

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 1

CAPITULO XXIII

REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Consideraciones generales

En desarrollo de sus operaciones, las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) se exponen al Riesgo Operativo (RO).

Por tal razón, dichas entidades deben desarrollar, establecer, implementar y mantener un Sistema de Administración de Riesgo Operativo (SARO), acorde con su estructura, tamaño, objeto social y actividades de apoyo, estas últimas realizadas directamente o a través de terceros, que les permita identificar, medir, controlar y monitorear eficazmente este riesgo.

Dicho sistema está compuesto por elementos mínimos (políticas, procedimientos, documentación, estructura organizacional, el registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación) mediante los cuales se busca obtener una efectiva administración del riesgo operativo.

1. **Ámbito de aplicación**

Todas las entidades sometidas a la inspección y vigilancia de la SFC, deben adoptar un Sistema de Administración de Riesgo Operativo (SARO), con excepción de las Oficinas de Representación de instituciones financieras y reaseguradoras del exterior.

2. **Definiciones**

Las siguientes definiciones se tendrán en cuenta para los fines de la presente Circular:

2.1. **Riesgo Operativo (RO)**

Se entiende por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores.

2.1.1. **Riesgo legal**

Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

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

2.1.2. **Riesgo reputacional**

Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

2.2. **Perfil de Riesgo**

Resultado consolidado de la medición **permanente** de los riesgos a los que se ve expuesta la entidad.

2.3. **Factores de riesgo**

Se entiende por factores de riesgo las fuentes 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.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 2

2.3.1. Internos

2.3.1.1. Recurso Humano

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

Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente.

La vinculación indirecta hace referencia a aquellas personas que tienen con la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo

2.3.1.2. Procesos

Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

2.3.1.3. Tecnología

Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y telecomunicaciones.

2.3.1.4. Infraestructura

Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

2.3.2. Externos

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

2.4. Pérdidas

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

2.5. Evento

Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

2.6. Eventos de pérdida

Son aquellos incidentes que generan pérdidas por riesgo operativo a las entidades.

2.6.1. Clasificación de los riesgos operativos

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

2.6.1.1. Fraude Interno

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

2.6.1.2. Fraude Externo

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

2.6.1.3. Relaciones laborales

Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y, en general, la legislación vigente sobre la materia.

2.6.1.4. Clientes

Fallas negligentes o involuntarias de las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.

2.6.1.5. Daños a activos físicos

Pérdidas derivadas de daños o perjuicios a activos físicos de la entidad.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 3

2.6.1.6. Fallas tecnológicas

Pérdidas derivadas de incidentes por fallas tecnológicas.

2.6.1.7. Ejecución y administración de procesos

Pérdidas derivadas de errores en la ejecución y administración de los procesos.

2.7. Sistema de Administración de Riesgo Operativo (SARO)

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

2.8. Riesgo inherente

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

2.9. Riesgo residual

Nivel resultante del riesgo después de aplicar los controles.

2.10. 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.

2.11. Plan de contingencia

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

2.12. Manual de Riesgo Operativo

Es el documento contentivo de todas las políticas, objetivos, estructura organizacional, estrategias, los procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del SARO.

2.13. La Unidad de Riesgo Operativo

Se entiende por Unidad de Riesgo Operativo el área o cargo, designada por el Representante Legal de la entidad, que debe coordinar la puesta en marcha y seguimiento del SARO.

3. Sistema de Administración del Riesgo Operativo (SARO)

Previo a la implementación de las etapas del SARO, las entidades deben establecer las políticas, objetivos, procedimientos y estructura para la administración de riesgo operativo. El sistema debe estar alineado con los planes estratégicos de cada entidad.

3.1. Etapas de la Administración del Riesgo Operativo

En la administración del riesgo operativo, las entidades deben desarrollar las siguientes etapas:

3.1.1. Identificación

En desarrollo del SARO las entidades deben identificar **los riesgos operativos a que se ven expuestas**, teniendo en cuenta los factores de riesgo definidos en este **capítulo**.

