Compendio de Normas que regulan a las Cajas de Compensación de Asignación Familiar

6.1.5 EXIGENCIAS DE GESTIÓN QUE DEBEN CUMPLIR LAS C.C.A.F. PARA IMPLEMENTAR ADECUADAMENTE EL PROCESO DE GESTIÓN DE RIESGO OPERACIONAL

La Caja de Compensación debe contar con procedimientos documentados y debidamente aprobados para implementar el proceso de gestión de riesgo operacional, los que deben considerar al menos los siguientes elementos:

6.1.5.1 Política de Gestión de Riesgo Operacional

El Directorio de la C.C.A.F. debe aprobar y ordenar la implementación de una Política de Gestión de Riesgo Operacional, destinada a establecer las medidas que debe adoptar la administración de la entidad en dicho ámbito.

La Política de Gestión de Riesgo Operacional debe contener al menos los siguientes elementos:

6.1.5.1.1 Roles y responsabilidades

Se deben definir las obligaciones y responsabilidades de quienes participan en el proceso de gestión de riesgo operacional. La Caja debe poseer una unidad especializada en la administración del riesgo operacional y debe disponer de los recursos necesarios, físicos, humanos y tecnológicos para cumplir a cabalidad con su labor. El tamaño de esta unidad especialista en riesgo operacional estará directamente relacionado con la complejidad y volumen de operaciones de la C.C.A.F., y estar en constante coordinación con las otras unidades especializadas que se preocupan de la gestión del riesgo de crédito, liquidez y mercado. Debe existir consistencia entre la estrategia de gestión del riesgo operacional definida por la entidad y el volumen de sus actividades. Adicionalmente, la política debe establecer la función de Auditoría Interna en la gestión del riesgo operacional que realiza la C.C.A.F.

6.1.5.1.2 Definición de objetivos del proceso de gestión de riesgo operacional

La C.C.A.F. debe establecer los objetivos que persigue la implementación del proceso de gestión de riesgo operacional, los cuales deben estar alineados con sus objetivos estratégicos.

6.1.5.1.3 Definición de riesgos

La C.C.A.F. debe definir con claridad los riesgos operacionales que le corresponde gestionar, con el objetivo de determinar los tipos de riesgos que serán administrados y la forma a partir de la cual, ellos serán gestionados.

6.1.5.1.4 Definición de riesgo aceptado

La C.C.A.F. debe establecer los criterios para determinar el riesgo aceptado, el cual debe ser consecuente con los criterios de evaluación y tratamiento de riesgos y con el marco legal y reglamentario aplicable a la entidad.

6.1.5.1.5 Criterios de evaluación y tratamiento de riesgos

La C.C.A.F. debe definir el criterio de evaluación de riesgo que mejor se adecúe a su contexto organizacional y estratégico. Además, debe especificar los criterios de tratamiento de los riesgos, junto con las variables a considerar en cada una de ellas.

6.1.5.1.6 Criterios de Divulgación de los riesgos a los actores relevantes

La C.C.A.F. debe definir en su política la forma de entrega de información sobre la gestión del riesgo operacional a los actores relevantes (entidades supervisoras, entidades empleadoras, público en general, acreedores, entre otros).

6.1.5.1.7 Periodicidad en la entrega de información al Directorio

La C.C.A.F. debe establecer la forma y periodicidad con la que se informe al Directorio y a la Gerencia General, entre otros, sobre la exposición al riesgo operacional de la Caja y de cada unidad de negocio.

6.1.5.2 Manual de Gestión de Riesgo Operacional

Basándose en la Política, la Caja de Compensación debe establecer procedimientos formales para la gestión de los riesgos que surjan de los procesos asociados a las actividades efectuadas por dichas entidades.

Tales procedimientos deben estar debidamente documentados en un manual de gestión de riesgo operacional que describa las etapas del proceso de gestión de dicho riesgo, junto a los requerimientos de documentación y de informes resultantes, teniendo en consideración lo que se establece en el presente Título I del Libro VI del Compendio de la Ley N°18.833.

