Compendio de Normas del Seguro Social de Accidentes del Trabajo y Enfermedades Profesionales

CAPÍTULO V. Riesgo operacional

1. Procesos sujetos a riesgo operacional en la mutualidad

Los riesgos operacionales deben ser identificados para poder ser gestionados; sin embargo, y a diferencia de otros riesgos, el riesgo operacional debe normalmente ser evaluado a nivel de unidades de negocio y procesos, con la activa participación del personal de las unidades correspondientes.

Para ello se debe contar con mapas de procesos, de entre los cuales se deben identificar aquellos procesos críticos con base en la definición de los objetivos estratégicos de la mutualidad, y en función de su nivel de riesgo inherente y residual evaluado.

Se considerará buena práctica que la metodología de evaluación acerca de cuáles procesos son críticos sea aprobada por el directorio. Sin perjuicio de ello, la mutualidad debe evaluar la totalidad de sus procesos con el fin de definir y evaluar mitigadores que minimicen sus riesgos.

Las mutualidades, en la gestión de los riesgos operacionales, deben tener en cuenta los siguientes macroprocesos:

a) Prestaciones médicas

b) Prestaciones económicas

c) Prestaciones preventivas

d) Reservas técnicas (conformación de las bases de datos, procesos de consulta a esas bases, determinación de parámetros externos, cálculos actuariales, registro contable, presentación en los estados financieros):

   i) Reserva por pago de prestaciones económicas

   ii) Reserva por prestaciones médicas

e) Inversiones

f) Afiliación o adhesión

g) Recaudación de cotizaciones

h) Cobranzas, incluido el manejo del incobrable, y sus respectivas imputaciones contables

i) Recepción de demandas judiciales y juicios

La mutualidad debe realizar una revaluación periódica de la efectividad de sus controles considerando la criticidad de los procesos relacionados. Para lo anterior, podrá utilizar matrices de priorización, las cuales deben considerar ciclos de revisión cuya extensión máxima sea de 36 meses, a excepción de los nuevos procesos y los clasificados como críticos, los cuales deben considerar ciclos de revisión cuya extensión máxima sea de 12 meses.

2. Actividades de gestión del riesgo operacional

La mutualidad, junto con aplicar lo señalado en la Letra B, Título II, de este Libro VII, sobre sistema de control interno, deberá implementar un sistema estructurado bajo el cual los riesgos operacionales sean identificados, analizados, evaluados, monitoreados y controlados, realizando al menos las siguientes actividades:

a) La mutualidad deberá identificar los macroprocesos, procesos y subprocesos en los que se descomponen las actividades efectuadas por la entidad, y sus interrelaciones con total cobertura de sus procesos, identificando a los respectivos dueños. De existir un área especializada en gestión de riesgos, será ésta quién asuma dicha función.

b) Los dueños de procesos deberán describir de manera precisa los macroprocesos, procesos y subprocesos, por medio de diagramas de flujos, matrices de riesgos u otros equivalentes.

c) El área responsable de la gestión de riesgos en conjunto con el dueño de cada proceso, deberá:

i) 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 deberá estimar el riesgo residual. Esta evaluación se deberá documentar en una matriz de riesgos y controles.

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

iii) Realizar, al menos una vez al año, revaluaciones 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.

iv) Analizar las distintas opciones para el tratamiento de los riesgos, definidas en la política de gestión de riesgo operacional, preparando planes de acción para su tratamiento y definir la forma en que estos últimos se implementarán. Esta decisión se deberá documentar en la matriz de riesgos y controles, la cual, en este ámbito, deberá indicar para cada proceso o subproceso revisado, a lo menos lo siguiente, según corresponda:

- Macro proceso, proceso y sub proceso al cual pertenece.
- Descripción del evento de riesgo.
- Identificación de las causas del riesgo.
- Categoría de riesgo operacional.
- Nivel de riesgo inherente, residual y efectividad de los controles existentes.
- Descripción de controles y objetivos de control (para los controles existentes).
- Descripción de la acción a tomar (para la implementación de planes de mitigación).
- Responsable de la implementación de planes de mitigación.
- Plazo y estado de la implementación de planes de mitigación.
- Apoyo de otras áreas de la entidad para la implementación de planes de mitigación.

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

d) Las mutualidades deberán monitorear de forma permanente sus principales riesgos, junto a la efectividad de las actividades de control implementadas.

Los resultados del monitoreo deberán ser informados periódicamente a los miembros del directorio, comité de riesgos, gerencia general y a los dueños de procesos si fuera el caso, a través de reportes periódicos. Para tales efectos, la mutualidad deberán implementar indicadores para realizar el monitoreo sobre:

- Los riesgos de la entidad y su evolución.
- La evolución de los impactos asociados a los eventos de riesgo operacional.
- Los factores de riesgo asociados.
- La efectividad de medidas de control implementadas o existentes.