Para identificar el riesgo las entidades deben como mínimo:

- a) Identificar y documentar la totalidad de los procesos.
- b) Establecer metodologías de identificación, que sean aplicables a los procesos, con el fin de determinar **los riesgos operativos**.
- c) Con base en las metodologías establecidas en desarrollo del literal b) del numeral 3.1.1 del presente **capítulo**, identificar **los riesgos operativos**, potenciales y ocurridos, en cada uno de los procesos.
- d) La etapa de identificación debe realizarse previamente a la implementación o modificación de cualquier proceso, **así como** en los casos de fusión, adquisición, cesión de activos, pasivos y contratos, entre otros.

3.1.2. Medición

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 4

Una vez concluida la etapa de identificación, las entidades deben 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.

En el proceso de medición de **los riesgos operativos**, las entidades deben desarrollar, como mínimo, los siguientes pasos:

- a) Establecer la metodología de medición **individual y consolidada** susceptible de **aplicarse** a los riesgos operativos identificados. La metodología debe ser aplicable tanto a la probabilidad de ocurrencia como al impacto.
- b) Aplicar la metodología establecida en desarrollo del literal a) del numeral 3.1.2 del presente **capítulo** para lograr una medición de la probabilidad de ocurrencia y del impacto **de los riesgos operativos** en la totalidad de los procesos de la entidad, **conforme a la clasificación establecida en el numeral 2.6.1.**
- c) Determinar el perfil de riesgo inherente **de la entidad.**

3.1.3. Control

Las entidades deben tomar medidas para controlar **los riesgos inherentes** a que se ven expuestas con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que se materialicen.

Durante esta etapa las entidades deben como mínimo:

- a) Establecer la metodología con base en la cual definan las medidas de control **de los riesgos operativos.**
- b) De acuerdo con la metodología establecida en desarrollo del literal a) del numeral 3.1.3 del presente **capítulo**, implementar las medidas de control sobre cada uno **de los riesgos operativos.**
- c) Determinar las medidas que permitan asegurar la continuidad del negocio.
- d) Estar en capacidad de determinar el perfil de riesgo residual **de la entidad.**

Sin perjuicio de lo anterior, las entidades podrán decidir si transfieren, aceptan o evitan el riesgo, en los casos en que esto sea posible.

La utilización de ciertas medidas, como la contratación de un seguro o **tercerización (outsourcing)**, puede ser fuente generadora de **otros riesgos operativos**, los cuales deben ser a su vez administrados.

3.1.3.1. Administración de la continuidad del negocio

De acuerdo con su estructura, tamaño, objeto social y actividades de apoyo, las entidades deben definir, implementar, probar y mantener un proceso para administrar la continuidad del negocio que incluya elementos como: prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

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

- a) Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia.
- b) Ser conocidos por todos los interesados.
- c) Cubrir por lo menos los siguientes aspectos: identificación de **los riesgos** que pueden afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y regreso a la actividad normal.

3.1.4. Monitoreo

Las entidades deben hacer un monitoreo periódico **del perfil de riesgo y de la exposición a pérdidas.**

Para el efecto, éstas deben cumplir, como mínimo, con los siguientes requisitos:

- a) Desarrollar un proceso de seguimiento efectivo, que facilite la rápida detección y corrección de las deficiencias en **el SARO**. Dicho seguimiento debe 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. En cualquier caso, el seguimiento debe realizarse con una periodicidad mínima semestral.
- b) Establecer indicadores descriptivos y/o prospectivos que evidencien los potenciales **riesgos operativos.**
- c) Asegurar que los controles estén funcionando en forma oportuna, efectiva y **eficiente.**

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 5

- d) Asegurar que los riesgos residuales se encuentren en los niveles de aceptación establecidos por la entidad.

3.2. Elementos del SARO

3.2.1. Políticas

Son los lineamientos generales que las entidades deben adoptar en relación con el SARO.

Cada una de las etapas y elementos del sistema **deben** contar con unas políticas claras y efectivamente **aplicables**.

Las políticas que se adopten deben permitir un adecuado funcionamiento del SARO y traducirse en reglas de conducta y procedimientos que orienten la actuación de la entidad.

