

Marco para la Gestión del Riesgo Operacional

Fecha: 31/01/2026

Índice

1.	CONCEPTOS Y DEFINICIONES	3
1.1.	Riesgo Operacional	3
1.2.	Gestión del riesgo operacional	3
1.3.	Eventos de pérdidas.....	4
1.4.	Marco para la gestión del riesgo operacional.....	4
1.5.	Estrategia	5
1.6.	Políticas.....	5
1.7.	Estructura organizacional	5
2.	ESTRATEGIA	6
3.	POLÍTICAS	6
4.	PROCESO	7
4.1.	Identificación y evaluación	7
4.2.	Control y Mitigación	11
4.3.	Seguimiento.....	11
5.	ESTRUCTURA ORGANIZACIONAL Y RESPONSABILIDADES	12
5.1.	Directorio.....	13
5.2.	Alta Gerencia.....	13
5.3.	Compliance and Risk Management.....	14
5.4.	Comité de Gestión Integral de Riesgos.....	16
5.5.	Gerencias.....	17
5.6.	Auditoría interna.....	17
6.	COBERTURA DEL RIESGO OPERACIONAL.....	17
7.	PLANES DE CONTINGENCIA	18
8.	APROBACIONES Y MODIFICACIONES.....	19

1. CONCEPTOS Y DEFINICIONES

1.1. Riesgo Operacional

Se entiende por riesgo operacional al riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, de la actuación del personal o de los sistemas o bien aquellas que sean producto de eventos externos. Este concepto incluye el riesgo legal, el riesgo informático, y excluye el riesgo estratégico y de reputación.

El riesgo legal, que puede verificarse en forma endógena o exógena a la entidad financiera, comprende, entre otros aspectos, la exposición a sanciones, penalidades u otras consecuencias económicas y de otra índole por incumplimiento de leyes, reglas, normas y prácticas y obligaciones contractuales, o cuando los derechos y obligaciones legales de las partes respecto a una transacción no están bien establecidos.

El riesgo informático es el que se deriva de la vulnerabilidad y amenazas a las que se encuentran expuestos los activos informáticos. Estos activos incluyen la información, los sistemas aplicativos que se utilizan para operarla y los servidores y otros elementos de arquitectura donde se alojan y comunican.

Se define por riesgo estratégico al procedente de una estrategia de negocios inadecuada o de un cambio adverso en las previsiones, parámetros, objetivos y otras funciones que respaldan esa estrategia. *(Ver Marco para la Gestión del Riesgo Estratégico)*

Se define por riesgo de reputación a la posibilidad de que se produzca una pérdida debido, entre otros casos, a la formación de una opinión pública negativa sobre los servicios prestados por la entidad financiera -fundada o infundada-, que fomente la creación de una mala imagen o un posicionamiento negativo de los clientes, que conlleve a una disminución del volumen de clientes, a la caída de los ingresos, de los depósitos, etc. *(Ver Marco para la Gestión del Riesgo Reputacional)*

1.2. Gestión del riesgo operacional

La gestión del riesgo operacional es el proceso de identificación, evaluación, seguimiento, control y mitigación que involucra diversas etapas, entre ellas, evaluar su vulnerabilidad ante los eventos, para así comprender mejor su perfil de riesgo operacional y, en su caso, adoptar las medidas correctivas que sean pertinentes y la planificación para las contingencias.

1.3. Eventos de pérdidas

Los conceptos que integran eventos de pérdida a modo enunciativo son:

1. Fraude interno: información falsa sobre posiciones -propias o de clientes-, robos por parte de empleados, utilización de información confidencial de la entidad financiera en beneficio del empleado, etc.
2. Fraude externo: robo, falsificación, daños por intromisión en los sistemas informáticos, etc.
3. Relaciones laborales y seguridad en el puesto de trabajo: reclamos de indemnizaciones por parte de los empleados, infracciones a las normas laborales de seguridad e higiene, de discriminación, responsabilidades generales, etc.
4. Prácticas con los clientes, productos y negocios: abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas de la entidad financiera, lavado de dinero, venta de productos no autorizados, etc.
5. Daños a activos físicos derivados de: actos de terrorismo y vandalismo, terremotos, incendios, inundaciones, etc.
6. Alteraciones en la actividad y fallas tecnológicas: fallas del “hardware” o del “software”, problemas en las telecomunicaciones, interrupción en la prestación de servicios públicos, etc.
7. Ejecución, gestión y cumplimiento del plazo de los procesos: errores en la introducción de datos, fallas en la administración de garantías, documentación jurídica incompleta, concesión de acceso no autorizado a las cuentas de los clientes, litigios con proveedores, etc.

