativos.
- d. Adoptar medidas por el incumplimiento del SARO.

5.3. DOCUMENTACIÓN

Las etapas y los elementos del SARO implementados deben constar en documentos y

CIRCULAR BASICA CONTABLE Y FINANCIERA

registros, garantizando la integridad, oportunidad, confiabilidad y disponibilidad de la información allí contenida. La documentación debe incluir como mínimo:

- a. El manual de riesgo operativo.
- b. Los documentos y registros que evidencien la operación efectiva del SARO
- c. Los informes del Consejo de Administración, del Representante legal y de los Órganos de control relacionados con este riesgo.

5.3.1. Manual de Riesgo Operativo

El Manual de riesgo operativo debe contener, como mínimo, la siguiente información:

- a. Las políticas para la administración del riesgo operativo.
- b. La estructura organizacional del SARO.
- c. Los roles y responsabilidades de quienes participan en la administración del riesgo operativo.
- d. Las medidas necesarias para asegurar el cumplimiento de las políticas y objetivos del SARO.
- e. Los procedimientos y metodologías para identificar, medir, controlar y monitorear los riesgos operativos y su nivel de aceptación.
- f. Los procedimientos y metodologías para implementar y mantener el registro de eventos.
- g. Los procedimientos que deben implementar los órganos de control frente al SARO.
- h. Las estrategias de capacitación y divulgación del SARO

5.4. ESTRUCTURA ORGANIZACIONAL

La organización debe establecer y asignar como mínimo las siguientes funciones, en relación con las distintas etapas y elementos del SARO, a cargo de los órganos de dirección, administración y demás áreas de la organización:

5.4.1. Consejo de Administración

Las siguientes son las funciones mínimas a cargo del Consejo de Administración, en relación con el SARO:

- a. Establecer las políticas para la administración del SARO.

CIRCULAR BASICA CONTABLE Y FINANCIERA

- b. Aprobar el Manual de riesgo operativo y sus actualizaciones.
- c. Hacer seguimiento y pronunciarse sobre el perfil de riesgo operativo de la organización.
- d. Establecer las medidas relativas al perfil de riesgo operativo, teniendo en cuenta el nivel de tolerancia al riesgo, el cual debe ser determinado por el mismo Consejo de Administración.
- e. Pronunciarse y hacer seguimiento a los informes periódicos que presente el Representante Legal, dejando constancia en las actas de las reuniones respectivas.
- f. Pronunciarse sobre la evaluación periódica del SARO, que realicen los órganos de control, dejando constancia en las actas de las reuniones respectivas.
- g. Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente el SARO.
- h. Aprobar los planes de contingencia, de continuidad del negocio y de seguridad de la información.
- i. Designar el área o persona que actuará como responsable de la implementación y seguimiento del SARO.

5.4.2. Representante Legal

Sin perjuicio de las funciones asignadas en otras disposiciones, son funciones mínimas del Representante Legal frente al SARO:

- a. Diseñar y someter a aprobación del Consejo de Administración, el Manual de riesgo operativo y sus actualizaciones.
- b. Velar por el cumplimiento efectivo de las políticas establecidas por el Consejo de Administración.
- c. Adelantar un seguimiento permanente de las etapas y elementos constitutivos del SARO.
- d. Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la administración de este riesgo implica para la organización.
- e. Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo operativo, fijado por el Consejo de Administración.
- f. Velar por la correcta aplicación de los controles del riesgo inherente.

CIRCULAR BASICA CONTABLE Y FINANCIERA

- g. Recibir y evaluar los informes presentados por el área o funcionario encargado del riesgo operativo.
- h. Velar porque las etapas y elementos del SARO cumplan, como mínimo, con las disposiciones señaladas en el presente capítulo.
- i. Velar porque se implementen los procedimientos para la adecuada administración del riesgo operativo a que se vea expuesta la organización, en desarrollo de su actividad.
- j. Presentar un informe periódico, al Consejo de Administración sobre la evolución y aspectos relevantes del SARO, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área o funcionario responsable.
- k. Establecer un procedimiento para realizar el registro de eventos de riesgo operativo.
- l. Velar porque el registro de eventos de riesgo operativo cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, eficiencia y confidencialidad de la información allí contenida.

