

TITULO V

GESTIÓN DE RIESGO OPERATIVO

TABLA DE CONTENIDO

Capítulo I: Reglamento sobre Manuales de Procedimientos

Capítulo II: Directrices Básicas para la Gestión del Riesgo Operativo

Sección 1: Aspectos generales

Sección 2: Lineamientos para la gestión del riesgo operativo

Sección 3: Políticas y procedimientos para la gestión del riesgo operativo

Sección 4: Estructura organizativa, funciones y responsabilidades en la gestión del riesgo operativo

Sección 5: Registro de eventos de riesgo operativo

Sección 6: Sistemas de información para la gestión del riesgo operativo

Sección 7: Rol de la Unidad de Auditoría Interna

Sección 8: Otras disposiciones

Sección 9: Disposiciones transitorias

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

CAPÍTULO I: REGLAMENTO SOBRE MANUALES DE PROCEDIMIENTOS

REGLAMENTO ABROGADO

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS***CAPÍTULO II: DIRECTRICES BÁSICAS PARA LA GESTIÓN DEL RIESGO OPERATIVO******SECCIÓN I: ASPECTOS GENERALES***

Artículo 1° - (Objeto) El presente Capítulo tiene por objeto establecer directrices básicas que mínimamente las entidades de intermediación financiera y empresas de servicios financieros complementarios deben cumplir respecto a la gestión del riesgo operativo.

Artículo 2° - (Ámbito de aplicación) Las disposiciones contenidas en el presente Capítulo son de aplicación obligatoria para las entidades de intermediación financiera y empresas de servicios financieros complementarios, con excepción de las casas de cambio, que cuenten con licencia de funcionamiento emitida por la [Autoridad de Supervisión del Sistema Financiero \(ASFI\)](#), en adelante denominadas entidad supervisada.

Artículo 3° - (Definiciones) Para efectos del presente Capítulo, de manera enunciativa y no limitativa, se considerarán las siguientes definiciones:

- a. **Alta Gerencia:** Gerente general y gerentes de área o instancias equivalentes que conforman el plantel ejecutivo de la entidad supervisada;
- b. **Central de Información de Riesgo Operativo (CIRO):** Sistema de información administrado por [ASFI](#), que consolida los datos proporcionados por las entidades supervisadas, con relación a los eventos de riesgo operativo y pérdidas;
- c. **Comité de Riesgos:** Es el Órgano creado por la entidad supervisada, responsable del diseño de las políticas, sistemas, metodologías, modelos y procedimientos para la eficiente gestión del riesgo operativo.

Este Comité está integrado al menos por: un miembro del Directorio u Órgano equivalente, que será quien lo presida, el Gerente General y el responsable de la Unidad de Gestión de Riesgos. Para el caso del riesgo operativo, a dicho Comité se integrará necesariamente el Gerente de Operaciones o su instancia equivalente, con derecho a voz.

En el caso que la entidad supervisada se constituya como Sociedad de Responsabilidad Limitada (S.R.L.), ésta debe establecer una instancia equivalente que cumpla con las responsabilidades y funciones determinadas para este Comité;

- d. **Directorio u Órgano equivalente:** Órgano principal de dirección y administración de las entidades supervisadas, designado por la Junta General de Accionistas o Asamblea General de Socios o Asociados, según corresponda a su naturaleza jurídica;
- e. **Eventos de pérdida:** Son aquellos incidentes que generan pérdidas por riesgo operativo a las entidades supervisadas;
- f. **Evento de riesgo operativo:** Es un incidente o conjunto de ellos, que provocan que los resultados difieran de los esperados, debido a procesos defectuosos, recursos humanos inadecuados, fallos en los sistemas o por causas externas;
- g. **Evento Crítico:** Es un incidente o conjunto de ellos, que provocan que los resultados difieran de los esperados, debido a procesos defectuosos, recursos humanos inadecuados,

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

fallos en los sistemas o por causas externas, que superan la criticidad establecida en el perfil de riesgo operativo de la entidad;

- h. Factores de riesgo operativo:** Son la fuente, causa primaria o el origen de un evento de riesgo operativo, que pueden o no ocasionar pérdidas a la entidad supervisada, que incluyen a los procesos internos, personas, tecnología de información, eventos externos e infraestructura;
- i. Gestión del riesgo operativo:** Es el proceso estructurado, consistente y continuo para identificar, medir, monitorear, controlar, mitigar y divulgar el riesgo operativo al cual la entidad supervisada se encuentra expuesta, en el marco del conjunto de estrategias, objetivos, políticas, procedimientos y acciones, establecidas por la entidad para este propósito;
- j. Línea de negocio:** Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad supervisada;
- k. Perfil de riesgo:** Es la cantidad de riesgo que una entidad supervisada está dispuesta a asumir en su búsqueda de rentabilidad y solvencia;
- l. Pérdida por riesgo operativo:** Es la cuantificación económica del impacto negativo registrado en las cuentas de resultados o en la situación patrimonial de la entidad supervisada que haya sido provocado a consecuencia de cualquier evento de riesgo operativo;
- m. Plan de contingencia:** Es el documento que contempla procedimientos y acciones que deben entrar en funcionamiento al ocurrir un evento de riesgo operativo;
- n. Plan de continuidad del negocio:** Es el documento que contempla la logística que debe seguir la entidad supervisada a objeto de restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado, después de una paralización o desastre, a causa de un evento de riesgo operativo;
- o. Proceso:** Es un conjunto de actividades planificadas y estructuradas que implican la participación de un número de personas y de recursos materiales coordinados para conseguir un objetivo previamente identificado, que permite desarrollar con regularidad las operaciones propias de la entidad supervisada;
- p. Procesos críticos:** Proceso o sistema de información que al dejar de funcionar, afecta la continuidad operativa de la entidad supervisada;
- q. Riesgo:** Es la contingencia, probabilidad o posibilidad de que eventos, anticipados o no, puedan tener un impacto adverso contra ingresos y/o patrimonio de la entidad supervisada;
- r. Riesgo legal:** Es la posibilidad o probabilidad de que una entidad supervisada incurra en pérdidas derivadas del incumplimiento de la legislación y normativa vigentes o de relaciones contractuales inadecuadamente instrumentadas, siendo este un componente del riesgo operativo;
- s. Riesgo operativo:** Es la posibilidad o probabilidad de que una entidad supervisada incurra en pérdidas por fraude interno o externo, fallas en las personas, procesos y sistemas, eventos internos de orden estratégico y operativo y otros eventos externos;