En dicho manual, debe estar identificada la unidad responsable de desarrollar, implementar e impulsar la gestión de riesgo operacional en la entidad.

La C.C.A.F. debe contar con un manual de gestión del riesgo operacional que contemple, por lo menos, los siguientes aspectos:

a) Funciones y responsabilidades asociadas con la gestión del riesgo operacional del Directorio, la Gerencia General, el Comité de Riesgos, la Unidad de Riesgos (o la unidad especializada, si corresponde) y las unidades de negocio y de apoyo.

b) Descripción de la metodología aplicada para la gestión del riesgo operacional.

c) El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que debe contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

6.1.5.3 Análisis y evaluación de riesgos

La C.C.A.F. debe implementar un proceso estructurado bajo el cual los riesgos son identificados, medidos, monitoreados y controlados, considerando al menos los siguientes aspectos:

6.1.5.3.1 Levantamiento de procesos

La unidad responsable de la gestión de riesgo operacional, debe identificar los procesos y subprocesos en los que se descomponen las actividades efectuadas por la entidad, con total cobertura de sus procesos relevantes, identificando a los respectivos dueños de dichos procesos.

6.1.5.3.2 Diagramas de procesos y matrices de riesgo

Los dueños de procesos deben describir de manera precisa los procesos y/o subprocesos, por medio de diagramas de procesos, matrices de riesgos u otros equivalentes.

6.1.5.3.3 Evaluación de riesgos

La unidad responsable de la gestión de riesgo operacional en conjunto con el dueño de cada proceso debe:

a) Identificar y evaluar los diferentes riesgos y factores que influyen sobre éstos mediante un análisis combinado de riesgo inherente, impacto y probabilidad de materialización, considerando la efectividad de las actividades de control implementadas para mitigar dichos riesgos. A partir de ello, se debe estimar el riesgo residual o nivel de riesgo expuesto. Esta evaluación se debe documentar en una matriz de riesgos y controles.

b) Comparar el resultado de esta evaluación con el nivel de riesgo aceptado, definido en la política de gestión de riesgo operacional.

c) Realizar reevaluaciones de forma periódica de los riesgos de la entidad con el fin de asegurar la visión actualizada de los riesgos a los que se encuentra expuesta la entidad, así como la consideración de un correcto nivel de exposición al riesgo.

d) Mantener actualizada y disponible en todo momento la documentación asociada.

6.1.5.4 Tratamiento de Riesgos

De acuerdo con las prioridades establecidas en la etapa de análisis y evaluación de riesgos, la unidad responsable de la gestión de riesgo operacional, en conjunto con el dueño de cada proceso, debe analizar las distintas opciones para el tratamiento de los riesgos, definidas en la política de gestión de riesgo operacional, preparar planes de acción para su tratamiento y definir la forma en que estos últimos se implementarán.

Esta decisión debe estar documentada en la matriz de riesgos y controles, la cual, en este ámbito, debe indicar para cada proceso o subproceso revisado, a lo menos lo siguiente:

a) Descripción del riesgo.

b) Nivel de riesgo o riesgo inherente.

c) Descripción de la acción a tomar.

d) Responsable de la implementación.

e) Plazo y estado de la implementación.

f) Apoyo de otras áreas de la entidad.

6.1.5.5 Responsabilidades y Estructura Organizacional

La C.C.A.F. debe mantener una estructura organizacional apta para la definición, administración y el control del riesgo operacional, derivado del desarrollo de sus actividades. La estructura organizacional de las entidades debe considerar, al menos:

6.1.5.5.1 Directorio

El Directorio tiene las siguientes responsabilidades específicas respecto a la gestión del riesgo operacional:

a) Definir la política general para la gestión del riesgo operacional.

b) Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiados.

c) Pronunciarse sobre la conveniencia de establecer un sistema de incentivos, tanto pecuniarios como no pecuniarios, que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.

d) Aprobar el manual de gestión del riesgo operacional.

e) Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo adecuados niveles de riesgo aceptado.

f) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.

g) Obtener aseguramiento razonable que la Caja cuenta con una efectiva gestión del riesgo operacional, y que los principales riesgos identificados se encuentran bajo control dentro de los límites que han establecido.

h) Velar por el cumplimiento de las instrucciones contenidas en este Título I del Libro VI del Compendio de la Ley N°18.833.

