

PARTE 1
ADMINISTRACIÓN DE RIESGOS

CAPÍTULO 1
SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS
(SIAR)

SECCIÓN 1
GENERALIDADES DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS
CONSIDERACIONES GENERALES

(SIAR)

1.1.1.1.

El presente capítulo contiene los lineamientos y parámetros mínimos que sus destinatarios deben observar para una gestión adecuada e integral de los riesgos inherentes al desarrollo del negocio. El texto está compuesto por cinco ~~Partes~~secciones. La primera ~~sección~~ contiene las generalidades del Sistema Integral de Administración de Riesgos (SIAR). La segunda señala las instrucciones para la administración de los riesgos de crédito, mercado, operacional, liquidez, país, contraparte, de seguros, garantía del Fondo Nacional de Garantías (FNG) y riesgo de tasa de interés del libro bancario. La tercera establece las instrucciones para la medición y/o reporte estándar de los riesgos de crédito, mercado, operacional, liquidez, país y riesgo tasa de interés del libro bancario. La cuarta ~~sección~~ contiene la agregación de datos sobre riesgos y presentación de informes. La ~~sección~~ quinta incluye las definiciones utilizadas en las ~~Partes I, II,~~ ~~secciones 1, 2, 3 y IV~~4.

~~PARTE I. GENERALIDADES DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DE~~
~~RIESGOS~~
~~(SIAR)~~

INTRODUCCIÓN

1.1. SIAR

1.1.1.2.

Las entidades ~~de las que trata~~señaladas en el ~~subnumeral~~párrafo 1.21.1.6. de la presente ~~Parte~~sección deben diseñar, implementar y mantener el SIAR. Este sistema es un conjunto de políticas, estrategias, prácticas, procedimientos, metodologías, controles y umbrales y/o límites que, de manera integrada y coordinada, le permiten a la entidad:

- a. Establecer y fomentar una cultura de riesgo.
- b. Diseñar, implementar y monitorear el marco de apetito de riesgo y la estrategia para su ejecución.
- c. Articular la gestión de riesgos con el plan del negocio, los niveles de capital y liquidez y el apetito de riesgo.
- d. Identificar, medir, controlar, monitorear y reportar oportuna e integralmente los riesgos inherentes al desarrollo del negocio, incluidos los derivados de la administración de activos de terceros.
- e. Contribuir a la evaluación de la suficiencia de capital y liquidez.
- f. Guardar coherencia entre sus políticas de gestión de riesgos y las de sus subordinadas, cuando aplique.

1.1.1.3.

El SIAR debe estar acorde con el perfil y apetito de riesgo, el plan de negocio, la naturaleza, el tamaño, la complejidad y diversidad de las actividades que desarrolle la

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

entidad, así como con los entornos económicos y de los mercados en donde opera la entidad. El SIAR debe revisarse por lo menos una vez al año y actualizarse cuando resulte necesario con el fin de incorporar los cambios en los elementos antes indicados.

1.1.1.4.

Para efectos del SIAR, la entidad debe gestionar los riesgos tanto a nivel individual como consolidado. Lo anterior, sin perjuicio de la responsabilidad de las entidades subordinadas de gestionar sus riesgos y su negocio. En este sentido cada una de las subordinadas debe implementar un SIAR, o un Sistema de Administración de Riesgos de las Entidades Exceptuadas del SIAR (SARE), cuando esté obligada a hacerlo, el cual debe estar en armonía con el SIAR de la entidad controlante.

1.1.1.5.

El SIAR incluye los lineamientos definidos en la presente [Partesección](#), así como los señalados en las ~~Partes II, III~~[secciones 2, 3, 4](#) y ~~IV~~[5](#) del presente capítulo.

Ámbito de aplicación

1.1.1.6.

Las entidades vigiladas deben diseñar, implementar y mantener un SIAR, respecto de todos los riesgos inherentes al desarrollo del negocio, siguiendo los parámetros mínimos señalados en la presente [Partesección](#), tanto a nivel individual como consolidado.

• Excepciones

1.1.1.7.

Están exceptuadas de cumplir las instrucciones de la presente [Partesección](#):

- a. Los holdings financieros que no ejerzan directamente actividades financieras, de seguros, bursátil o en general relacionada con el manejo, aprovechamiento e inversión de los recursos captados del público, las Sociedades de Depósitos y Pagos Electrónicos (SEDPE), las oficinas de representación de instituciones financieras del exterior en Colombia, las reaseguradoras del exterior en Colombia y las Institutos de Fomento y Desarrollo Regional (INFIS).
- b. Las sociedades corredoras de seguros y reaseguros, los almacenes generales de depósito, las sociedades de intermediación cambiaria y servicios financieros especiales, los organismos de autorregulación, las bolsas de valores, las sociedades administradoras de depósitos centralizados de valores, las sociedades calificadoras de valores, la cámara de riesgo central de contraparte, los fondos de garantías diferentes al FNG, las administradoras de sistemas de pago de bajo valor, las bolsas agropecuarias, las sociedades administradoras de sistemas de negociación y registro de divisas, las sociedades administradoras de sistemas de negociación de valores y de registro de operaciones sobre valores, las sociedades administradoras de sistemas de compensación y liquidación de divisas, los proveedores de precios para valoración, el Banco de la República, las titularizadoras, y las sociedades que realicen la actividad de financiación colaborativa (SOFICO).