5.4.3. Área o funcionario encargado del riesgo operativo

El área o funcionario encargado del riesgo operativo debe cumplir como mínimo con las siguientes condiciones:

- a. El personal del área o funcionario responsable debe tener conocimientos y experiencia en administración de riesgo operativo.
- b. No tener dependencia de los órganos de control, ni de las áreas de operaciones o de tecnología, ni relaciones que originen conflictos de interés.
- c. Contar con los recursos suficientes para desarrollar sus funciones.

El área o el funcionario responsable de la administración del riesgo operativo tendrá, como mínimo, las siguientes funciones:

- a. Definir los instrumentos, metodologías y procedimientos tendientes a que la organización administre efectivamente sus riesgos operativos, en concordancia con los lineamientos, etapas y elementos mínimos previstos en este capítulo.
- b. Desarrollar e implementar el sistema de reportes, internos y externos de riesgo operativo de la organización.
- c. Administrar la base de datos de eventos de riesgo operativo.
- d. Coordinar la recolección de la información para alimentar el registro de eventos de

CIRCULAR BASICA CONTABLE Y FINANCIERA

- riesgo operativo.
- e. Evaluar la efectividad de las medidas de control para los riesgos operativos medidos.
 - f. Establecer y monitorear el perfil de riesgo operativo de la organización e informarlo al órgano correspondiente, en los términos del presente Capítulo.
 - g. Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO y proponer sus correspondientes actualizaciones y modificaciones.
 - h. Coordinar y desarrollar las metodologías definidas para gestionar las etapas de identificación, medición, control y monitoreo del riesgo operativo.
 - i. Coordinar con el representante legal, el desarrollo de los programas de capacitación de la organización relacionados con el SARO.
 - j. Realizar seguimiento a las medidas de control adoptadas para mitigar el riesgo operativo inherente, con el propósito de evaluar su efectividad.
 - k. Presentar mensualmente al Representante Legal y al comité de riesgos, un informe sobre la evolución del riesgo operativo, los controles implementados y el monitoreo que se realice sobre el mismo, en los términos del presente capítulo.

Las organizaciones solidarias vigiladas podrán contratar a un experto externo a la organización que lleve a cabo funciones o actividades operativas que apoyen el área o al funcionario responsable de la administración de las etapas y elementos del SARO. El experto deberá contar con conocimientos y experiencia demostrable en la administración de riesgos operativos.

5.5. REGISTRO DE EVENTOS DE RIESGO OPERATIVO

Para la administración del riesgo operativo, la organización debe construir un registro de eventos de riesgo y mantenerlo actualizado. Este registro debe contener todos los eventos de riesgo operativo ocurridos y que:

- a. Generen pérdidas y que afecten el estado de resultados.
- b. No generen pérdidas y por lo tanto no afectan el estado de resultados de la organización.

Estos eventos deben revelarse en los términos señalados en el numeral 5.5.2 del presente capítulo, teniendo en cuenta que en los casos del literal b) del presente numeral, la medición será de carácter cualitativo.

5.5.1. Procedimiento para registrar los eventos de riesgo operativo

CIRCULAR BASICA CONTABLE Y FINANCIERA

Los eventos de pérdida por riesgo operativo y su registro en una base de datos, parte de un enfoque sistémico del entendimiento de los sucesos derivados de los riesgos operativos, entendiendo la interrelación entre la identificación de los riesgos operativos, sus causas, consecuencias y controles, de manera que se pueda priorizar en aquellos riesgos que tengan mayor severidad en su operación.