6.1.5.5.2 Gerencia General

La gerencia general tiene la responsabilidad de implementar la gestión del riesgo operacional conforme a las disposiciones del Directorio. Por su parte, los gerentes de las unidades organizativas de negocios o de apoyo tienen la responsabilidad de gestionar el riesgo operacional en su ámbito de acción, dentro de las políticas, límites y procedimientos establecidos.

6.1.5.5.3 Comité de Riesgos

La C.C.A.F. debe contar con un Comité de Riesgos, que sesione en forma periódica, instancia en la que se debe abordar de manera adecuada el riesgo operacional. En estos comités deben participar miembros del Directorio y de la Alta Gerencia de

la C.C.A.F. Las decisiones y aspectos relevantes tratados en la sesión del Comité deben quedar registrados formalmente.

6.1.5.5.4 Comité de Auditoría

La Caja de Compensación debe contar con un órgano de decisión o Comité de Auditoría, que analice los resultados e informes de auditoría y de control, en términos de riesgo operacional, con el fin de obtener conclusiones y tomar acuerdos que trasladará a las Unidades y Direcciones competentes. El Comité de Auditoría debe debatir materias relativas a Riesgo Operacional en aquellos casos en los cuales a partir del proceso de auditoría interna realizado sobre las metodologías de medición y gestión del Riesgo Operacional surjan aspectos relevantes a discutir en dicha instancia. Las decisiones y aspectos relevantes tratados en la sesión del Comité deben quedar registrados formalmente.

6.1.5.5.5 Unidad Especializada en Riesgo Operacional

La C.C.A.F. debe contar con una unidad especializada de gestión del riesgo operacional que cumpla, entre otras, con las siguientes funciones:

a) Proponer políticas para la gestión del riesgo operacional.

b) Participar en el diseño y permanente actualización del Manual de gestión del riesgo operacional.

c) Desarrollar la metodología para la gestión del riesgo operacional.

d) Apoyar y asistir a las demás unidades de la Caja para la aplicación de la metodología de gestión del riesgo operacional.

e) Evaluación del riesgo operacional, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.

f) Consolidación y desarrollo de reportes e informes sobre la gestión del riesgo operacional por proceso, o unidades de negocio y apoyo.

g) Identificación de las necesidades de capacitación y difusión para una adecuada gestión del riesgo operacional.

h) Otras necesarias para el desarrollo de la función.

i) Informar al Directorio y a la Alta Gerencia periódicamente sobre el cumplimiento de las políticas y procedimientos de la gestión del riesgo operacional.

Esta unidad puede delegar determinadas funciones de evaluación, tales como la realización de pruebas a los procedimientos y controles, a otras personas o entidades calificadas externas. No obstante, dicha unidad seguirá siendo responsable de aquellas funciones, las cuales se efectuarán bajo su propia supervisión.

La C.C.A.F. debe asegurar que la función o unidad especializada de gestión del riesgo operacional cuente con recursos suficientes para el pleno desarrollo de sus actividades, así como independencia suficiente en la toma de decisiones.

6.1.5.5.6 Cultura de Riesgo Operacional

Los funcionarios de la C.C.A.F. deben conocer y dar cumplimiento cabal a la política de gestión de riesgo operacional. Además, debe existir evidencia de la toma de conocimiento de la política.

Asimismo, la C.C.A.F. debe promover la capacitación en la gestión del riesgo operacional de su personal, considerando sus diferentes casuísticas en las responsabilidades de los distintos roles.