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

- t. **Riesgo tecnológico:** Es la posibilidad o probabilidad de sufrir pérdidas por caídas o fallos en los sistemas informáticos o en la transmisión de datos, errores de programación u otros, siendo éste un componente del riesgo operativo;
- u. **Tipos de evento de pérdida:** Se refiere a los diferentes tipos de eventos de pérdida por riesgo operativo a los cuales se enfrenta la entidad supervisada, que con carácter enunciativo y no limitativo pueden corresponder a: fraudes interno o externo, relaciones laborales y seguridad en el puesto de trabajo, clientes, productos y prácticas empresariales, daños a activos materiales, incidencias en el negocio y fallos en los sistemas y ejecución, entrega y gestión de procesos;
- v. **Tipo de evento de pérdida por clientes, productos y prácticas empresariales:** Corresponde a fallas negligentes o involuntarias en las obligaciones que la entidad supervisada tiene frente a clientes concretos o de la naturaleza o diseño de un producto;
- w. **Tipo de evento de pérdida por daños a activos materiales:** Son eventos de pérdida derivados de daños o perjuicios a activos físicos de la entidad supervisada;
- x. **Tipo de evento de pérdida por ejecución, entrega y gestión de procesos:** Es aquel que se deriva de errores en la ejecución de operaciones, entrega o en la gestión de procesos en la entidad supervisada;
- y. **Tipo de evento de pérdida por fraude externo:** Son eventos de pérdida que se derivan de actos realizados por terceros con el fin de defraudar o apropiarse indebidamente de bienes de la entidad supervisada o incumplir disposiciones legales y reglamentarias;
- z. **Tipo de evento de pérdida por fraude interno:** Corresponde a eventos de pérdida resultantes de actos realizados en forma intencionada para defraudar o apropiarse indebidamente de bienes de la entidad supervisada o incumplir disposiciones legales y reglamentarias, en los que se ve involucrado cuando menos uno de sus funcionarios, en beneficio propio o de un tercero;
- aa. **Tipo de evento de pérdida por incidencias en el negocio y fallos en los sistemas:** Son eventos de pérdida derivados de interrupciones en el negocio e incidentes que se originan por fallos en hardware, software y las telecomunicaciones de la entidad supervisada;
- bb. **Tipo de evento de pérdida por relaciones laborales y seguridad en el puesto de trabajo:** Corresponde a eventos de pérdida derivados de actos incompatibles con la legislación laboral asociadas con el desarrollo de relaciones laborales y la seguridad que tienen las personas en el lugar de su trabajo;
- cc. **Unidad de Gestión de Riesgos:** Es un órgano autónomo responsable de identificar, medir, monitorear, controlar, mitigar y divulgar todos los riesgos que enfrenta la entidad supervisada. Esta unidad debe ser independiente de las áreas de negocios y del área de registro de operaciones, a fin de evitar conflictos de intereses y asegurar una adecuada separación de responsabilidades;

Su tamaño y ámbito deberán estar en relación con el tamaño y la estructura de la entidad y con el volumen y complejidad de los riesgos en los que incurra.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS**SECCIÓN 2: LINEAMIENTOS PARA LA GESTIÓN DEL RIESGO OPERATIVO**

Artículo 1° - (Implementación de la gestión del riesgo operativo) La entidad supervisada es responsable de administrar su riesgo operativo, a cuyo efecto debe contar con procesos formales para su gestión que le permitan identificar, medir, monitorear, controlar, mitigar y divulgar las exposiciones de riesgo que está asumiendo.

El proceso de gestión del riesgo operativo, debe considerar la exposición de la entidad supervisada a los riesgos legal y tecnológico. En este último caso se deben considerar en lo que corresponda las disposiciones establecidas en el [Reglamento para la Gestión de Seguridad de la Información](#) contenido en la [Recopilación de Normas para Servicios Financieros](#).

La administración del riesgo operativo, implica que la entidad supervisada debe definir su perfil de riesgo, de acuerdo a su naturaleza, tamaño y complejidad de sus operaciones.

El conjunto de políticas, procedimientos y acciones que constituyen un sistema para la gestión del riesgo operativo, deben ser revisados y actualizados permanentemente. Este sistema debe formar parte de la estrategia institucional de la entidad supervisada.