De acuerdo con lo anterior, es necesario contar con un procedimiento que asegure el correcto levantamiento de eventos por riesgo operativo importantes. Esto se cumple con información completa, valorada y validada del evento. Para ello, el procedimiento debe contemplar al menos los siguientes aspectos:

- a. Un procedimiento claro, no complejo, que permita a los funcionarios identificar que está sucediendo un “potencial evento o pérdida” por riesgo operativo. Se debe definir un formulario, con información mínima, para ser diligenciada por el funcionario que identifica el problema, para luego ser enviado al área o funcionario responsable del SARO.
- b. El funcionario responsable es quien debe finalmente recibir y analizar la información del potencial evento o pérdida, y tomar la decisión de su relevancia o no para iniciar la documentación y registro de un nuevo evento de pérdida por riesgo operativo.
- c. Para asegurar la integridad de la información de la base de datos de eventos por riesgo operativo, el procedimiento debe contener unas actividades de revisión y certificación de la calidad de la información registrada.

5.5.2. Información del registro de eventos de riesgo operativo

El registro de un evento por riesgo operativo debe contener, como mínimo, los siguientes campos:

- a. Referencia: un código interno que relacione el evento en forma secuencial.
- b. Fecha de inicio del evento: Fecha en que se inició el evento, indicando día, mes año, hora
- c. Fecha de finalización del evento: Fecha en que se finalizó el evento, indicando día, mes, año, hora.
- d. Fecha del descubrimiento: Fecha en que se descubre el evento, indicando día, mes año, hora.
- e. Fecha de contabilización: Fecha en que se registra contablemente la pérdida tipo a) por el evento, según lo señalado en el numeral 5.5 del presente capítulo.
- f. Cuantía: El monto de dinero al que asciende la pérdida según la descripción contenida en el numeral 5.5, del presente capítulo.

CIRCULAR BASICA CONTABLE Y FINANCIERA

- g. Cuantía total recuperada: El monto de dinero recuperado por acción directa de la organización solidaria.
- h. Cuantía recuperada por seguros: Corresponde al monto de dinero recuperado por el cubrimiento a través de un seguro.
- i. Clase de riesgo operativo: Se establece la clasificación por factor de riesgo operativo asociada al evento registrado, según la clasificación definida en el **Anexo 1** del presente Capítulo.
- j. Cuenta Contable afectada: Identifica la cuenta del Plan Único de Información Financiera con fines de supervisión afectada, donde se registra contablemente la pérdida por el evento, si aplica.
- k. Producto/servicio afectado: Identifica el principal producto o servicio afectado, si aplica.
- l. Proceso: Identifica el proceso principal afectado.
- m. Descripción del evento: Descripción detallada del evento.
- n. Canal de servicio o atención al cliente donde se evidencio el evento, si aplica.
- o. Ciudad o zona geográfica donde se materializó el evento, si aplica.

Para la construcción de la base de datos de registro de eventos de riesgo operativo, la organización puede utilizar, además de los campos descritos en este numeral, otros que considere relevantes.

5.6. ÓRGANOS DE CONTROL

La organización solidaria debe establecer instancias responsables de efectuar una evaluación del SARO, las cuales deberán informar, de forma oportuna, los resultados obtenidos, a los órganos competentes y en ningún caso cumplirán las funciones asignadas al área o funcionario responsable del riesgo operativo.

Los órganos de control serán por lo menos los siguientes: Revisoría Fiscal y Auditoría Interna o quien ejerza el control interno, los cuales tendrán las funciones que se relacionan a continuación:

5.6.1. Revisoría Fiscal

Sin perjuicio de las funciones asignadas en otras disposiciones al Revisor Fiscal, éste debe cumplir como mínimo, con las siguientes funciones frente al SARO:

CIRCULAR BASICA CONTABLE Y FINANCIERA

- a. Poner en conocimiento del Representante Legal, comité de riesgo y consejo de administración, los incumplimientos del SARO que evidencie en el desarrollo de sus auditorías, incluyendo el seguimiento a las recomendaciones. sin perjuicio de la obligación de informar sobre ellos al Consejo de Administración.
- b. Informar de manera oportuna y permanente a la Superintendencia de Economía Solidaria, las irregularidades materiales que advierta en la aplicación de lo dispuesto en el presente capítulo, en desarrollo de lo dispuesto en el numeral 3) del artículo 207, del Código de Comercio.
- c. Elaborar un informe al cierre de cada ejercicio contable, dirigido al consejo de administración, representante legal y comité de riesgos acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el SARO y la efectividad del sistema adoptado por la organización solidaria.
- d. Incluir un pronunciamiento expreso sobre el SARO en el dictamen sobre los estados financieros.