6.1.5.5.7 Auditoría Interna

La Unidad y/o Gerencia de Auditoría Interna debe evaluar el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional de acuerdo con las exigencias contenidas en el presente Título I del Libro VI de este Compendio de la Ley N°18.833.

El rol de la Auditoría Interna debe ser independiente del área encargada de la gestión del riesgo operacional, y debe contar con los recursos necesarios, independencia y objetividad para entregar información para la toma de decisiones al Directorio sobre la calidad de la gestión de los riesgos que realiza la C.C.A.F.

De forma específica, la función de Auditoría Interna debe:

a) Verificar que el sistema de medición del riesgo está correctamente integrado en la gestión de la Caja de Compensación.

b) Analizar la adecuación de las infraestructuras tecnológicas y la captura y mantenimiento de los datos.

c) Verificar el correcto funcionamiento de los procedimientos y herramientas de la gestión del Riesgo Operacional, validando:

- Los datos internos cargados en la Base de Datos de Pérdidas por Riesgo Operacional.
- El rigor en la cumplimentación de cuestionarios.
- La coherencia entre ambas metodologías.
- El adecuado seguimiento de los Planes de Acción.
- Los procedimientos para revisar y actualizar el Marco de Gestión de Riesgo Operacional.
- Los procedimientos de reporte de la información de gestión.

6.1.5.6 Base de datos de pérdida

6.1.5.6.1 Registro de información de pérdidas

La Caja debe contar con una base de datos de los eventos de pérdida por riesgo operacional. Debe tenerse en cuenta que un evento puede tener como efecto una o más pérdidas y que podrían existir recuperaciones directas o indirectas sobre las mismas, por lo cual la C.C.A.F. debe estar en capacidad de agrupar las pérdidas ocurridas por evento. La base de datos debe cumplir con los siguientes criterios:

a) Deben registrarse los eventos de pérdida originados en toda la C.C.A.F., para lo cual la entidad debe contar con políticas, procedimientos de captura, identificación y asignación de roles y responsabilidades y entrenamiento al personal que interviene en el proceso.

b) Deben registrarse de forma diferenciada cada uno de los impactos económicos y recuperaciones, tanto directas como por seguros, asociadas al evento de pérdidas. Para cada uno de ellos, se deben registrar las categorizaciones, fechas y valores que permitan su completa caracterización sin netear.

c) Debe adelantarse, en lo posible, el reconocimiento y registro por parte de la Caja sobre aquellos eventos de que se tiene conocimiento o certeza razonable que acabarán generando pérdidas por riesgo operacional en la Entidad. Esto incluye a los eventos provisionados.

d) Debe registrarse, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas:

- Código único de identificación del evento.
- Tipo de evento de pérdida, según tipos de eventos señalados en el Anexo N°1: Tipos de evento riesgo operacional nivel I y nivel II del Título I del Libro VI del Compendio de la Ley N°18.833.
- Línea de negocio asociada, según líneas señaladas en el Anexo N°2: Líneas de negocio genéricas para C.C.A.F. del Título I del Libro VIdel Compendio de la Ley N°18.833. Estos cuadros pueden ser actualizados por la Superintendencia. En el caso de que la C.C.A.F. cuente con líneas de negocio internas, éstas deben encontrarse mapeadas a las líneas de negocio definidas en este Título I del Libro VI del Compendio de la Ley N°18.833 y sus procedimientos de asignación documentados.
- Descripción del evento.
- Fecha de ocurrencia o de inicio del evento.
- Fecha de descubrimiento o toma de consciencia del evento.
- Fecha de registro contable del evento.
- Monto(s) bruto(s) de la(s) pérdida(s).
- Monto total recuperado.
- Cuenta(s) contable(s) asociadas.
- Identificación si el evento está asociado con el riesgo de crédito.

6.1.5.6.2 Conciliación contable

La C.C.A.F. debe establecer y ejecutar procedimientos robustos que le permitan asegurar la conciliación de la información registrada en la Base de Pérdidas con el registro contable y que la información de pérdidas por riesgo operacional reflejada

en la contabilidad se encuentre debidamente registrada en la Base de Pérdidas.