COMPONENTES DEL SIAR

Marco de apetito de riesgo

~~La entidad debe~~1.1.1.8.

[Las entidades deben](#) establecer el apetito de riesgo, es decir, los niveles y tipos de riesgos que ~~está dispuesta~~[están dispuestas](#) a asumir con el fin de cumplir con el plan de negocio.

1.1.1.9.

El marco de apetito de riesgo (MAR) es el conjunto de políticas, metodologías, procedimientos, controles y umbrales y/o límites a partir del cual la entidad: (i) identifica los riesgos asociados al plan de negocio, (ii) evalúa si dichos riesgos se asumen, mitigan, evitan o transfieren, y (iii) monitorea y controla que dichos riesgos se encuentren dentro de los umbrales y/o límites definidos por la Alta Gerencia (AG) y aprobados por la Junta Directiva (JD).

1.1.1.10.

Un adecuado MAR debe como mínimo:

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

- a. Ser difundido y comprendido por la AG, la JD, ~~quien(es) desarrolle(n)~~quienes desarrollen la función de gestión de riesgos, el comité de riesgos, la auditoría interna, el revisor fiscal y las unidades de negocio de la entidad.
- b. Ser consistente con el plan de negocio, las actividades que desarrolla la entidad, su perfil de riesgo, y sus niveles de capital y liquidez, así como con los demás requerimientos regulatorios, las condiciones de las economías y los mercados en donde ~~esta~~la entidad opera y su gestión de los riesgos.
- c. Incluir elementos cualitativos y cuantitativos, para lo cual, por lo menos se deben medir las pérdidas o niveles de riesgo que la entidad está dispuesta a asumir. A nivel cuantitativo, estas deben expresarse ~~cómo~~como mínimo en términos de capital, rentabilidad, volatilidad y/o liquidez, en el caso en que aplique.
- d. Incluir un análisis prospectivo de tal manera que le permita a la entidad anticiparse y prepararse para la materialización de los riesgos tanto en escenarios normales como adversos.
- e. Definir objetivos, controles y umbrales y/o límites frente a las pérdidas o los niveles de riesgo que la entidad está dispuesta a asumir, con un desglose para cada una de las actividades significativas que desarrolle y por jurisdicción donde opere. Esto debe incluir la definición de la capacidad y tolerancia a los riesgos asumidos.
- f. Ser parte del proceso de toma de decisiones de la JD y la AG y de la evaluación y seguimiento de los riesgos.
- g. Estar documentado.

Etapas del SIAR

1.1.1.11.

La entidad debe atender las siguientes etapas del SIAR, las cuales deben estar en línea con el MAR-:

- a. Identificación: consiste en determinar los riesgos (actuales y potenciales) inherentes a las actividades que desarrolla o planea desarrollar la entidad. En el caso de la implementación de nuevas actividades o modificación sobre las que están en operación y/o cambios en el plan de negocio, esta etapa debe realizarse previamente.
- b. Medición: consiste en cuantificar y/o evaluar la exposición a los riesgos inherentes a las actividades que desarrolla o planea desarrollar la entidad y su impacto en caso de materializarse. Esta medición debe ser cualitativa y/o cuantitativa.
- c. Control: consiste en establecer los mecanismos tendientes a mitigar y/o minimizar la posibilidad de ocurrencia e impacto de la materialización de los riesgos inherentes a las actividades que desarrolla la entidad. Los controles deben permitirle a la entidad conocer el grado de cumplimiento de sus políticas, estrategias, procedimientos, metodologías, controles, umbrales y/o límites y marco regulatorio, así como contar con información actualizada, confiable, oportuna y completa.
- d. Monitoreo: consiste en realizar un seguimiento permanente y efectivo a las fuentes de riesgo, al perfil de riesgo, a las desviaciones frente a los límites y/o umbrales, a la efectividad de los controles implementados y al posible impacto de la materialización de los riesgos. Adicionalmente, debe facilitar la rápida detección y corrección de las deficiencias en el SIAR. El monitoreo debe ser intensivo en relación con las deficiencias identificadas en la gestión de los riesgos y en los correctivos y acciones de mejora.

Políticas del SIAR

1.1.1.12.

Es el conjunto de directrices sobre las cuales se fundamenta la gestión de los riesgos de la entidad. Estas políticas deben: (i) ser claras y de conocimiento y cumplimiento de todos los funcionarios de la entidad y verse reflejadas en las responsabilidades y

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

facultades que estos desempeñan y (ii) estar soportadas e implementadas a través de procedimientos, estrategias, metodologías, modelos, controles y umbrales y/o límites.

~~La entidad debe~~ 1.1.1.13.

Las entidades deben como mínimo definir y adoptar políticas y procedimientos que ~~les~~ permitan cumplir con lo siguiente:

- **Gestión de riesgos**

1.1.1.14.

Divulgar el SIAR y el MAR a la JD, la AG, a ~~quien(es) desarrolle(n)~~ quienes desarrollen la función de gestión de riesgos, el comité de riesgos, el revisor fiscal, la auditoría interna y a las unidades de negocio de la entidad.

1.1.1.15.

Divulgar las políticas y elementos del SIAR, incluidos los lineamientos de conducta o ética al interior de la entidad a fin de promover la cultura de riesgo y tomar las medidas correctivas y de mejora en caso de incumplimiento.