1.4. Marco para la gestión del riesgo operacional

El marco para la gestión del riesgo de operacional incluye la estrategia, la política, estructura organizacional y responsabilidades con las que cuenta Banco CMF S.A. para una adecuada administración de este riesgo.

Dicho marco es proporcional a la dimensión de Banco CMF S.A. y a la naturaleza y complejidad de sus operaciones. Engloba a todos los riesgos de carácter operacional, contempla una estrategia que comprende el enfoque general sobre dichos riesgos. Aplica tanto a Banco CMF S.A. como a sus compañías subsidiarias.

Los principios básicos y las técnicas empíricas utilizadas para cuantificar el riesgo operacional se encuentran contenidas en el presente documento marco.

Banco CMF S.A. cuenta con un proceso para identificar, evaluar, seguir, controlar y mitigar el riesgo operacional, en el marco de un conjunto documentado de políticas, controles y procedimientos internos relativos al funcionamiento del sistema de gestión del riesgo de operacional, el cual es llevado a cabo por Compliance and Risk Management.

1.5. Estrategia

La estrategia de gestión del riesgo operacional es el enfoque general que aplica Banco CMF S.A. para administrar este riesgo, la cual fija políticas y prácticas adecuadas, contemplando el objetivo de control y reducción de riesgos operacionales, el nivel de tolerancia al riesgo establecido y la capacidad para realizar los ajustes que pudieran corresponder.

1.6. Políticas

Banco CMF S.A. cuenta con un proceso adecuado para identificar, evaluar, seguir, controlar y mitigar el riesgo operacional, que garantiza el cumplimiento de un conjunto documentado de políticas, controles y procedimientos internos relativos al funcionamiento del sistema de gestión del riesgo operacional, el cual es llevado a cabo por Compliance and Risk Management.

Las políticas incluyen los siguientes elementos:

- Especificación de factores de riesgo operacional
- Estructura organizativa y responsabilidades
- Registro de eventos
- Auto-evaluación del riesgo operacional
- Asignación de riesgos o mapeo de riesgos
- Indicadores de riesgo
- Reportes para monitoreo
- Programas de cobertura
- Planificación para la contingencia y de continuidad de la actividad

1.7. Estructura organizacional

La estructura organizacional de Banco CMF S.A. consiste en el esquema de roles y responsabilidades asignados a los funcionarios de la entidad, a través de los cuales se hace posible implementar la estrategia definida y contempla la asignación de la responsabilidad de gestionar el riesgo operacional a Compliance and Risk Management. Dicha área es independiente de las gerencias operativas del banco.

2. ESTRATEGIA

La estrategia de gestión de Riesgo Operacional de Banco CMF S.A. reposa principalmente en su capital humano, altamente capacitado y confiable. Por su parte, la operatoria bancaria se desenvuelve en el marco de manuales y procedimientos para sus operaciones. La articulación de ambos pilares se basa en una clara asignación de responsabilidades y segregación de funciones.

Se promueve persistentemente una cultura fuertemente inclinada a los controles internos que salvaguarde la eficiente gestión de Riesgo Operacional aún cuando el ambiente de negocios cambie a mayor velocidad que la actualización de los manuales.

El umbral de tolerancia a los eventos de Riesgo Operacional es mínimo para lo cual se realizan procesos permanentes de sensibilización a los funcionarios.

3. POLÍTICAS

Banco CMF S.A. implementa el modelo de gestión del riesgo operacional a través de un conjunto de políticas, procedimientos, y asignación de responsabilidades que se focalizan en la identificación, evaluación, seguimiento, control y mitigación de eventos o fallas de ese tipo de riesgo.

El modelo de gestión del riesgo operacional compromete de manera integral a la organización.