Artículo 2° - (Principios para la gestión del riesgo operativo) La entidad supervisada, en la implementación de la gestión del riesgo operativo, debe observar mínimamente los siguientes principios:

- a. Contar con una estrategia formal para la gestión del riesgo operativo, desarrollada a partir de la estrategia general de la entidad supervisada que responda a su modelo de negocios;
- b. Establecer una estructura organizativa con una clara segregación de funciones, acorde a la estrategia, tamaño y complejidad de las operaciones de la entidad supervisada, que facilite la gestión del riesgo operativo y evite posibles conflictos de interés;
- c. Desarrollar políticas, procedimientos y herramientas adecuadas a la estrategia, tamaño y complejidad de las operaciones de la entidad supervisada, que apoyen la gestión de riesgo operativo;
- d. Actualizar oportunamente el proceso de gestión del riesgo operativo en respuesta a los cambios en el entorno, modelo de negocios y/o el perfil de riesgo de la entidad supervisada;
- e. Promover una cultura de gestión del riesgo operativo al interior de la entidad supervisada;
- f. Implementar sistemas de información que permitan la divulgación del riesgo operativo al cual se encuentra expuesta la entidad supervisada, a las instancias que correspondan;
- g. Priorizar la implementación de acciones preventivas, antes que correctivas;
- h. Identificar y evaluar el riesgo operativo inherente a todos los productos, actividades, procesos y sistemas;
- i. Instaurar un proceso para el seguimiento regular de los perfiles de riesgo operativo y de su exposición a pérdidas;
- j. Implementar planes de contingencia y de continuidad del negocio a fin de garantizar su capacidad de operar en forma continua y minimizar las pérdidas en caso de interrupción del negocio;

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

Artículo 3° - (Etapas del proceso de gestión del riesgo operativo) La entidad supervisada para la gestión del riesgo operativo, debe observar las seis etapas comprendidas en el [Artículo 3°, Sección 2 de las Directrices Básicas para la Gestión Integral de Riesgos](#) contenidas en la [Recopilación de Normas para Servicios Financieros](#).

Artículo 4° - (Factores de riesgo operativo) La entidad supervisada, en la ejecución de sus operaciones y prestación de servicios tiene que considerar la existencia de fuentes de riesgo operativo, sobre las cuales debe:

- a. Gestionar apropiadamente el riesgo de incurrir en pérdidas financieras que se asocian a la implementación de procesos internos, como consecuencia del diseño inapropiado de los procesos o por políticas y procedimientos inadecuados o inexistentes, que puedan derivar en la ejecución deficiente de las operaciones y servicios o la suspensión de los mismos;
- b. Evaluar la posibilidad de sufrir pérdidas financieras relacionadas con el personal, derivadas de un ambiente laboral desfavorable, la falta de especificaciones claras en los términos de contratación del personal, inadecuada capacitación de funcionarios o actitudes y comportamientos inapropiados de éstos (negligencia, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros);
- c. Administrar los riesgos vinculados a la tecnología de información, que se relacionan entre otros con, fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas, compatibilidad e integración de los mismos, los problemas de calidad de la información, la inadecuada inversión en tecnología y las fallas en la adecuación a los objetivos del negocio.

A tal efecto la entidad supervisada debe considerar en lo correspondiente las disposiciones establecidas en el [Reglamento para la Gestión de Seguridad de la Información](#) contenidas en la [Recopilación de Normas para Servicios Financieros](#);

- d. Gestionar los riesgos asociados a eventos externos ajenos al control de la entidad supervisada, que puedan alterar el desarrollo de sus actividades (fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores);
- e. Administrar los elementos de apoyo para el funcionamiento de una organización diferentes a aquellos de carácter tecnológico, que entre otros pueden incluir edificios, espacios de trabajo, almacenamiento y transporte.

Artículo 5° - (Inventario de procesos) La entidad supervisada en la gestión del riesgo operativo que lleva adelante, debe realizar un inventario de procesos, determinando aquellos considerados como críticos. Dicho inventario tiene que contener mínimamente la siguiente información:

- a. Denominación del proceso;
- b. La periodicidad de su ejecución;
- c. Nivel de automatización;
- d. Grado de descentralización;
- e. Responsables de su ejecución, revisión y aprobación;
- f. Documentación de entrada y de salida del proceso;
- g. Productos y servicios que genera el proceso;
- h. Su clasificación como proceso crítico o no.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

La entidad supervisada con base en el inventario realizado, debe efectuar un análisis y evaluación de los procesos determinados, a efectos de establecer la posible existencia de debilidades en los mismos y adoptar las medidas oportunas, tendientes a reducir el riesgo operativo al que se encuentran expuestos.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS**SECCIÓN 3: POLÍTICAS Y PROCEDIMIENTOS PARA LA GESTIÓN DEL RIESGO OPERATIVO**

Artículo 1° - (Establecimiento de políticas) La entidad supervisada debe contar con políticas formalmente aprobadas por el Directorio u Órgano equivalente que sean concordantes con su Plan Estratégico y que respondan en todo momento a la naturaleza, complejidad y volumen de las operaciones que caracterizan su modelo de negocios y el perfil de riesgo que está asumiendo, logrando un adecuado equilibrio entre riesgo y rentabilidad.