Las políticas que adopten las entidades deben cumplir con los siguientes requisitos mínimos:

- a) Impulsar a nivel institucional la cultura en materia de riesgo operativo.
- b) **Establecer** el deber de los órganos de administración, de control y de sus demás funcionarios, de asegurar el cumplimiento de las normas internas y externas relacionadas con la administración del riesgo operativo.
- c) Permitir la prevención y resolución de conflictos de interés en la recolección de información en las diferentes etapas del SARO, especialmente para el registro de eventos de riesgo operativo.
- d) Permitir la identificación de los cambios en los controles y **en el perfil de riesgo**.
- e) Desarrollar e implementar planes de continuidad del negocio.

3.2.2. Procedimientos

Las entidades deben establecer los procedimientos aplicables para la adecuada implementación y funcionamiento de las etapas y elementos del SARO.

Los procedimientos que en esta materia adopten las entidades deben contemplar, como mínimo, los siguientes requisitos:

- a) Instrumentar las diferentes etapas y elementos del SARO.
- b) Identificar los cambios y la evolución de los controles, **así como del** perfil de riesgo.
- c) Adoptar las medidas por el incumplimiento del SARO.

3.2.3. Documentación

Las etapas y los elementos del SARO implementados por las entidades deben constar en documentos y registros, garantizando la integridad, oportunidad, confiabilidad y disponibilidad de la información allí contenida. La documentación debe incluir como mínimo:

- a) Manual de Riesgo Operativo.
- b) Los documentos y registros que evidencien la operación efectiva del SARO.
- c) Los informes de la Junta Directiva, el Representante Legal y los órganos de control en los términos de la presente Circular.

3.2.3.1. Manual de Riesgo Operativo

El Manual de Riesgo Operativo debe contener, como mínimo, lo siguiente:

- 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 del SARO y

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 6

- i) Las estrategias de divulgación del SARO.

3.2.4. Estructura Organizacional

Las entidades deben establecer y asignar funciones en relación con las distintas etapas y elementos del SARO.

Se deben establecer como mínimo las siguientes funciones a cargo de los órganos de dirección, administración y demás áreas de la entidad.

3.2.4.1. Junta Directiva u órgano que haga sus veces

Sin perjuicio de las funciones asignadas en otras disposiciones, el SARO debe contemplar como mínimo las siguientes funciones a cargo de la Junta Directiva u órgano que haga sus veces:

- a) Establecer las políticas relativas al SARO.
- b) Aprobar el Manual de Riesgo Operativo y sus actualizaciones.
- c) Hacer seguimiento y pronunciarse sobre el perfil de riesgo operativo de la entidad.
- d) Establecer las medidas relativas al perfil de riesgo operativo, teniendo en cuenta el nivel de tolerancia al riesgo de la entidad, fijado por la misma Junta Directiva.
- e) Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el Representante Legal.
- f) Pronunciarse sobre la evaluación periódica del SARO, que realicen los órganos de control.
- g) Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SARO.

3.2.4.2. Representante Legal

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

- a) Diseñar y someter a aprobación de la Junta Directiva u órgano que haga sus veces, el Manual de Riesgo Operativo y sus actualizaciones.
- b) Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva.
- c) Adelantar un seguimiento permanente de las etapas y elementos constitutivos del SARO.
- d) Designar el área o cargo que actuará como responsable de la implementación y seguimiento del SARO – (Unidad de Riesgo Operativo).
- e) 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 entidad.
- f) Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva, de acuerdo con el literal d) numeral 3.2.4.1. de la presente Circular.
- g) Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.
- h) Recibir y evaluar los informes presentados por la Unidad de Riesgo Operativo, de acuerdo con los términos establecidos en el numeral 3.2.4.3 de la presente Circular.
- i) Velar porque las etapas y elementos del SARO cumplan, como mínimo, con las disposiciones señaladas en la presente Circular.
- j) Velar porque se implementen los procedimientos para la adecuada administración del riesgo operativo a que se vea expuesta la entidad en desarrollo de su actividad.
- k) Aprobar los planes de contingencia y de continuidad del negocio y disponer de los recursos necesarios para su oportuna ejecución.
- l) Presentar un informe periódico, como mínimo semestral, a la Junta Directiva sobre la evolución y aspectos relevantes del SARO, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.
- m) Establecer un procedimiento para alimentar el registro de eventos de riesgo operativo, de acuerdo con lo previsto en el numeral 3.2.5 de la presente Circular.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 7

- n) Velar porque el registro de eventos de riesgo operativo cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.