Su naturaleza "integral" obedece a una serie de factores:

- La secuencia concatenada de tareas, desde la identificación de los riesgos, hasta la medición, seguimiento, control y mitigación, círculo virtuoso que asegura que luego de sucesivos ciclos efectivos se logre ubicar a los factores de riesgos en niveles aceptables para Banco CMF S.A., así como también capturar situaciones nuevas que merezcan ser analizadas (por ej.: lanzamiento de nuevos productos).
- La necesaria evaluación de todos los procesos que reflejan la operatoria de Banco CMF S.A., desde el frente de negocios y el back office, hasta los servicios de apoyo.
- La incumbencia de todo el staff, desde la línea gerencial hasta todo su personal, en su gestión. De allí, la importancia de la difusión y comunicación a lo largo y ancho de la organización que permita el acabado entendimiento y asegure el necesario compromiso de todas las partes de acuerdo con sus responsabilidades.

4. PROCESO

La gestión efectiva del riesgo operacional contribuye a prevenir futuras pérdidas derivadas e inherentes a estos eventos. En este sentido Banco CMF S.A. gestiona el riesgo operacional inherente a sus productos, actividades, procesos y sistemas relevantes, basado en los lineamientos establecidos en su marco normativo (marco, proceso y metodología de gestión de riesgo operacional), y con el soporte de la herramienta Aleph Manager.

Asimismo, y en forma previa a un lanzamiento o presentación de nuevos productos, inicio de actividades, puesta en marcha de procesos o sistemas, también deberán comprobar que se evalúa adecuadamente su riesgo operacional inherente.

El proceso de gestión del riesgo operacional de Banco CMF S.A. comprende las siguientes etapas:

4.1. Identificación y evaluación

Para la identificación del riesgo operacional, se tienen en cuenta factores que pudieran afectar el desarrollo de los procesos e influir negativamente en las proyecciones realizadas conforme a las estrategias de negocios definidas por Banco CMF S.A.

- Factores de carácter internos: como, la estructura de la entidad financiera y la naturaleza de sus actividades.
- Factores de carácter externos: como, cambios en el sector y avances tecnológicos, etc.

Se utilizan datos internos, debiendo establecer un proceso para registrar y consignar en forma sistemática la frecuencia, severidad, categorías y otros aspectos relevantes de los eventos de pérdida por riesgo operacional.

Registro de eventos:

La registración de esos eventos contribuye a reducir los incidentes, las pérdidas y a mejorar la calidad del servicio y de los productos.

En base a los resultados que arrojen todas las herramientas se registran eventos identificados y/o riesgos no materializados que por su naturaleza no se puedan dejar de monitorear en forma constante.

Los eventos se clasifican dentro de las principales fuentes causales de Riesgo Operacional, las cuales se detallan a continuación en categorías y subcategorías:

- Categoría: Organización
 - Subcategorías: Ambiente-Cultura Organizacional, Controles Internos, Misiones- Funciones-Organigrama, Políticas-Manuales- Procedimientos.
- Categoría: Recursos Humanos
 - Subcategorías: Beneficios, Capacitación, Evaluación de Desempeño, Prácticas laborales, Remuneraciones.
- Categoría: Instalaciones
 - Subcategorías: Circuitos Cerrados de Televisión (CCTV), Edificio, Lay out, Seguridad.
- Categoría: Sistemas
 - Subcategorías: Desarrollo, Producción, Seguridad Informática.
- Categoría: Factores Externos

Los eventos se miden cualitativamente de acuerdo a su probabilidad e impacto.

Clasificación de eventos de Riesgo Operacional.

Cada evento se clasifica de acuerdo a las 7 categorías de riesgo definidas por las mejores prácticas internacionales y el marco regulatorio vigente, tal como se detalló en el punto 1.3. “Eventos de Pérdidas”.

Recolección de datos:

El proceso de recolección de datos permite fomentar su registración, promoviendo de este modo una cultura organizacional para el reporte de tales datos y de controles que contribuyan a la verificación de su consistencia e integridad.

Herramientas para identificar y evaluar sus riesgos operacionales:

En la gestión de Riesgo Operacional se utilizan una serie de herramientas que permiten alcanzar eficiente y eficazmente los objetivos de la gestión de riesgo operacional.