Estas políticas deben contemplar mínimamente, los objetivos y lineamientos para las diferentes etapas del proceso de gestión del riesgo operativo, la clasificación y tratamiento de los eventos de riesgo operativo, la identificación de procesos críticos, la definición de líneas de negocios y el establecimiento del nivel de riesgo que la entidad supervisada está dispuesta a asumir, que puede expresarse a través de límites internos, u otros.

Artículo 2° - (Determinación del perfil de riesgo) Los criterios, metodologías y técnicas para la cuantificación del riesgo operativo, que consideren la complejidad de las operaciones y los niveles de riesgo asumidos, que le permita a la entidad supervisada establecer su perfil de riesgo, deben ser formalmente establecidos en un documento específico y enmarcarse en sus políticas.

Artículo 3° - (Simulación de escenarios) Las políticas deben reflejar un manejo prudente por lo cual deben incorporar el análisis de distintos escenarios alternativos, así como el establecimiento de márgenes con relación a los niveles de exposición definidos para el riesgo, mismos que le permitan a la entidad supervisada adoptar acciones oportunas, tendientes a evitar incumplimientos y/o le garanticen la continuidad de sus operaciones.

Los estudios documentados que respalden la construcción de los diferentes escenarios, deben reflejar las variables y supuestos utilizados por la entidad supervisada en su construcción y éstos a su vez deben ser el insumo para la elaboración de los planes de contingencia de acuerdo al tipo de riesgo que se analice. Dichos estudios deben permanecer a disposición de la [Autoridad de Supervisión del Sistema Financiero](#).

Artículo 4° - (Tratamiento de excepciones) La entidad supervisada, que producto de un análisis decida establecer un tratamiento de excepciones a sus políticas internas, debe especificar en el respectivo documento, mínimamente las condiciones, situaciones o factores que pueden ser considerados, para dar curso a las mismas, estableciendo un tiempo razonable para subsanar las desviaciones temporales acontecidas, mismas que no deben tener un carácter recurrente. Dichas excepciones no pueden estar relacionadas con el cumplimiento del marco normativo y legal vigente.

Artículo 5° - (Procesamiento de la información) Las políticas deben establecer la utilización de los sistemas informáticos que propicien un adecuado procesamiento de la información para la gestión del riesgo operativo, contemplando medidas de seguridad y planes de contingencia que protejan la información de acuerdo con las disposiciones establecidas en el [Reglamento para la Gestión de Seguridad de la Información](#) contenido en la Recopilación de Normas para Servicios Financieros según corresponda.

Artículo 6° - (Planes de contingencia y de continuidad del negocio) La entidad supervisada, en concordancia con sus estrategias y políticas debe desarrollar planes de contingencia y de continuidad del negocio que aseguren su capacidad de operar y limiten sus pérdidas ante la ocurrencia de eventos de riesgo operativo.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

Los planes de contingencia y de continuidad del negocio, deben detallar mínimamente los procesos críticos que fueron identificados por la entidad supervisada, incluidos aquellos que se encuentran tercerizados. Asimismo, deben establecer los mecanismos necesarios que permitan asegurar una rápida, efectiva y ordenada respuesta a los eventos de riesgo operativo.

En el caso de los eventos de riesgo operativo asociados a factores tecnológicos, la entidad supervisada debe considerar, según corresponda, las disposiciones establecidas en la [Sección 10 del Reglamento para la Gestión de Seguridad de la Información](#) contenido en la Recopilación de Normas para Servicios Financieros.

La entidad supervisada debe asegurarse permanentemente que el plan de contingencias y de continuidad del negocio son efectivos, para lo cual la Unidad de Gestión de Riesgos debe realizar las pruebas necesarias y remitir informes al Comité de Riesgos, Directorio u Órgano equivalente y a la Alta Gerencia sobre los resultados de dichas pruebas.

Artículo 7° - (Desarrollo de procedimientos) La entidad supervisada debe desarrollar e implementar procedimientos formales para la gestión del riesgo operativo, que estén en concordancia con las estrategias, principios y políticas, establecidos para este fin. Estos procesos deben guardar estrecha relación con la estructura organizacional, funciones y responsabilidades de las áreas involucradas en la gestión del riesgo operativo.

Los procedimientos desarrollados deben servir de soporte funcional para la gestión del riesgo operativo y ser periódicamente verificados en cuanto a su eficiencia, a fin de justificar actualizaciones o mejoras según demanden sus necesidades y/o se generen cambios en las estrategias y/o políticas de la entidad supervisada.

Las metodologías y herramientas establecidas por la entidad supervisada, deben formar parte de los procedimientos que desarrolla para gestionar su exposición al riesgo operativo.

Artículo 8° - (Nuevos productos y servicios financieros) La entidad supervisada, en el marco de lo establecido en el [Artículo 453 de la Ley N° 393 de Servicios Financieros \(LSF\)](#), para la creación de nuevos productos y servicios financieros, debe considerar los riesgos operativos que se encuentran asociados a la sofisticación de los servicios financieros, modernización continua de la tecnología y las telecomunicaciones, así como la incursión en nuevos mercados e innovaciones financieras.