1.1.1.16.

Instrumentar las etapas del SIAR y sus elementos.

1.1.1.17.

Revisar periódicamente la idoneidad y funcionamiento del SIAR y actualizarlo cuando resulte necesario.

1.1.1.18.

Definir y aprobar los mercados y actividades que la entidad desarrolla y/o planea desarrollar o modificar, así como su composición de activos, pasivos y capital.

1.1.1.19.

Gestionar los riesgos inherentes a los nuevos mercados, procesos y/o actividades.

1.1.1.20.

Definir, monitorear y reportar los umbrales y límites del MAR y niveles máximos de exposición, concentración y pérdida tolerada por tipo de riesgo, con un desglose de las posiciones por sector económico, actividad, plazo, tipo de operación, reasegurador, contraparte, vinculados, partes relacionadas, área geográfica y divisa, cuando aplique.

1.1.1.21.

Contar con criterios para exigir, aceptar y realizar el avalúo de las garantías y contragarantías, cuando aplique. Lo anterior, sin perjuicio de las garantías exigidas por los administradores de los sistemas de negociación de valores, sistemas de registro de operaciones sobre valores, bolsas de valores, bolsas de bienes y productos agropecuarios, agroindustriales o de otras materias primas, el sistema de compensación y liquidación de operaciones y cámaras de riesgo central de contraparte.

1.1.1.22.

Tomar e implementar las acciones necesarias, incluidas las disciplinarias, ante: (i) cambios inesperados en la exposición de riesgo, (ii) activación del sistema de alertas tempranas e (iii) incumplimiento de los límites internos y/o regulatorios. De igual forma implementar los lineamientos de cuándo y a quiénes se escalan y reportan los eventos mencionados anteriormente.

1.1.1.23.

Implementar las medidas necesarias ante la materialización de los riesgos y la revisión periódica de la efectividad de dichas medidas.

1.1.1.24.

Diseñar e implementar los planes de contingencia y la gestión y plan de continuidad del negocio, así como realizar la revisión periódica de la efectividad de dichos planes.

1.1.1.25.

Administrar el registro de eventos de riesgo operacional.

1.1.1.26.

Contratar seguros y tercerizar en personas naturales y/o jurídicas el desarrollo de sus procesos, siempre que no implique la delegación de la profesionalidad.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

• Gobierno de riesgos y control

[1.1.1.27.](#)

Asignar el personal y los recursos físicos, económicos y tecnológicos para el desarrollo, implementación y mantenimiento adecuado del SIAR, así como las cualidades mínimas que estos deben tener.

[1.1.1.28.](#)

Capacitar al personal de la entidad para fortalecer sus competencias en materia de gestión de riesgos y para asegurar la efectiva ejecución de las funciones asignadas.

[1.1.1.29.](#)

Contar con lineamientos de conducta o ética que orienten la actuación de los funcionarios de la entidad para el efectivo y oportuno funcionamiento del SIAR.

[1.1.1.30.](#)

Evaluar la correspondencia entre el plan de negocio y los niveles de capital y liquidez y el MAR de la entidad, así como con las funciones y atribuciones asignadas a la AG, la JD, a ~~quien(es) desarrolle(n)~~[quienes desarrollen](#) la función de gestión de riesgos, el comité de riesgos, el revisor fiscal y la auditoría interna.

[1.1.1.31.](#)

Identificar, administrar, revelar, comunicar y resolver los conflictos de interés en concordancia con el código de ética o de conducta de la entidad y la legislación vigente.

[1.1.1.32.](#)

Gestionar, comunicar y aprobar las operaciones intragrupo y con vinculados y partes relacionadas.

[1.1.1.33.](#)

Adecuar el sistema de control interno al SIAR, [en lo que está relacionado con la gestión de riesgos](#).

[1.1.1.34.](#)

Determinar los incentivos adecuados acordes con una prudente asunción de riesgos y con el MAR, los objetivos a largo plazo y los niveles de capital y liquidez de la entidad.

• Información

[1.1.1.35.](#)

Comunicar a la JD, comité de riesgos y a la AG sobre la gestión de los riesgos, así como los hallazgos y recomendaciones de ~~quien(es) desarrolle(n)~~[quienes desarrollen](#) la función de gestión de riesgos, la auditoría interna y el revisor fiscal.

[1.1.1.36.](#)

Atender los requerimientos de información por parte de la Superintendencia Financiera de Colombia (SFC) y/o demás autoridades competentes, así como contar con los mecanismos para validar la calidad de la información suministrada.

ESTRUCTURA DE GOBIERNO DE RIESGOS

~~La entidad debe~~[1.1.1.37.](#)

[Las entidades deben](#) contar con una estructura organizacional apropiada para la gestión de los riesgos y cumplimiento del SIAR, la cual debe estar en línea con los negocios y riesgos a los que está expuesta. Esta estructura debe incluir:

- a. Los procedimientos que le permitan a la entidad la toma de decisiones informadas, la gestión de los riesgos, el diseño y seguimiento del SIAR y el reporte y rendición de cuentas.
- b. Las funciones y responsabilidades claramente definidas para las áreas y el personal de la entidad que participan en la gestión de riesgos, así como procedimientos para evaluar su desempeño.