Las herramientas sirven de soporte para la toma de decisiones y se enumeran a continuación:

- Auto-evaluación.
- Matriz de Riesgo Operacional.
- Base de Datos de Pérdida Operacional.
- Indicadores de Riesgo Operacional.
- Seguimiento de planes de acción.

Las citadas herramientas permiten obtener información para análisis, impulsar acciones de información periódica o revisiones a los planes de acción correctivos, siempre en permanente contacto con las áreas de negocios (Gerencias) y la Alta Gerencia (Gerencia General).

- **Auto-evaluación**

Desarrolla un proceso interno que conlleva la utilización de listas de control o de grupos de trabajo para identificar fortalezas y debilidades del entorno de riesgo operacional.

La Auto-evaluación por parte de las Gerencias y el personal del Banco para la identificación y notificación de eventos de Riesgo Operacional es fundamental, a la vez que esto fortalece los mecanismos para la identificación y evaluación de los riesgos.

Las actividades de auto-evaluación buscan la retrospección de las actividades llevadas a cabo en períodos anteriores que provean elementos para fundamentar las distintas etapas del proceso permitiendo detectar tanto fortalezas como debilidades del entorno operacional en lo relativo a riesgo.

En este proceso de Auto-evaluación el responsable de los procesos y subprocesos para los que se han identificado eventos de Riesgo Operacional, debe evaluarlos y comunicarlos.

- **Matriz de Riesgo Operacional**

La matriz de Riesgo Operacional es una representación gráfica de los eventos de riesgo o probables fallas operativas de Banco CMF S.A. en un momento determinado para cada proceso, y refleja la probabilidad de que ocurran, así como también el impacto en el negocio del Banco en caso que la ocurrencia se verifique.

La severidad de los riesgos, sienta las bases para el impulso de las acciones de administración de riesgos que correspondan.

La evaluación de riesgo recae en cada Gerencia/Área, asesorada antes, durante y después por Compliance and Risk Management. La evaluación se hace en forma cualitativa, se asignan cuatro categorías de probabilidad (común, frecuente, ocasional, raro) y cuatro de impacto (bajo, moderadamente bajo, moderadamente alto y alto).

En base a la evaluación visualizada en la Matriz de Riesgo Operacional, el Banco puede distinguir entre riesgos aceptables, tolerables, moderados, importantes / inaceptables, a la vez que se evalúa el nivel de probabilidad y el nivel de impacto.

La evaluación de cada evento de riesgo posibilita el diseño de acciones que mejor se ajusten a sus umbrales de riesgo.

- **Base de Datos de Pérdida Operacional**

La Base de Datos de Pérdida Operacional es un soporte informático que reúne las pérdidas operacionales registradas, más los elementos que permitan evaluar de manera completa el evento ocurrido, razón por la cual, requiere fuentes de información adicionales al sistema contable.

Las pérdidas operacionales son eventos ocurridos que generan una pérdida efectiva para el Banco y son capturados por la contabilidad.

La información contenida en la Base de Datos de Pérdida Operacional se utilizará para la obtención de estadísticas que permitan evaluar la frecuencia, causalidad e impacto de los riesgos a los que está expuesto. La Base de Datos de Pérdida Operacional es una herramienta fundamental para poder establecer planes para la mitigación de los riesgos operacionales ya que provee de manera objetiva y detallada el historial en la materia.

La construcción de una base de datos interna conlleva la posibilidad de tomar conciencia de las exposiciones a los riesgos y sus consecuencias negativas para la organización, la cuantificación de la exposición de manera de focalizar más eficientemente los recursos para su mitigación y la provisión de información rica para el entendimiento de las causas básicas que ocasionaron los eventos.

- **Indicadores de Riesgo Operacional**

Los indicadores de Riesgo Operacional reflejan las fuentes potenciales de este riesgo, tales como una expansión acelerada, el lanzamiento de nuevos productos, la rotación del personal, interrupciones en las operaciones o en los sistemas, etc.

Los Indicadores de Riesgo Operacional son mediciones de variables representativas de eventos de riesgo que podrían ocasionar pérdidas operacionales para Banco CMF S.A.

Los indicadores permiten obtener información periódica de los posibles eventos que pudieran materializar riesgos operacionales facilitando el proceso de establecimiento e implementación de acciones correctivas. Además, se utilizan para verificar la eficacia de los planes de acción implementados.