En el desarrollo y aprobación de nuevos productos y servicios financieros, la entidad supervisada debe establecer las estrategias de cobertura de riesgos necesarias, el proceso de registro y dinámica contable, valorización y aprobación en concordancia con las políticas y procedimientos establecidos para tal fin.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS**SECCIÓN 4: ESTRUCTURA ORGANIZATIVA, FUNCIONES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO OPERATIVO**

Artículo 1° - (Estructura organizacional) Para la gestión del riesgo operativo, las entidades supervisadas deben establecer una adecuada estructura organizacional que delimite claramente las obligaciones, funciones y responsabilidades, así como los niveles de dependencia e interrelación entre las áreas involucradas en la gestión del riesgo operativo y las áreas de monitoreo y control del riesgo, las cuales deben estar adecuadamente segregadas.

A fin de evitar posibles conflictos de interés que puedan afectar el desempeño de las funciones de la gestión del riesgo operativo, debe existir independencia, entre las unidades de negocios y operativas, con las que administran el riesgo. Asimismo, el personal debe contar con los conocimientos y habilidades necesarias para desempeñar sus funciones dentro del proceso de la gestión del riesgo operativo.

Todos estos aspectos deben estar contemplados en un manual de organización y funciones.

Artículo 2° - (Responsabilidades y funciones del Directorio u Órgano Equivalente) El Directorio u Órgano equivalente, de la entidad supervisada, es responsable de la gestión del riesgo operativo, debiendo en consecuencia cumplir, al menos las siguientes tareas:

- a. Aprobar, revisar, actualizar y realizar seguimiento a las estrategias, políticas y procedimientos para identificar, medir, monitorear, controlar, mitigar y divulgar la gestión del riesgo operativo;
- b. Asegurar que se establezcan y revisen los procedimientos y mecanismos orientados a generar un sistema adecuado de la gestión del riesgo operativo;
- c. Conocer los principales riesgos operativos, establecer niveles aceptables de exposición y asegurarse que la gerencia general los cumpla;
- d. Aprobar la estructura organizacional para la gestión del riesgo operativo. Así como sus manuales de organización y funciones y de procedimientos, debiendo asegurar que exista una clara delimitación de líneas de responsabilidad y de funciones de todas las áreas involucradas en la asunción, registro y control del riesgo operativo;
- e. Asegurar que permanentemente se revise la actualización de los manuales de organización y funciones y de procedimientos relacionados con la gestión del riesgo operativo;
- f. Designar a los miembros del Comité de Riesgos;
- g. Conformar dentro de la estructura de la entidad supervisada una Unidad de Gestión de Riesgos y designar al responsable de esta Unidad;
- h. Asegurar que la Unidad de Gestión de Riesgos desarrolle sus funciones con absoluta independencia, para lo cual deberá otorgarle un nivel jerárquico cuando menos equivalente al inmediato nivel ejecutivo después de la gerencia general o asignarle dependencia directa del Directorio u Órgano equivalente;
- i. Asegurar que el Comité de Riesgos y la Unidad de Gestión de Riesgos implementen y ejecuten, según corresponda, las disposiciones establecidas en las políticas y procedimientos para la gestión del riesgo operativo;

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

- j. Asumir una actitud proactiva y preventiva frente a la gestión del riesgo operativo y garantizar la efectividad de los mecanismos de difusión de la cultura orientada a la gestión de los riesgos hacia todos los niveles de la estructura organizacional, para lo cual deberá aprobar planes de capacitación dirigidos a todas las áreas y funcionarios de la entidad;
- k. Aprobar la incursión en productos nuevos, operaciones, servicios financieros y actividades, de acuerdo con la estrategia del negocio, las normas legales, estatutarias y las políticas internas;
- l. Aprobar planes de contingencia y de continuidad del negocio para la gestión del riesgo operativo, que permitan a la entidad supervisada una reacción eficaz frente a situaciones adversas;
- m. Aprobar el tratamiento de excepciones temporales a sus políticas cuando corresponda;
- n. Asegurar que la entidad supervisada cuente con sistemas de información que permitan una apropiada gestión del riesgo operativo y que los informes periódicos presentados al Directorio u Órgano equivalente y/o alta gerencia reflejen el perfil de riesgo de la entidad;
- o. Aprobar las metodologías de medición de niveles de exposición para el riesgo operativo;
- p. Evaluar el riesgo operativo asumido por la entidad supervisada, la evolución y el perfil del mismo y las necesidades de cobertura que presenten.

Artículo 3° - (Responsabilidades y funciones de la Gerencia General) La Gerencia General de la entidad supervisada es responsable de implementar y velar por el cumplimiento de la gestión del riesgo operativo y de establecer las acciones preventivas o correctivas que correspondan, para lo cual debe realizar mínimamente las siguientes funciones:

- a. Implementar el sistema de gestión del riesgo operativo, aprobado por el Directorio u Órgano equivalente, que debe ser aplicado a todos los productos nuevos y existentes, procesos y sistemas de la entidad supervisada, optimizando la relación riesgo-retorno;
- b. Asegurar la correcta exposición de la información en los registros contables, en el marco de los lineamientos expuestos en el presente Capítulo;
- c. Implementar y velar por el cumplimiento de los manuales de procedimientos, organización y funciones y otros relacionados con la gestión del riesgo operativo y disponer su permanente revisión y actualización;
- d. Establecer programas de capacitación y actualización sobre gestión del riesgo operativo para el personal de la Unidad de Gestión de Riesgos y para todo aquel involucrado en las operaciones que impliquen a dicho riesgo;
- e. Asegurar el cumplimiento estricto de las disposiciones contenidas en el presente Capítulo.