[1.1.1.38.](#)

Las unidades de negocio de la entidad deben hacer parte de la gestión integral de los riesgos en la medida en que estas toman y/o generan exposición a uno o varios riesgos y por tanto son responsables de su continua gestión. Por lo anterior, las políticas, prácticas, estrategias, procedimientos, metodologías, modelos y umbrales y/o límites de

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

gestión de riesgos deben estar integradas en las actividades que desarrollan las unidades de negocio.

1.1.1.39.

Para la adecuada gestión de los riesgos a nivel consolidado, la entidad controlante debe: (i) contar con la información suficiente de las subordinadas, teniendo en cuenta las posibles restricciones de acceso por confidencialidad de la información para la entidad que consolida, e (ii) implementar los mecanismos de coordinación y de reporte que resulten necesarios.

Junta Directiva

1.1.1.40.

La JD o el órgano que haga sus veces debe cumplir como mínimo con las siguientes funciones y responsabilidades:

• **Gestión de riesgos**

- a. Aprobar el plan de negocio de la entidad y verificar su cumplimiento.
- b. Aprobar y verificar el cumplimiento del MAR, las políticas del SIAR, los límites generales de exposición y concentración, la estructura de gobierno de riesgos, las estrategias para gestionar: (i) los riesgos, (ii) el capital, (iii) la liquidez y (iv) los conflictos de interés y su revelación; así como sus actualizaciones. Para lo anterior se debe verificar que estos elementos sean acordes con el perfil y apetito de riesgo, el plan de negocio, la naturaleza, el tamaño, la complejidad y diversidad de las actividades que desarrolle la entidad, y los entornos económicos y los mercados en donde esta opera la entidad.
- c. Aprobar: (i) los lineamientos de los informes internos que se le presenten en relación con la gestión de los riesgos y (ii) el plan de contingencia de liquidez; así como sus actualizaciones.
- d. Aprobar las medidas a implementar y realizar seguimiento a su aplicación y efectividad, cuando se presenten: (i) incrementos en la exposición a los riesgos que resulten en sobrepasos en los umbrales y/o límites regulatorios y/o internos definidos por la entidad o incumplimientos en el MAR, (ii) debilidades en el SIAR para realizar una gestión de los riesgos acorde con las economías y mercado en donde opera la entidad, su nivel de capital y liquidez, el marco regulatorio, el plan de negocio y el perfil y apetito de riesgo de la entidad y (iii) las acciones correctivas y de mejora, una vez se hayan superado las instancias previas en la estructura de gobierno.
- e. Conocer los resultados de las pruebas de estrésresistencia y aprobar las medidas o planes a implementar para mitigar los riesgos con base en sus resultados.
- f. Monitorear, por lo menos una vez al año, la efectividad e idoneidad del SIAR para realizar una adecuada gestión de los riesgos, y su concordancia con el plan de negocio y con las economías y mercados en donde opera la entidad, así como aprobar las acciones de mejora.
- g. Aprobar de forma previa la reclasificación de una posición en el libro de tesorería o en el libro bancario, como resultado de una estrategia de cobertura identificada. La reclasificación sólo regirá a partir de los 30 días hábiles siguientes a su adopción. Lo anterior no supone ni permite la reclasificación de inversiones para efectos de valoración y contabilización, cuyas reglas se encuentran consignadas en el **capítulo de valoración de inversiones de la Circular Básica Contable y Financiera (CBCF)**. En todo caso, las estrategias de cobertura a implementar deberán cumplir los criterios definidos en el **capítulo XVIII de la CBCF**.

• **Recursos**

- h. Designar los miembros que hacen parte del comité de riesgos, aprobar su reglamento y definir sus funciones.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

- i. Aprobar, ~~por lo menos una vez al año, la política de capacitación del personal que hace parte de la estructura del gobierno de riesgos de la entidad, así como~~ los lineamientos en materia de ética o conducta y de control interno relacionados con el SIAR.

1.1.1.41.

Las decisiones que tome la JD en desarrollo de las atribuciones antes mencionadas deben constar por escrito en el acta de la reunión respectiva y estar debidamente motivadas.

Representante legal

1.1.1.42.

El representante legal debe, bajo la dirección y supervisión de la JD, ejecutar y monitorear la implementación y cumplimiento del plan de negocio y del SIAR, razón por la cual debe como mínimo cumplir con las siguientes funciones y responsabilidades:

• Gestión de riesgos

- a. Someter a aprobación de la JD el plan de negocio, el MAR, las políticas del SIAR, los límites generales de exposición y concentración, la estructura de gobierno de riesgos, las estrategias para gestionar: (i) los riesgos, (ii) el capital, (iii) la liquidez y (iv) los conflictos de interés y su revelación; así como sus actualizaciones. De igual forma debe velar por su cumplimiento.
- b. Someter a aprobación de la JD: (i) los lineamientos de los informes internos que se le presenten en relación con la gestión de los riesgos y (ii) el plan de contingencia de liquidez; así como sus actualizaciones.
- c. Aprobar el manual del SIAR y los planes de contingencia y de continuidad del negocio. Este último debe contemplar los riesgos asociados a la interconectividad con otras infraestructuras y/o entidades vigiladas o proveedores (terceros).
- d. Verificar que los planes de contingencia y continuidad del negocio se contemplen en el presupuesto para su oportuna ejecución.
- e. Monitorear que el SIAR resulte adecuado para gestionar los riesgos y sea acorde con el perfil y apetito de riesgo, plan de negocio, naturaleza, tamaño y complejidad de la entidad, el marco regulatorio y las condiciones de las economías y mercados en donde esta opera.
- f. Revisar periódicamente la composición, características y nivel de diversificación de los activos, pasivos, capital, liquidez y estrategia de fondeo.