3.2.4.3. La Unidad de Riesgo Operativo

La Unidad de Riesgo Operativo debe cumplir como mínimo con las siguientes condiciones:

- a) **Contar con personal que tenga conocimiento** en administración de riesgo operativo.
- b) Ser organizacionalmente de alto nivel y tener capacidad decisoria.
- c) No tener dependencia de los órganos de control, ni de las áreas de operaciones o de tecnología, ni relaciones que originen conflictos de interés.
- d) **Contar con los recursos suficientes para desarrollar sus funciones.**

En virtud de lo anterior, la Unidad de Riesgo Operativo tendrá como mínimo las siguientes funciones:

- a) Definir los instrumentos, metodologías y procedimientos tendientes a que la entidad 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, del riesgo operativo de la entidad.
- c) Administrar el registro de eventos de riesgo operativo.
- d) Coordinar la recolección de la información para alimentar el registro de **eventos de riesgo operativo**.
- e) Evaluar **la efectividad** de las medidas de control potenciales **y ejecutadas** para los riesgos **operativos** medidos.
- f) Establecer y monitorear el perfil de riesgo de la entidad 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) Desarrollar los modelos de medición del riesgo operativo.
- i) Desarrollar los programas de capacitación de la entidad relacionados con el SARO.
- j) Realizar seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.
- k) Reportar semestralmente al Representante Legal la evolución del riesgo, los controles implementados y el monitoreo que se realice sobre el mismo, en los términos de la presente Circular.

3.2.5. Registro de eventos de riesgo operativo

En los términos del numeral 3.2.5.1 de la presente Circular y para la administración del riesgo operativo las entidades deben construir un registro de eventos de riesgo operativo y mantenerlo actualizado. Este registro debe contener todos los eventos de riesgo operativo ocurridos y que:

- a) Generan pérdidas y afectan el estado de resultados de la entidad.
- b) Generan pérdidas y no afectan el estado de resultados de la entidad.
- c) No generan pérdidas y por lo tanto no afectan el estado de resultados de la entidad.

Dichos eventos deben revelarse en los términos del numeral 3.2.8.3 de la presente Circular.

Es importante anotar, que para los casos de los literales b) y c) del presente numeral, la medición será de carácter cualitativo.

3.2.5.1. Características mínimas del registro de eventos de riesgo operativo

- a) Cada entidad debe tener su propio y único registro de eventos de riesgo operativo. La entidad con matriz internacional debe tener disponible y centralizada en Colombia, la información relacionada con los eventos de riesgo operativo locales.
- b) Comprender la totalidad de los eventos de riesgo operativo.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 8

- c) Contener los siguientes campos mínimos, que corresponden a la información de los eventos de riesgo operativo :