Artículo 4° - (Responsabilidades y funciones del Comité de Riesgos) El Comité de Riesgos es responsable del diseño de las políticas, sistemas, metodologías, modelos y procedimientos para la eficiente gestión del riesgo operativo y de los límites de exposición a este riesgo.

Este Comité al menos debe cumplir con las siguientes funciones:

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

- a. Diseñar y proponer para la aprobación del Directorio u Órgano equivalente las estrategias, políticas y procedimientos para la gestión del riesgo operativo, considerando las etapas de identificación, medición, monitoreo, control, mitigación y divulgación de riesgos;
- b. Analizar y proponer para la aprobación del Directorio u Órgano equivalente los niveles de exposición al riesgo operativo;
- c. Establecer canales de comunicación efectivos entre las áreas involucradas en la asunción, registro y gestión del riesgo operativo;
- d. Informar periódicamente al Directorio u Órgano equivalente y cuando lo considere conveniente, sobre la exposición al riesgo operativo asumido por la entidad supervisada y los efectos negativos que se podrían producir, así como el cumplimiento de las políticas de este riesgo;
- e. Conocer, evaluar y efectuar seguimiento de las observaciones y recomendaciones que, con distintos motivos, formule la Autoridad de Supervisión del Sistema Financiero;
- f. Informar al Directorio u Órgano equivalente sobre las medidas correctivas implementadas, como efecto de los resultados de las revisiones efectuadas por la Unidad de Auditoría Interna acerca de la gestión del riesgo operativo y/o producto de las observaciones formuladas por la Autoridad de Supervisión del Sistema Financiero;
- g. Evaluar y proponer al Directorio u Órgano equivalente, cuando así se analice y determine el tratamiento de excepciones temporales a sus políticas internas, relacionadas con la gestión del riesgo operativo, las que deben contemplar mecanismos de control;
- h. Proponer al Directorio u Órgano equivalente, mecanismos que aseguren la correcta ejecución de las estrategias, políticas, metodologías, procesos y procedimientos para la gestión del riesgo operativo por parte de la gerencia general y las áreas involucradas;
- i. Proponer al Directorio u Órgano equivalente, sistemas de información gerencial relacionados con la gestión del riesgo operativo, los que deben contemplar reportes de exposición a este riesgo, así como recomendaciones de acciones correctivas si corresponde;
- j. Proponer al Directorio u Órgano equivalente, planes de contingencia y de continuidad del negocio para hacer frente al riesgo operativo en situaciones atípicas.

El Comité debe contar con un Manual de organización y funciones, debiendo las determinaciones adoptadas en las reuniones de este Comité constar en un Libro de Actas, el cual deberá permanecer a disposición de la Autoridad de Supervisión del Sistema Financiero.

La existencia de este Comité no exime de las responsabilidades que, en el proceso de medición, evaluación y control de los riesgos, tienen: el Directorio u Órgano equivalente, la Gerencia General y demás personeros de la entidad supervisada.

Artículo 5° - (Responsabilidades y funciones de la Unidad de Gestión de Riesgos) Esta Unidad es responsable de identificar, medir, monitorear, mitigar, controlar y divulgar el riesgo operativo que enfrenta la entidad supervisada.

Esta Unidad mínimamente debe cumplir las siguientes funciones:

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

- a. Informar al Comité de Riesgos y a las áreas de decisión correspondientes sobre el grado de exposición al riesgo operativo, así como de su administración, de acuerdo a las políticas y procedimientos establecidos;
- b. Desarrollar manuales de procedimientos que contemplen las seis etapas de la gestión del riesgo operativo;
- c. Elaborar con eficiencia y oportunidad los requerimientos de información de la Autoridad de Supervisión del Sistema Financiero;
- d. Coordinar con las áreas operativas y administrativas en lo referente a la correcta identificación, medición, monitoreo, control, mitigación y divulgación del riesgo operativo asumido por la entidad supervisada;
- e. Difundir la cultura de gestión del riesgo operativo en toda la estructura organizacional de la entidad supervisada, estableciendo un lenguaje común basado en las definiciones del presente Capítulo;
- f. Apoyar al Comité de Riesgos en el diseño y desarrollo de políticas para la gestión del riesgo operativo, de acuerdo con los lineamientos que fije el Directorio u Órgano equivalente de la entidad supervisada;
- g. Elaborar y someter a consideración del Comité de Riesgos las metodologías a ser utilizadas en las diferentes etapas del proceso de gestión del riesgo operativo;
- h. Realizar las pruebas necesarias a los planes de contingencias y de continuidad del negocio y remitir al Directorio u Órgano equivalente a través del Comité de Riesgos un informe que contenga el resultado de dichas pruebas;
- i. Investigar, documentar y evaluar las causas que originan desviaciones a las políticas internas, e identificar si éstas se presentan en forma recurrente, debiendo informar de manera oportuna sus resultados al Comité de Riesgos;
- j. Diseñar y someter a consideración del Comité de Riesgos un sistema de información gerencial para uso interno de la entidad supervisada, que refleje su perfil de riesgo;
- k. Proporcionar al Comité de Riesgos, Gerente General, gerentes de las áreas de negocios y demás instancias pertinentes, la evolución histórica de los niveles de exposición al riesgo operativo asumidos por la entidad supervisada;
- l. Establecer un Plan de Trabajo para revisiones anuales y evaluaciones más frecuentes de las políticas y procedimientos a fin de que las mismas respondan a su evolución y modelo de negocios;
- m. Verificar que el inventario de procesos se encuentre actualizado y señalar la existencia de procesos críticos en los cuales se hubiesen identificado debilidades;
- n. Realizar el seguimiento a la implementación de acciones correctivas ante los eventos de riesgo operativo reportados a la Central de Información de Riesgo Operativo.