~~g. Velar porque el registro de eventos de riesgo operacional cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida, así como porque exista un procedimiento para alimentar dicho registro.~~

~~h.g.~~ Propender por la calidad y consistencia de la información de todos los riesgos previstos en el SIAR.

~~j.h.~~ Cumplir con las funciones y responsabilidades a las que se refieren los literales ~~(c,)~~, ~~(d-)~~, ~~(e)~~ y ~~(f)~~ del ~~subnumeral 3.4.párrafo 1.1.1.51.~~ de la presente ~~Parte~~sección, cuando la entidad no cuente con un comité de riesgos de conformidad con lo señalado en dicho subnumeral.

i. Aprobar, por lo menos una vez al año, la política de capacitación del personal que hace parte de la estructura del gobierno de riesgos de la entidad.

• Reportes e información

~~k.j.~~ Informar trimestralmente a la JD sobre el desempeño de la entidad, su situación financiera y los problemas identificados en la gestión de riesgos junto con las respectivas recomendaciones.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

- ~~h.k.~~ Informar oportunamente a la JD sobre: (i) los cambios o desviaciones frente al plan de negocio y el apetito de riesgo, (ii) cualquier situación o evento de riesgo que pueda comprometer la viabilidad del negocio o la confianza del público y garantizar que se tomen las medidas correctivas y/o acciones de mejora.
- ~~m.l.~~ Informar oportunamente a la SFC sobre cualquier situación o evento de riesgo que comprometa la viabilidad del negocio o la confianza del público, así como las causas que la originaron y las medidas que pondrán en marcha para corregir o enfrentar dicha situación.
- ~~m.m.~~ Comunicar por escrito a la SFC dentro de los 10 días hábiles siguientes a la autorización de que trata el literal [\(g\)](#) del ~~subnumeral 3.párrafo~~ [1.1.1.40](#) de la presente ~~Parte~~[sección](#).

Función de gestión de riesgos

- [1.1.1.43.](#)
La entidad debe desarrollar la gestión de riesgos de tal forma que sea organizacionalmente independiente de las unidades de negocio, áreas de tecnología y demás dependencias que podrían generar conflictos de interés. ~~Quien(es) desarrolle(n)~~[Quienes desarrollen](#) dicha función ~~debe(n):deben:~~ (i) tener acceso directo a la JD, al comité de riesgos, la AG, a las unidades de negocio y demás dependencias de la entidad, así como a sus registros e información; y (ii) contar con el nivel jerárquico, el poder de decisión y la autoridad suficiente para cumplir con sus funciones y responsabilidades y para hacer recomendaciones y seguimiento a las medidas tomadas por la administración en respuesta a los problemas y oportunidades de mejora identificados.
- [1.1.1.44.](#)
Adicionalmente, las entidades vigiladas que consoliden y que tengan subordinadas vigiladas y/o extranjeras que ejerzan una actividad propia de las entidades vigiladas por la SFC en al menos dos o más industrias, deben contar con un ejecutivo de alto nivel jerárquico y autoridad dentro de la organización, ~~quien~~ es el encargado directo de la función de gestión de riesgos. Este funcionario debe: (i) tener una visión integral de los riesgos de la entidad y comprender los riesgos de las subordinadas y (ii) ser independiente de las unidades de negocio de ésta y de sus subordinadas. Se considera una buena práctica que [este funcionario](#) sea nombrado por la JD. En todo caso, debe cumplir con las funciones establecidas en el presente subnumeral.
- [1.1.1.45.](#)
Para las demás entidades vigiladas, la ~~adopción~~[designación del ejecutivo](#) de ~~esta figura~~[alto nivel jerárquico de que trata el párrafo anterior](#) dependerá de la naturaleza, el tamaño y la complejidad de las actividades que desarrolle [la entidad vigilada](#).

~~Quien(es) desarrolle(n)~~[1.1.1.46.](#)
[Quienes desarrollen](#) la gestión de riesgos en la entidad ~~debe(n):deben~~ cumplir como mínimo con las siguientes funciones y responsabilidades:

- **Gestión de riesgos**
- a. Elaborar con el representante legal el MAR, el manual del SIAR y sus actualizaciones.
- b. Desarrollar las políticas, los procedimientos, las estrategias, las metodologías, los modelos, umbrales y/o los límites, los controles, los planes de contingencia y el plan de continuidad del negocio y el marco de indicadores de alertas tempranas y de seguimiento del MAR. Presentar al representante legal las actualizaciones que resulten pertinentes.
- c. Evaluar, en coordinación con las demás áreas involucradas en la gestión de riesgos, los planes de contingencia y continuidad de negocio, la exposición y gestión a los riesgos y sus desviaciones frente a los límites y el apetito al riesgo y su concordancia con los niveles de capital y liquidez. Lo anterior debe incluir los

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

riesgos inherentes a las nuevas actividades y/o mercados, y su impacto en el perfil y gestión de riesgos de la entidad.