- I. Referencia**
Código interno que relacione el evento en forma secuencial.
- II. Fecha de inicio del evento**
Fecha en que se inicia el evento.
Día, mes, año, hora.
- III. Fecha de finalización del evento**
Fecha en que finaliza el evento.
Día, mes, año, hora.
- IV. Fecha del descubrimiento**
Fecha en que se descubre el evento.
Día, mes, año, hora.
- V. Fecha de contabilización**
Fecha en que se registra contablemente la pérdida por el evento.
Día, mes, año, hora.
- VI. Divisa**
Moneda extranjera en la que se materializa el evento.
- VII. Cuantía**
El monto de dinero (moneda legal) a que asciende la pérdida, definida de acuerdo con el numeral 2.4. de la presente Circular.
- VIII. Cuantía total recuperada**
El monto de dinero recuperado por acción directa de la entidad. Incluye las cuantías recuperadas por seguros.
- IX. Cuantía recuperada por seguros**
Corresponde al monto de dinero recuperado por el cubrimiento a través de un seguro.
- X. Clase de riesgo operativo**
Especifica la clase de **riesgo**, según la clasificación adoptada en el numeral 2.6.1. de la presente Circular.
- XI. Producto/servicio afectado**
Identifica el producto o servicio afectado.
- XII. Cuentas PUC afectadas**
Identifica las cuentas del "Plan Único de Cuentas" (PUC) afectadas.
- XIII. Proceso**
Identifica el proceso afectado.
- XIV. Tipo de pérdida**
Identifica el tipo de pérdida, de acuerdo con la clasificación adoptada en el numeral 3.2.5 literales a), b) y c) de la presente Circular.
- XV. Descripción del evento**
Descripción detallada del evento.
 - Canal de servicio o atención al cliente (cuando aplica)
 - Zona geográfica
- XVI. Líneas operativas:**
Identificación según clasificación **adoptada por la SFC en el Anexo I del presente capítulo.**

Para la construcción del registro de eventos de riesgo operativo las entidades podrán utilizar, además de los campos descritos en este numeral, otros que se consideren relevantes.

3.2.6. Órganos de control

Las entidades deben establecer instancias responsables de efectuar una evaluación del SARO, dichas instancias informarán, de forma oportuna, los resultados a los órganos competentes **y en ningún caso cumplirá las funciones asignadas a la unidad de riesgo operativo.**

Los órganos de control serán por lo menos los siguientes: Revisoría Fiscal y Auditoría Interna o quien ejerza el control interno.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Página 9

3.2.6.1. Revisoría Fiscal

Sin perjuicio de las funciones asignadas en otras disposiciones al Revisor Fiscal, éste debe elaborar un reporte al cierre de cada ejercicio contable, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el SARO.

A su vez, debe poner en conocimiento del Representante Legal los incumplimientos del SARO, sin perjuicio de la obligación de informar sobre ellos a la Junta Directiva u órgano que haga sus veces.

3.2.6.2. 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 evaluar periódicamente 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. Así mismo, debe informar los resultados de la evaluación a la Unidad de Riesgo Operativo y al Representante Legal.

También debe 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 3.2.5. de la presente Circular.

3.2.7. Plataforma tecnológica

Las entidades, de acuerdo con sus actividades y tamaño, deben contar con la tecnología y los sistemas necesarios para garantizar el adecuado funcionamiento del SARO.

3.2.8. Divulgación de información

La divulgación de la información debe hacerse en forma periódica y estar disponible, cuando así se requiera.

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

3.2.8.1. Interna

Como resultado del monitoreo deben elaborarse reportes semestrales que permitan establecer, el perfil de riesgo residual de la entidad.

Los administradores de la entidad, en su informe de gestión, al cierre de cada ejercicio contable, deben incluir una indicación sobre la gestión adelantada en materia de administración del riesgo operativo.

3.2.8.2. Externa

En concordancia con el artículo 97 del Estatuto Orgánico del Sistema Financiero (EOSF) y demás disposiciones legales vigentes sobre la materia, las entidades deben suministrar al público la información necesaria con el fin de que el mercado pueda evaluar las estrategias de gestión del riesgo operativo adoptadas por la entidad.

Las características de la información divulgada estarán relacionadas con el volumen, la complejidad y el perfil de riesgo de la entidad.

3.2.8.3. Revelación contable

Las pérdidas definidas de acuerdo con el numeral 2.4. de la presente Circular, cuando afecten el estado de resultados, deben registrarse en cuentas de gastos en el período en el que se materializó la pérdida.

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 esta Superintendencia en el Plan Único de Cuentas respectivo.

3.2.9. Capacitación

Las entidades deben diseñar, programar y coordinar planes de capacitación sobre el SARO dirigidos a todas las áreas y funcionarios.

Tales programas deben, cuando menos cumplir con las siguientes condiciones:

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

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CAPITULO XXIII REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO Página 10

- c) Ser impartidos a los terceros siempre **que exista** una relación contractual con éstos y **desempeñen funciones de la entidad**.
- 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.