Artículo 6° - (Requisitos de los integrantes del Comité de Riesgos y de la Unidad de Gestión de Riesgos) Los integrantes del Comité de Riesgos, así como los funcionarios de la Unidad de

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

Gestión de Riesgos, deben contar con formación profesional, conocimientos y experiencia que les permitan el apropiado cumplimiento de sus funciones.

No podrán ser integrantes de estos órganos quienes estén incluidos en alguna situación que genere conflicto de interés o que limite su independencia.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS**SECCIÓN 5: REGISTRO DE EVENTOS DE RIESGO OPERATIVO**

Artículo 1° - (Categorización de eventos de riesgo operativo) La entidad supervisada como parte de la gestión del riesgo operativo que realiza, debe efectuar la clasificación de los eventos sujetos a este riesgo, considerando a tal efecto los siguientes criterios:

- a. Eventos de riesgo operativo que generan pérdidas y afectan el Estado de Ganancias y Pérdidas;
- b. Eventos de riesgo operativo que generan pérdidas y no afectan el Estado de Ganancias y Pérdidas;
- c. Eventos de riesgo operativo que no generan pérdidas y no afectan el Estado de Ganancias y Pérdidas.

Artículo 2° - (Eventos de pérdida) La entidad supervisada a efectos de establecer el origen de la pérdida generada por eventos de riesgo operativo debe agrupar los mismos de acuerdo a los siguientes tipos:

- a. Clientes, productos y prácticas empresariales;
- b. Daños a activos materiales;
- c. Ejecución, entrega y gestión de procesos;
- d. Fraude externo;
- e. Fraude interno;
- f. Incidencias en el negocio y fallos en los sistemas;
- g. Relaciones laborales y seguridad en el puesto de trabajo.

El historial de eventos de pérdidas por riesgo operativo debe estar debidamente documentado, por la entidad supervisada.

Artículo 3° - (Líneas de negocios) La entidad supervisada debe contar con un detalle de los procesos que se encuentran agrupados en cada línea de negocio determinada, de acuerdo a sus políticas, a efectos de realizar el registro de eventos de riesgo operativo. La asignación de los procesos debe considerar mínimamente lo siguiente:

- a. Todos los procesos deben estar asignados entre las líneas de negocios definidas por la entidad supervisada;
- b. Cada proceso debe estar asociado a una sola línea de negocio;
- c. Cuando un proceso apoye a más de una línea de negocio la entidad supervisada debe establecer criterios formales de asignación.

Artículo 4° - (Clasificación de eventos en líneas de negocio) Para el registro de eventos de riesgo operativo y de pérdida en relación a una línea de negocio la entidad supervisada debe considerar los siguientes criterios:

- a. Los eventos de riesgo operativo se registran en la línea de negocio que corresponde a la actividad principal, a la cual se asocian;

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

- b. Los eventos de pérdida que involucren a más de una línea de negocio, deben ser reportados en aquella línea que se vea más afectada con la pérdida producida;
- c. Cuando un evento de pérdida afecte a más de una línea de negocio en la misma proporción, se debe asignar el valor de la pérdida que corresponde a cada línea de negocio involucrada.

Artículo 5° - (Base de datos de eventos de riesgo operativo) La entidad supervisada debe mantener una base de datos histórica de eventos de riesgo operativo, que considere los criterios establecidos en el [Artículo 4°, Sección 2](#) del presente Capítulo y en los [Artículos 1°, 2°, 3° y 4°](#) precedentes.

La citada base de datos debe ser reportada a la Central de Información de Riesgo Operativo (CIRO) en el marco de lo dispuesto en el Artículo 480 de la Ley N° 393 de Servicios Financieros, de acuerdo lo establecido en el [Manual de Envío de Información Electrónica a la Central de Información de Riesgo Operativo](#) de la Autoridad de Supervisión del Sistema Financiero.

Artículo 6° - (Seguimiento de eventos de riesgo operativo) La entidad supervisada, con base en el registro de eventos de riesgo operativo debe adoptar medidas correctivas oportunas tendientes a asegurar una rápida, efectiva y ordenada respuesta a los mismos.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS**SECCIÓN 6: SISTEMAS DE INFORMACIÓN PARA LA GESTIÓN DEL RIESGO OPERATIVO**

Artículo 1° - (Sistemas de información) La entidad supervisada debe desarrollar e implementar sistemas de información y mecanismos de divulgación que le permitan una adecuada gestión del riesgo operativo.

Todos los niveles de la organización, dentro de sus competencias y de acuerdo con sus políticas para el tratamiento de la información, deben hacer seguimiento sistemático de las exposiciones del riesgo operativo y de los resultados de las acciones adoptadas, lo cual significa un monitoreo permanente a través de un sistema de información.