5.6.2. Auditoría Interna o quien ejerza el control interno

Sin perjuicio de las funciones asignadas en otras disposiciones a la Auditoría Interna, o quien ejerza el control interno, ésta debe:

- a. Evaluar semestralmente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARO, con el fin de determinar las deficiencias y sus posibles soluciones.
- b. Informar los resultados de la evaluación al área o funcionario encargado del riesgo operativo y al Representante Legal.
- c. Realizar una revisión periódica del registro de eventos de riesgo operativo e informar al Representante Legal sobre el cumplimiento de las condiciones señaladas en el numeral 5.5 del presente capítulo.

5.7. INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS DE INFORMACIÓN

Las organizaciones vigiladas deben contar con la tecnología y los sistemas necesarios para garantizar el funcionamiento eficiente, eficaz y oportuno del SARO.

Para ello deben contar con un soporte tecnológico acorde con su tamaño, naturaleza, complejidad y volumen de sus operaciones.

5.8. DIVULGACIÓN DE INFORMACIÓN

La divulgación de la información debe hacerse en forma periódica y estar disponible, cuando así se requiera, para hacer un seguimiento continuo del nivel de exposición al riesgo

CIRCULAR BASICA CONTABLE Y FINANCIERA

operativo, al igual que de los avances y mejoras realizadas al SARO.

5.8.1. Interna

Las organizaciones deben diseñar un sistema adecuado de reportes internos, que garantice el funcionamiento de sus propios procedimientos y el cumplimiento de los requerimientos normativos.

Como resultado del monitoreo, se deben elaborar reportes semestrales que permitan establecer el perfil de riesgo residual de la organización solidaria, en concordancia con lo previsto en el literal k) del numeral 5.4.3 del presente capítulo.

5.8.2. Externa

En su informe de gestión, al cierre de cada ejercicio contable, los administradores deben incluir información sobre la gestión adelantada en materia de administración del riesgo operativo.

Así mismo, en las revelaciones que acompañan los estados financieros de cierre de ejercicio, se debe presentar un detalle de la situación en materia de riesgo operativo, señalando las causas que originaron los eventos de riesgo operativo.

5.8.3. Revelación de información

- a. Las pérdidas causadas por un evento operativo, cuando afecten el estado de resultados, deben registrarse en cuentas de gastos en el período en el que se materializó la pérdida.
- b. Las recuperaciones por concepto de riesgo operativo cuando afecten el estado de resultados deben registrarse en cuentas de ingreso en el período en el que se materializó la recuperación.

Las cuentas de gastos e ingresos requeridas serán definidas por la Superintendencia de Economía Solidaria, en el Catálogo Único de Información con fines de supervisión.

5.9. CAPACITACIÓN

La organización solidaria debe diseñar, programar y coordinar planes de capacitación sobre el SARO dirigidos a todas las áreas, funcionarios e integrantes de los órganos de administración y control. Tales programas deben cumplir mínimo, con las siguientes condiciones:

- a. Periodicidad anual.
- b. Ser impartidos durante el proceso de inducción de los nuevos funcionarios.

CIRCULAR BASICA CONTABLE Y FINANCIERA

- c. Ser impartidos a los terceros siempre que exista una relación contractual con éstos y desempeñen funciones de la organización.
- d. Ser constantemente revisados y actualizados.
- e. Contar con los mecanismos de evaluación de los resultados obtenidos con el fin de determinar la eficacia de dichos programas y el alcance de los objetivos propuestos.