- d. Monitorear la influencia de las posiciones y características de fondeo de las partes relacionadas en el riesgo de liquidez de la entidad.
- e. Pronunciarse sobre las operaciones que no cumplan con las políticas, controles y/o límites de riesgo establecidos por la entidad o en el marco regulatorio y reportarlas a la mayor brevedad al representante legal y a los responsables de las unidades de negocio.

~~f. Realizar pruebas de estrés que permitan establecer las potenciales exposiciones al riesgo de la entidad bajo una variedad de escenarios y diseñar las medidas o planes a implementar para mitigar los riesgos con base en sus resultados.~~

~~h. Comparar los resultados de las pruebas de estrés frente a los niveles de apetito de riesgo e identificar las acciones mitigantes de los riesgos correspondientes y reportar los resultados a la JD, al representante legal y al comité de riesgos.~~

f. Realizar pruebas de resistencia de conformidad con el **Capítulo XXVIII de la CBCF.**

i.g. Administrar el registro de eventos de riesgo operacional y coordinar la recolección de la información para dicho registro y, a partir de este, generar información que contribuya a la gestión de los riesgos.

j.h. Cumplir con las funciones a las que se refieren los literales a y b del subnumeral 3.4. de la presente Parte, cuando la entidad no cuente con un comité de riesgos de conformidad con lo señalado en dicho subnumeral.

• **Reportes de información**

k.i. Reportar trimestralmente a la JD sobre la naturaleza y el nivel de los riesgos de la entidad y su consistencia con el apetito de riesgo y los niveles de capital y liquidez, incluyendo los posibles resultados en condiciones extremas basadas en hipótesis razonables. En todo caso, se le debe informar oportunamente cuando se presenten incrementos significativos en la exposición de los riesgos, así como su afectación en los niveles actuales y futuros de capital y liquidez.

l.j. Reportar mensualmente al representante legal y al comité de riesgos:

- i. La exposición a los riesgos de la entidad con un desglose, como mínimo, de la exposición específica de cada actividad significativa y por riesgo, sus desviaciones frente a los límites establecidos y su correspondencia con los niveles de capital y liquidez, en caso en que aplique. Los informes sobre la exposición al riesgo de liquidez deben incluir la cuantificación de los descargos o desbalances de flujos en comparación con el monto de activos líquidos disponibles por la entidad, realizando un énfasis especial en las operaciones celebradas con entidades del conglomerado financiero y con las partes relacionadas, así como un análisis de sensibilidad y pruebas bajo condiciones extremas basadas en hipótesis razonables.
- ii. Para el caso del riesgo de contraparte, el nivel de concentración global y segmentado por tipo de garantía que respalde la operación vigente de cumplimiento de los clientes. Dicha información debe desagregarse como mínimo por plazo, tipo de operación y tipo de contraparte.

m.k. Reportar semestralmente a la JD, al comité de riesgos, y al representante legal la evolución del riesgo operacional, los controles implementados y el monitoreo que se realice sobre el mismo, así como las acciones preventivas y correctivas implementadas o por implementar y el área responsable.

n.l. Reportar al representante legal y a los responsables de las unidades de negocio:

- i. Por lo menos una vez al día, y dependiendo del tipo de negocio o actividad, el comportamiento del riesgo de mercado y liquidez al responsable de la unidad de negocio correspondiente. Este reporte debe hacerse al

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

[representante legal por lo menos una vez a la semana y, en todo caso, cuando se presenten situaciones que puedan afectar la liquidez requerida por la entidad se debe aumentar la periodicidad de reporte.](#)

- ii. Semanalmente, los niveles de riesgo de mercado, las condiciones de las negociaciones realizadas y, en particular, los incumplimientos a los límites, las operaciones poco convencionales o por fuera de las condiciones de mercado, y las operaciones con vinculados y partes relacionadas.

e.m. Asegurar que la JD, la AG y el comité de riesgos, estén oportuna y debidamente informados sobre:

- i. Los incumplimientos del MAR, los umbrales y/o límites internos y/o regulatorios y proponer las medidas correctivas correspondientes.
- ii. Los cambios en las condiciones del entorno económico, político y de los mercados, tanto local como externo, que puedan afectar el perfil de riesgo actual y futuro de la entidad y/o comprometer el cumplimiento de los límites y políticas del SIAR.
- iii. Los riesgos inherentes a las nuevas actividades y/o mercados y su impacto en el perfil y gestión de riesgos de la entidad y en los niveles de capital y liquidez.

p.n. Reportar de forma oportuna y comprensible a la AG y a los responsables de las unidades de negocio, los problemas identificados en la gestión de riesgos junto con las respectivas recomendaciones.

Comité de riesgos

[1.1.1.47.](#)

Sin perjuicio de la existencia de los comités que cada entidad decida establecer dentro de su estructura de gobierno de riesgos, las entidades vigiladas que consoliden y que tengan subordinadas vigiladas y/o extranjeras que ejerzan una actividad propia de las entidades vigiladas por la SFC en al menos dos o más industrias, deben contar con un comité de riesgos. Este [comité](#) debe estar conformado por un número impar de miembros, como mínimo 3 y sesionar de manera ordinaria por lo menos cada 3 meses.