Estos sistemas mantendrán información suficiente para apoyar los procesos de toma de decisiones, que permita la generación de informes permanentes, oportunos, objetivos, relevantes, consistentes y dirigidos a los correspondientes niveles de la administración.

Los sistemas de información deben contar con información histórica que asegure una revisión periódica, continua y objetiva de su perfil de riesgo, así como de la existencia de eventuales excepciones si corresponde.

Artículo 2° - (Reportes de información) La entidad supervisada a través de su sistema de información debe desarrollar e implementar informes y reportes efectivos, comprensivos y oportunos que le permitan una eficiente gestión del riesgo operativo, los cuales deben considerar las diferentes instancias y áreas involucradas en la administración del mismo, así como la frecuencia que deben tener los reportes diseñados.

El sistema de información de la entidad supervisada debe generar la información para la Central de Información de Riesgo Operativo (CIRO), misma que debe ser remitida a la Autoridad de Supervisión del Sistema Financiero (ASFI) a través del Sistema de Captura de Información Periódica (SCIP), el cual provee los mecanismos que permiten la carga, validación de consistencia y envío de dicha información.

Esta información debe ser reportada bajo la estructura de archivo y formatos definidos en el [Manual de Envío de Información Electrónica a la CIRO](#), emitido por ASFI, en el plazo dispuesto en el [Reglamento para el Envío de Información](#) de la Recopilación de Normas para Servicios Financieros.

Artículo 3° - (Reporte de eventos críticos) La entidad supervisada debe comunicar a ASFI todo evento crítico en el día de ocurrido el mismo, a través del SCIP bajo la misma estructura de reporte a la CIRO, remitiendo además, hasta el siguiente día hábil administrativo de sucedido el citado evento, un informe impreso que detalle lo acontecido e indique las medidas que fueron adoptadas.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

SECCIÓN 7: ROL DE LA UNIDAD DE AUDITORÍA INTERNA

Artículo Único - (Control Interno) La Unidad de Auditoría Interna es un elemento clave en la gestión del riesgo operativo, debiendo, mínimamente, cumplir con las siguientes funciones:

- a. Verificar que tanto las áreas comerciales, operativas y financieras como la Unidad de Gestión de Riesgos, hayan ejecutado correctamente las estrategias, políticas y procedimientos aprobados por el Directorio u Órgano equivalente, para la gestión del riesgo operativo;
- b. Verificar que el personal involucrado en la administración del riesgo operativo entienda completamente las políticas y que tenga la experiencia requerida para tomar decisiones efectivas y consistentes con dichas políticas;
- c. Verificar el correcto registro de la información utilizada para monitorear y controlar este riesgo, así como el registro de la base de datos de eventos de riesgo operativo;
- d. Realizar una revisión del cumplimiento de las obligaciones y responsabilidades encomendadas a la Unidad de Gestión de Riesgos;
- e. Elevar informes al Directorio u Órgano equivalente, a través de su Comité de Auditoría o Consejo de Vigilancia según corresponda, acerca de los resultados obtenidos y las recomendaciones sugeridas, derivadas de sus revisiones;
- f. Efectuar seguimiento de las observaciones y/o recomendaciones emitidas a las diferentes áreas y comunicar los resultados obtenidos al Directorio u Órgano equivalente, a través de su Comité de Auditoría o Consejo de Vigilancia según corresponda.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

SECCIÓN 8: OTRAS DISPOSICIONES

Artículo 1° - (Responsabilidad) Es responsabilidad del Gerente General de la entidad supervisada, el cumplimiento y difusión interna del presente Capítulo.

Artículo 2° - (Sanciones) El incumplimiento o inobservancia a la presente norma dará lugar al inicio del proceso administrativo sancionatorio.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS**SECCIÓN 9: DISPOSICIONES TRANSITORIAS**

Artículo 1° - (Plazo de adecuación) La entidad supervisada, debe adecuar, hasta el 31 de diciembre de 2014, sus estrategias, políticas, procedimientos, manuales, estructura organizativa y sistemas de información, de acuerdo a lo dispuesto en el presente Capítulo

Artículo 2° - (Reporte de líneas de negocios) A efectos de iniciar la fase de reporte de información a la [Autoridad de Supervisión del Sistema Financiero](#), la entidad supervisada debe remitir hasta el 30 de enero de 2015, el detalle de líneas de negocios y procesos asociadas a las mismas, que fueron identificados en el marco de lo establecido en el [Artículo 3°, Sección 5](#) de la presente norma.

Artículo 3° - (Central de información de riesgo operativo) Una vez cumplidas las disposiciones transitorias señaladas en los artículos precedentes, la Autoridad de Supervisión del Sistema Financiero comunicará a través de Carta Circular a las entidades supervisadas los lineamientos y la fecha a partir de la cual, deben iniciar el reporte de la información de la base de datos de eventos de riesgo operativo a la Central de Información de Riesgo Operativo, señalada en el [Artículo 5°, Sección 5](#) del presente Capítulo.

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS**CONTROL DE VERSIONES**

L03T05C02		Secciones									Anexo 1
Circular	Fecha	1	2	3	4	5	6	7	8	9	
ASFI/514/2018 ¹	08/01/2018	*		*	*	*	*			*	*
ASFI/358/2015	14/12/2015	*									
ASFI/207/2013	04/12/2013	*	*	*	*	*	*	*	*	*	*

¹ Se eliminó el Anexo 1.