Mientras que la Base de Datos de Pérdida Operacional recoge pérdidas efectivamente incurridas por el banco, los Indicadores de Riesgo Operacional dan información sobre potenciales riesgos.

Mediante mediciones periódicas, los Indicadores de Riesgo Operacional avisan con antelación los eventos que aumentan el riesgo de pérdidas. Actúan como modo de alertas tempranas de potenciales fuentes de Riesgo Operacional.

4.2. Control y Mitigación

La etapa de Control y Mitigación tiene por objetivo el establecimiento de mecanismos para el control y reducción de riesgos operacionales.

El monitoreo y mitigación buscan establecer procesos y procedimientos de control y contar con un marco que asegure el cumplimiento de las políticas internas reexaminando con una frecuencia mínima anual las estrategias de control y reducción de riesgos operacionales, debiendo realizar los ajustes que pudieran corresponder.

Comprende el diseño de planes de acción que puedan utilizarse para reducir la exposición a riesgos operacionales, ya sea corrigiendo modalidades operativas débiles o inadecuadas o bien contratando seguros o modificando cláusulas contractuales, etc.

4.3. Seguimiento

Se cuenta con un proceso de seguimiento a los efectos de facilitar la rápida detección y corrección de las posibles deficiencias que se produzcan en sus políticas, procesos y procedimientos de gestión del riesgo operacional.

Este proceso se inserta en las actividades habituales de la entidad financiera.

Además del seguimiento de los eventos de pérdidas operativas, se monitorea la evolución de los indicadores a los fines de evaluar la necesidad de reformularlos, o diseñar planes de acción, en función de la naturaleza de los eventos de pérdida producidos.

La etapa de Seguimiento se basa en el rastreo permanente del proceso de manera de posibilitar la introducción de actualizaciones o correcciones a las políticas, procesos y procedimientos de gestión de Riesgo Operacional.

Banco CMF S.A. cuenta con reportes específicos de seguimiento que permitan identificar de manera temprana las pérdidas operativas y/o los cursos de acción a seguir internamente y con las contrapartes.

Compliance and Risk Management (conforme la dimensión, la naturaleza y complejidad de sus productos y procesos y con la magnitud de sus operaciones) emiten reportes vinculados a los resultados del seguimiento realizado y las pertinentes propuestas de corrección en los procesos y procedimientos. Los reportes son consolidados por Compliance and Risk Management en el Panel de Gestión de Riesgos, para su análisis conjunto con la información relativa al resto de los riesgos del banco. Esto se realiza a los efectos de su presentación mensual en el Comité de Gestión Integral de Riesgos. La información tratada en el Comité, así como las decisiones tomadas por el mismo, son tratadas posteriormente en reunión de Directorio para su toma de conocimiento.

Dichos informes, una vez analizados por la Gerencia General, se distribuyen entre los niveles gerenciales correspondientes y las áreas de la entidad financiera que pudieran verse afectadas, a fin de que adopten esas medidas correctivas para asegurar una gestión eficaz del riesgo operacional.

5. ESTRUCTURA ORGANIZACIONAL Y RESPONSABILIDADES

Toda la organización debe estar involucrada en la gestión del Riesgo Operacional. Sin embargo, dependiendo de sus funciones y responsabilidades asignadas, la contribución al proceso es distinta.

Todo el staff, Gerencias y personal, debe comprender y estar comprometido con el objetivo de mantener el Riesgo Operacional en los umbrales de tolerancia y estar alerta ante eventuales cambios que pudieran surgir, y en consecuencia, afectar los criterios puestos en práctica.

La cultura organizacional debe estar fuertemente apegada a la cultura de controles internos y a su vez debe asimilar de manera positiva y como un aprendizaje, los reportes de eventos de Riesgo Operacional que se verifiquen.

El Directorio, la Alta Gerencia y Compliance and Risk Management deberán evidenciar un alto grado de compromiso tendiente a mantener una sólida cultura de la gestión del riesgo operacional en la cual las actividades relacionadas con ese riesgo formen parte de los procesos diarios de la entidad financiera.

El Directorio de Banco CMF S.A., es un órgano comprometido en la definición y monitoreo de los riesgos asumidos. Delega su administración en órganos separados e independientes. El Directorio y la Alta Gerencia están involucrados en el seguimiento de la administración, puesto que participan en cada uno de los comités (Comité de Gestión Integral de Riesgos).