Dichos procedimientos de conciliación se deben encontrar formalizados y validados.

La C.C.A.F. debe mantener registro de las pruebas periódicas realizadas sobre la conciliación, así como los resultados obtenidos y las acciones mitigantes o correctoras desarrolladas.

6.1.5.6.3 Pruebas de Calidad de Datos

La C.C.A.F. debe desarrollar de forma periódica, por lo menos una vez al año, pruebas específicas que le permitan asegurar la calidad de los datos registrados en la Base de Pérdidas, incluyendo razonabilidad de montos y fechas, así como la concentración o distribución de eventos.

Los procedimientos y el detalle de las pruebas deben estar formalizados en documentos validados.

La C.C.A.F. debe mantener registro de las pruebas periódicas realizadas sobre la calidad de los datos de la Base de Pérdidas, así como los resultados obtenidos y las acciones mitigantes o correctoras desarrolladas.

6.1.5.6.4 Documentación de eventos

La C.C.A.F. debe mantener registro físico, a disposición de la Superintendencia de Seguridad Social, del expediente con los eventos en los cuales la pérdida asociada sea mayor o igual a 40 U.F., o que cumplan con las demás características indicadas en la letra d) del número 1 del Anexo N°3: Formato y diccionario de archivos planos y formulario web del Título I del Libro VI del Compendio de la Ley N°18.833.

6.1.5.7 Planes de contingencia para asegurar capacidad operativa continua de la C.C.A.F.

Como parte de una adecuada gestión del riesgo operacional, las Cajas deben implementar un sistema de gestión de la continuidad del negocio que tenga como objetivo implementar respuestas efectivas para que la operatividad del negocio de la C.C.A.F. continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la entidad. El plan debe considerar tanto aquellos procesos de soporte o negocio que desarrolle de forma interna la entidad, como aquellos que se encuentren externalizados en proveedores de servicios.

La C.C.A.F. debe realizar de forma periódica, por lo menos una vez al año, pruebas sobre la efectividad de los planes de continuidad de negocio a nivel de la entidad. El plan de dichas pruebas debe quedar documentado, así como los resultados obtenidos y las posibles medidas correctoras identificadas.

Asimismo, la Caja debe contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información. En el diseño del sistema de seguridad de la información se debe tener en cuenta qué hay que proteger y por qué, de qué (o quién) se debe proteger y cómo protegerlo. Además, la Caja puede adherir a alguno de los estándares conocidos y aceptados de Seguridad de la Información, de acuerdo al nivel, complejidad y particularidades de las operaciones de cada Caja.

6.1.5.8 Política para administrar el riesgo asociado a actividades externalizadas

Con el fin de gestionar los riesgos operacionales asociados a la subcontratación, la Caja debe establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados, siendo la Caja la responsable última de dichos procesos. Dichas políticas y procedimientos deben considerar:

a) La evaluación del riesgo, que considere a todas las partes involucradas, previa decisión de externalización. Dicha evaluación debe considerar criterios tales como: los montos pagados, el volumen de transacciones y la frecuencia de trato con el proveedor del servicio.

b) El proceso de selección del proveedor del servicio.

c) La elaboración del acuerdo de subcontratación.

d) La gestión y monitoreo de los riesgos asociados con el acuerdo de subcontratación.

e) La identificación de la criticidad del proveedor.

f) La implementación de un entorno de control efectivo.

g) Establecimiento de planes de continuidad, así como sus pruebas periódicas y reporte de resultados.

h) Acceso a la información por parte del Regulador.

Los acuerdos de subcontratación deben formalizarse mediante contratos firmados entre las partes, los cuales deben incluir acuerdos de niveles de servicio, cláusulas de penalizaciones y definir claramente las responsabilidades del proveedor y de la C.C.A.F., así como establecer los mecanismos de control y seguimiento que se consideren necesarios.