[1.1.1.48.](#)

El comité debe ser presidido por un miembro independiente de la JD para aquellas entidades que por disposición legal o estatutaria cuenten con miembros independientes en el referido órgano social. Así mismo los integrantes deben contar con conocimientos y experiencia en materia de gestión de riesgos. El responsable directo de la función de gestión de riesgos debe apoyar al comité. Se considera una buena práctica que este comité esté conformado con más de un miembro de JD.

[1.1.1.49.](#)

El comité de riesgos de las entidades emisoras de valores que cumpla con la estructura organizacional señalada anteriormente, podrá asumir las funciones, responsabilidades y periodicidad a que se refiere el presente subnumeral.

[1.1.1.50.](#)

Para el caso de las sociedades administradoras de fondos de pensiones y cesantías, en adición a las funciones antes señaladas, se deben tener en cuenta las establecidas en el capítulo IV del título III de la parte 2 de la Circular Básica Jurídica (CBJ).

[1.1.1.51.](#)

El comité de riesgos debe cumplir como mínimo con las siguientes funciones y responsabilidades:

- a. Realizar seguimiento al perfil y apetito de riesgo de la entidad, así como evaluar su coherencia con el plan de negocio, los niveles de capital y liquidez, e informar a la JD sobre los principales resultados y emitir las correspondientes recomendaciones, cuando resulte necesario.
- b. Asesorar a la JD sobre las operaciones, eventos o actividades, incluida la incursión en nuevos mercados, que puedan (i) afectar la exposición y perfil de riesgos de la

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

entidad, (ii) constituir desviaciones frente al plan de negocio, apetito de riesgo y límites internos y regulatorios o (iii) comprometer la viabilidad del negocio.

- c. Revisar las políticas del SIAR al menos una vez al año y proponer a la JD para su respectiva aprobación los ajustes correspondientes.
- d. Asesorar a la JD sobre el estado de la cultura de riesgo en la entidad.
- e. Evaluar la idoneidad del plan de continuidad del negocio y los planes de contingencia.
- f. Informar a la JD su análisis del resultado de los reportes mensuales recibidos de [quien\(es\) desarrolle\(n\) quienes desarrollen](#) la función de gestión de riesgos.

Auditoría interna

[1.1.1.52.](#)

Sin perjuicio de las funciones y responsabilidades establecidas en el capítulo IV del título I de la parte I de la CBJ, la auditoría interna es la responsable de:

- a. Evaluar periódicamente la efectividad y cumplimiento del SIAR, o cuando se presenten situaciones que requieran su revisión e informar a [quien\(es\) desarrolle\(n\) quienes desarrollen](#) la función de gestión de riesgos, al representante legal, al comité de auditoría y a la JD los resultados de dicha evaluación, así como el seguimiento a las recomendaciones, acciones de mejora y cumplimiento del plan de auditoría. Esta evaluación debe cubrir de manera expresa, como mínimo, las operaciones y flujos de liquidez cursados hacia y desde partes relacionadas.
- b. Realizar el seguimiento a las recomendaciones o fallas identificadas en la gestión de riesgos que resulten de las evaluaciones de la SFC y de la propia auditoría interna, así como de los planes de acción y medidas adoptadas por la entidad.
- c. Informar a la SFC aquellas situaciones cuya materialidad puedan afectar el desarrollo del negocio y las acciones correctivas y de mejora que no hayan sido atendidas por la entidad.

[1.1.1.53.](#)

La evaluación realizada por la auditoría interna respecto del SIAR debe responder a los cambios en el entorno y en el perfil de riesgo de la entidad, así como basarse en los riesgos que esta enfrenta.

Revisor fiscal

[1.1.1.54.](#)

Sin perjuicio de las funciones asignadas en otras disposiciones, el revisor fiscal debe incluir dentro de su plan de auditoría la evaluación periódica del cumplimiento de las instrucciones del presente capítulo y debe elaborar un reporte anual con las conclusiones obtenidas en el proceso de evaluación y revisión del mismo, el cual debe quedar incluido en el dictamen sobre los estados financieros. Los mencionados reportes deben estar a disposición de la SFC.

[Así mismo 1.1.1.55.](#)

[Así mismo, en desarrollo de lo dispuesto en el artículo 207 del Código de Comercio](#), el revisor fiscal debe informar de manera oportuna a: (i) la asamblea de accionistas o equivalentes, (ii) la JD, (iii) el representante legal y (iv) la SFC, sobre las irregularidades materiales que advierta en el cumplimiento de las instrucciones establecidas en el presente capítulo, [incluyendo las instrucciones sobre los riesgos previstos en las partes II y III](#), y sobre las deficiencias en los controles internos. Dicho reporte debe estar debidamente documentado, incluyendo los resultados alcanzados, las acciones sugeridas y la respuesta de la entidad frente a sus observaciones.

INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS DE INFORMACIÓN

[1.1.1.56.](#)

La entidad debe contar con los sistemas, el soporte tecnológico y la arquitectura de datos que permitan una visión comprensiva de los riesgos, el funcionamiento del SIAR, la

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

presentación de informes, la toma de decisiones, así como el cumplimiento de los requerimientos normativos. Esta infraestructura debe contar como mínimo con:

- a. Un sistema de reportes tanto internos como externos, acorde con el tamaño, naturaleza y complejidad de las operaciones que realiza la entidad.
- b. Procedimientos para el manejo y almacenamiento de la información que permitan garantizar su confidencialidad, seguridad, calidad, disponibilidad, integridad, consistencia y consolidación.
- c. Bases de datos actualizadas e información suficiente y oportuna para realizar la gestión de riesgos.
- d. Lineamientos generales para la agregación de datos sobre riesgos y presentación de información de la entidad, conforme a las instrucciones [del numeral 10 de la Parte II del presente Capítulo de la sección 4 del capítulo 1 de la parte 1 de la CBRAPIF](#).
- e. Reportes de información con medidas comparables de las entidades subordinadas, sujetándose a la normatividad aplicable, sus limitaciones y excepciones.

1.1.1.57.

La entidad que opere con funciones de tesorería descentralizadas debe contar con un sistema de consolidación de las exposiciones a los diferentes riesgos, el cual debe ser validado por lo menos una vez al año y probado en diferentes escenarios como mínimo de tasas o precios, de forma tal que se ajuste a la realidad del mercado.

1.1.1.58.

El área encargada de realizar la validación y las pruebas [de funcionamiento de la infraestructura](#) debe enviar un reporte al comité de riesgos, en su defecto, al representante legal que incluya la descripción de la metodología utilizada para la validación y las pruebas, sus resultados y la identificación de las posibles acciones de mejora.

Información interna

1.1.1.59.

La entidad debe elaborar reportes periódicos que permitan: (i) establecer y conocer su perfil de riesgo en escenarios normales y adversos y la correspondencia con el apetito de riesgos, la estructura de activos y pasivos, los niveles de capital y liquidez, el plan de negocio y las condiciones de las economías y de los mercados en donde esta opera, (ii) anticiparse a los problemas, (iii) tomar decisiones informadas y (iv) proporcionar una evaluación de la gestión de los riesgos.

1.1.1.60.

El contenido y la frecuencia de los reportes de gestión de riesgos deben reflejar las necesidades de los destinatarios y la naturaleza del riesgo informado. La frecuencia de los informes debe aumentar en escenarios adversos. Estos reportes deben revelar las hipótesis o supuestos que se utilizaron para presentar la información y las limitaciones en la estimación de los riesgos.

1.1.1.61.

Adicionalmente, los administradores de la entidad deben incluir en su informe de gestión anual un reporte sobre las funciones desempeñadas en materia de gestión de los riesgos. Este informe de gestión debe ser presentado [a la JD y al representante legal de forma comprensible de forma comprensible a la asamblea general de accionista o el máximo órgano social, según el caso, de conformidad con lo previsto en los artículos 45, 46 y 47 de la Ley 222 de 1995 y en el artículo 446 del Código de Comercio](#).

Información externa

[De conformidad con el artículo 97 del Estatuto Orgánico del Sistema Financiero \(EOSF\) y demás disposiciones legales vigentes sobre la materia, la entidad debe suministrar al público la información necesaria con el fin de que éste pueda escoger las mejores opciones que le permitan tomar decisiones informadas. La información divulgada al público debe ser consistente con el tamaño, la complejidad, la naturaleza y el perfil de riesgo de las actividades que desarrolla la entidad. Así mismo, la entidad debe remitir la información a la SFC en los términos establecidos en el mencionado artículo y demás normas concordantes.](#)

1.1.1.62.

Las entidades deben dar cumplimiento a las disposiciones de la Ley 1328 de 2009, el artículo 97 del Estatuto Orgánico del Sistema Financiero, y las demás normas concordantes o que las sustituyen o modifiquen, en relación con la divulgación y remisión de información al público y a la SFC.

DOCUMENTACIÓN

1.1.1.63.

La entidad debe contar, como mínimo, con la siguiente documentación ~~como mínimo~~:

- a. El acta por medio de la cual la JD aprueba lo señalado en los literales a, b, c, d y g del ~~subnumeral 3~~ párrafo 1.1.1.40 de la presente ~~Parte~~ sección.
- b. La bitácora en la cual conste las actualizaciones y modificaciones del SIAR y el MAR.
- c. El manual del SIAR, el cual debe incluir: las etapas, las políticas, las estrategias, los procedimientos, las metodologías y las responsabilidades y funciones del gobierno de riesgos, en relación con la gestión de cada uno de los riesgos señalados en las ~~Partes~~ secciones 2 y 3 del presente capítulo y su gestión integral. Los ajustes a este manual deben estar documentados.
- d. Los modelos de riesgos.
- e. El plan de continuidad del negocio y los planes de contingencia.
- f. El sistema de alertas tempranas y demás indicadores implementados para el monitoreo de cada riesgo, así como las actuaciones, acciones correctivas y de mejora implementadas ante el incumplimiento de los límites o activación de las alarmas.
- g. Los reportes elaborados por los diferentes órganos y funcionarios del gobierno de riesgos en relación con la gestión de riesgos y demás documentos que soporten el monitoreo de dicha gestión.
- h. El código de ética o conducta.
- i. La estructura organizacional del gobierno de riesgos.
- j. El registro de eventos de riesgo operacional.

1.1.1.64.

El SIAR debe estar debidamente documentado teniendo un respaldo en medios verificables y contando con un plan de conservación, custodia y seguridad de la información, de forma tal que sólo se permita su consulta por los funcionarios autorizados.