El Directorio será responsable que la entidad cuente con una estrategia adecuada para la gestión del riesgo operacional asumido por la entidad y de la forma en que se gestiona.

El responsable de la gestión de riesgo operacional en el Banco CMF S.A. es Compliance and Risk Management que reporta al Gerente General.

Compliance and Risk Management podrá involucrar a personal de otras áreas siempre que las responsabilidades asignadas no impliquen conflictos de intereses en función de las respectivas incumbencias. Asimismo, existirá independencia entre el responsable de Riesgo Operacional y las unidades de negocio involucradas, así como una clara delimitación de funciones, responsabilidades y perfil de puestos en todos sus niveles.

5.1. Directorio

Respecto del Riesgo Operacional, el Directorio será responsable de:

- Aprobar el marco que se utilizará para la gestión del riesgo operacional cuya periodicidad mínima de revisión será anual o cada vez que se produzcan, a juicio de la entidad, hechos o situaciones de relevancia vinculadas con este riesgo, los cuales deberán ser puestos en conocimiento de la Superintendencia de Entidades Financieras y Cambiarias.
- Tener un claro conocimiento de los procedimientos desarrollados a efectos de gestionar el riesgo operacional y su grado de cumplimiento. Para ello deberá recibir, como mínimo semestralmente, información suficiente que permita analizar el perfil de riesgo operacional general de la entidad financiera y verificar las implicancias estratégicas y sustanciales para su actividad.
- Asegurar que el marco para la gestión del riesgo operacional esté sujeto a un proceso de auditoría interna -área que no será responsable de su gestión- que contemple una adecuada cobertura y profundidad de las revisiones y la adopción oportuna de medidas correctivas por parte de las áreas auditadas.
- Aprobar políticas de difusión del marco de gestión del riesgo operacional y de capacitación, dirigidas a todas las áreas y funcionarios de la entidad financiera.
- Establecer políticas para la gestión de los riesgos operacionales derivados de las actividades subcontratadas y de los servicios prestados por los proveedores.
- Aprobar una política para la difusión a terceros de la información que corresponda sobre el marco de gestión del riesgo operacional. El contenido de dicha información y sus características serán proporcionales al volumen, complejidad y perfil de riesgo de las operaciones de la entidad financiera.
- Garantizar que la entidad cuente con personal técnicamente calificado, así como también con los recursos necesarios para la gestión del riesgo operacional.
- Verificar que Compliance and Risk Management no desarrolle otras tareas en áreas que puedan generar conflictos de intereses con su función.

5.2. Alta Gerencia

La Alta Gerencia es la responsable de implementar la estrategia para la gestión del riesgo operacional y de las políticas y prácticas aprobadas por el Directorio. A esta instancia le corresponde elaborar procedimientos escritos para identificar, evaluar, seguir, controlar y mitigar este riesgo.

- Será la responsable de la implementación, reporte y control de los procesos y procedimientos para la puesta en práctica y funcionamiento del marco de gestión aprobado por el Directorio de Banco CMF S.A.

El marco de gestión será aplicado en forma consistente en toda la entidad financiera, debiendo todos los niveles de la organización comprender sus responsabilidades con respecto a la administración del riesgo operacional.

- Será la encargada de que existan procesos y procedimientos aplicables a cada unidad de negocio, destinados a la gestión del riesgo operacional de los productos, actividades, procesos y sistemas de la entidad financiera.
- Deberá establecer líneas claras de autoridad, responsabilidad y comunicación con las distintas gerencias para fomentar y mantener la asunción de responsabilidades.
- Asegurará la existencia de recursos suficientes para la realización de una gestión eficaz del riesgo operacional.
- Deberá evaluar si el proceso de vigilancia gerencial se adapta a los riesgos inherentes a las políticas de cada unidad de negocio.
- Recibirá informes de la Compliance and Risk Management con los resultados de la ejecución de los procesos y procedimientos, la detección de las posibles deficiencias que se produzcan en las políticas, procesos y procedimientos de gestión del riesgo operacional y las pertinentes propuestas para su corrección.

Se establecerá la periodicidad de los citados informes de acuerdo con su dimensión, la naturaleza y complejidad de sus productos y procesos y con la magnitud de sus operaciones.

- Informará al Directorio, como mínimo semestralmente, sobre los principales aspectos relacionados con la gestión del riesgo operacional.

5.3. Compliance and Risk Management

Esta área depende directamente de la Gerencia General.

Compliance and Risk Management articula los principales procesos que la entidad financiera necesita para gestionar el riesgo operacional, adoptando los mecanismos que permitan una comunicación, interacción y coordinación efectiva con los responsables de los otros riesgos que tenga la entidad conforme sus definiciones y los requerimientos del Banco Central de la República Argentina y de los responsables de contratar servicios externos.

Adicionalmente, reúne información concerniente a la gestión y al monitoreo del Riesgo Operacional y reporta a la Gerencia General y al Comité de Gestión Integral de Riesgos.

Las responsabilidades de la Compliance and Risk Management son:

- Desarrollar políticas, prácticas y procedimientos vinculados al riesgo operacional.
- Llevar a cabo la ronda anual de autoevaluación por parte de cada Gerencia/Área, en cuanto a sus riesgos operativos, según los procedimientos aprobados, documentados en el marco normativo de gestión de riesgo operacional (marco, proceso y metodología).
- Compilar la información de todas las áreas para la generación de las matrices de riesgo, a través de la herramienta automatizada que le sirve de soporte.
- Informar a la Gerencia General el resultado de las matrices de riesgo confeccionadas.
- Coordinar con las respectivas gerencias la generación y documentación de los planes de mitigación para los riesgos a mitigar, seleccionados en conjunto con la Gerencia General y aprobados por el Directorio.
- Efectuar el control y seguimiento de la ejecución de los planes de mitigación.
- Definir y controlar el seguimiento del desarrollo de herramientas necesarias para brindar soporte a sus funciones.
- Elaborar los indicadores de riesgo (KRI "Key Risk Indicator), para la medición de riesgos operativos a informar al B.C.R.A.
- Coordinar con Auditoría Interna el cumplimiento de las normas que surjan de los planes de mitigación.
- Generar el presupuesto anual y planes para su área. Desarrollar el seguimiento y control de los planes.
- Recibir de las Gerencias informes con los resultados de la ejecución de los procesos y procedimientos, con la periodicidad que Banco CMF S.A. establece de acuerdo a la dimensión, naturaleza y complejidad de productos y procesos, y con la magnitud de sus operaciones.
- Comunicar a la Gerencia General la detección de las posibles deficiencias que se produzcan en la aplicación de las políticas, procesos y procedimientos de gestión del riesgo operacional y las pertinentes propuestas para su corrección.

- Gestionar y administrar toda la información necesaria que será utilizada en los modelos y sistemas de medición de riesgo operacional y que se encuentren disponibles de manera oportuna.
- Evaluar los modelos y sistemas.
- Elaborar reportes agregados sobre la gestión de riesgo operacional.
- Participar del Comité de Gestión Integral de Riesgos.
- En nuevas operaciones, productos y servicios, elaborar y presentar al Comité de Gestión Integral de Riesgos las metodologías para la valuación, medición y control de los riesgos operacionales en los mismos.

5.4. Comité de Gestión Integral de Riesgos

Es competente en el proceso de gestión del riesgo operacional y vela por el cumplimiento de las políticas y estrategias vigentes en la materia, aprobadas y fijadas por el Directorio.

Las responsabilidades del comité son:

- Revisar los procesos de identificación de riesgo operacional.
- Reconocer y entender los riesgos asociados a la operatoria actual y los que puedan surgir de nuevas iniciativas.
- Proponer los niveles de tolerancia al riesgo operacional para su aprobación por el Directorio.
- Comprobar la medición de los riesgos operacionales identificados, verificando el cumplimiento de las políticas, los límites fijados y el impacto económico de los riesgos analizados.
- Solicitar la implementación de las medidas correctivas, en caso que existan desviaciones con respecto a los niveles de tolerancia al riesgo y a los grados de exposición asumidos.
- Realizar el seguimiento de la exposición al riesgo operativo y el resultado de las decisiones tomadas, asegurando una revisión periódica y objetiva de posiciones del riesgo, así como de eventuales excepciones.
- Proponer mejoras al marco para la gestión de riesgo operacional del banco.

- Dar seguimiento a las exposiciones a riesgo operativo. Comparar dichas exposiciones frente a los límites de tolerancia aprobados por el Directorio.
- Reportar al Directorio los resultados de sus valoraciones sobre las exposiciones a riesgo operativo del banco.
- Monitorear estrategias, políticas y límites que coadyuven con una efectiva gestión del riesgo operacional, así como definir los escenarios y el horizonte temporal en los cuales pueden aceptarse excesos a los límites o excepciones a las políticas, los cuales deberán ser aprobados por el Directorio, así como los posibles cursos de acción o mecanismos mediante los cuales se regularice la situación.

5.5. Gerencias

Las gerencias y diferentes unidades orgánicas serán responsables de aplicar, en las distintas unidades de negocios de acuerdo a su ámbito de competencia, los procesos y procedimientos concretos conforme al marco definido para la gestión del riesgo operacional, debiéndose asegurar que tanto los procedimientos como los controles sean adecuados y efectivos en el ámbito que se apliquen.

Asimismo, informarán a Compliance and Risk Management acerca de los resultados de la ejecución de los procesos y procedimientos, con la periodicidad que la entidad financiera establezca de acuerdo con su dimensión, la naturaleza y complejidad de sus productos y procesos y con la magnitud de sus operaciones.

5.6. Auditoría interna

Es responsabilidad de la Auditoría interna, en relación con la gestión de riesgo operacional, revisar anualmente el marco de gestión de riesgo operacional evaluando las actividades de Compliance and Risk Management que participan del proceso. Asimismo, deberá colaborar aportando su experiencia y conocimiento.

6. COBERTURA DEL RIESGO OPERACIONAL

A los efectos de reducir la exposición a los riesgos operacionales significativos, podrán utilizarse herramientas o programas de cobertura de riesgo como por ejemplo las pólizas de seguro, entre otras. Las coberturas son un complemento de las medidas de control interno adoptadas para esos riesgos, pero no se consideran sustitutos de la gestión del riesgo operacional.

El Directorio, el Gerente General, y Compliance and Risk Management, deben evidenciar alto grado de compromiso tendiente a mantener una sólida cultura de control interno, en la cual

las actividades relacionadas con el control del riesgo operacional formen parte de los procesos diarios de la entidad financiera.

7. PLANES DE CONTINGENCIA

La elaboración de los planes de contingencia y de continuidad de la actividad, deben ser acordes con el tamaño y complejidad de las operaciones de Banco CMF S.A., de modo que aseguren la prosecución de su capacidad operativa y la reducción de las pérdidas en caso de interrupción de la actividad.

A esos fines, se deben identificar los procesos más críticos, incluidos aquellos dependientes de terceras partes, y los mecanismos alternativos, a los efectos de reanudar el servicio en caso de su interrupción.

Banco CMF S.A. periódicamente deberá comprobar la eficacia de sus planes de recuperación y de continuidad del negocio mediante su puesta a prueba, verificando que sean acordes con las operaciones y estrategias de negocio.

En la elaboración de los planes de contingencia y de continuidad de la actividad referidos a tecnología informática, son aplicables las normas pertinentes sobre “Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información” y sus modificatorias.

8. APROBACIONES Y MODIFICACIONES

En este acápite se incluye un cuadro de evolución de las diferentes versiones del documento.

Fecha	Resolución	Capítulo	Punto	Observaciones
27/06/2012	Directorio			Creación del documento "Marco de Gestión del Riesgo Operacional"
28/03/2017	Directorio			Revisión completa del documento por asignación de las responsabilidades respecto de la gestión de Riesgo Operacional a UGIR
29/01/2018	Directorio			Revisión integral del documento.
30/09/2019	Directorio			Actualización de acuerdo a implementación de nueva herramienta para la gestión de este riesgo.
10/08/2020	Directorio			Revisión integral del documento.
30/11/2021	Directorio			Revisión integral del documento.
27/12/2022	Directorio			Revisión integral del documento.
31/01/2024	Directorio			Revisión integral del documento.
31/01/2025	Directorio			Revisión integral del documento.
31/01/2026	Directorio			Revisión integral del documento.