3. Generación de una base de eventos de riesgo operacional

Las mutualidades deben contar con una base de datos de eventos de riesgo operacional, cuya información debe ser remitida mensualmente a la Superintendencia de Seguridad Social.

Se entenderá por materialización de eventos, a la concreción de aquellos eventos de riesgo operacional, que generen un impacto en la organización y afecten el adecuado cumplimiento de la administración y otorgamiento de las prestaciones del Seguro de la Ley N°16.744. Este impacto, puede implicar o no, un perjuicio o desembolso monetario; sin embargo, independiente del tipo de perjuicio, se deben establecer metodologías adecuadas para la cuantificación de cada impacto del evento materializado.

Los eventos identificados susceptibles de incorporarse dentro de esta base, independiente de la naturaleza del riesgo operacional que lo originó, deben cumplir a lo menos una de estas condiciones:

- Impidan el oportuno o adecuado otorgamiento de prestaciones médicas, económicas y preventivas, incluyendo la interrupción de las operaciones normales.
- Se vean afectados 50 o más: trabajadores, empresas adherentes o pensionados.

- Generen pérdidas económicas.
- Se haya generado alarma pública o un potencial daño de imagen.
- Eventos que hayan dado origen a acciones judiciales, tanto en contra, como por parte de la mutualidad.
- Eventos vinculados a ciberincidentes, según lo establecido en el Capítulo II. Reporte de ciberincidentes, de la Letra D. Ciberseguridad, Título V. Gestión de la Seguridad de la Información, del presente Libro VII.

a) Registros de información de eventos

Se debe considerar que un evento puede tener como efecto uno o más impactos y que podrían existir recuperaciones directas o indirectas sobre las mismas, por lo cual las mutualidades deben registrar todos los impactos ocurridos bajo un mismo código de evento.

La Base de Eventos de Riesgo Operacional debe cumplir con los siguientes criterios:

i) Deben registrarse los eventos originados en la mutualidad, para lo cual la entidad debe contar con procedimientos de captura, identificación y asignación de roles y responsabilidades y entrenamiento al personal que interviene en el proceso, los que deben estar debidamente documentados.

ii) Deben registrarse los eventos y los respectivos impactos de riesgo operacional, sean o no monetarios, y las eventuales recuperaciones, tanto directas (ejemplo: gestión propia) como indirectas (ejemplo: seguros), asociadas al evento. Para el caso de eventos cuyos impactos no sean monetarios, se deberá cuantificar un monto bruto del impacto mediante metodologías construidas por la mutualidad para estos efectos.

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

iv) Debe registrarse, como mínimo, la siguiente información referida al evento, a los impactos y a las recuperaciones:

- Evento:
  Código único de identificación del evento.
  Línea(s) de negocio(s) asociada(s) al evento.
  Tipo o categoría del evento, según tipos de eventos señalados en el Anexo Nº18 "Tipo de eventos de riesgo operacional".
  Fecha de ocurrencia del evento o de inicio del evento.
  Fecha de detección o toma de conciencia del evento.
  Descripción del evento.
  Estatus de finalización o cierre del evento.

- Impacto:
  Código único de identificación del impacto.
  Monto bruto del impacto.
  Línea de negocio asociada al impacto, según lo señalado en el Anexo N° 19 "Líneas de negocio genéricas para mutualidades".
  Indicador de tipo de impacto (monetario / no monetario).
  Descripción del impacto.
  Fecha contable del impacto.
  Cuenta contable.

- Recuperación:
  Código único de identificación de la recuperación.
  Tipo de recuperación (directa o indirecta).
  Descripción de la recuperación.
  Monto bruto de la recuperación.
  Fecha recuperación.
  Fecha contable de la recuperación.
  Cuenta contable de la recuperación.

b) Conciliación contable

Tratándose de eventos con impacto monetario, la mutualidad debe establecer y ejecutar procedimientos robustos que le permitan asegurar la conciliación de la información registrada en la base de eventos de riesgo operacional 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 eventos de riesgo operacional.

Dichos procedimientos de conciliación deben encontrarse formalizados y validados.

La mutualidad debe mantener un registro de las pruebas periódicas realizadas sobre la conciliación, así como los

resultados obtenidos y las acciones mitigantes o correctoras desarrolladas.

c) Pruebas de calidad de datos

La mutualidad debe desarrollar de forma mensual, pruebas específicas que le permitan asegurar la calidad de los datos registrados en la base de eventos de riesgo operacional, incluyendo la 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 mutualidad debe mantener un registro de las pruebas periódicas realizadas sobre la calidad de los datos de la base de eventos de riesgo operacional, así como los resultados obtenidos y las acciones mitigantes o correctoras desarrolladas.

4. Política de actividades externalizadas

Con el fin de gestionar los riesgos operacionales asociados a la subcontratación, las mutualidades deberán establecer una política para evaluar, administrar y monitorear los procesos subcontratados, siendo la mutualidad la responsable última de dichos procesos.

Dicha política deberá 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 operacional, así como sus pruebas periódicas y reporte de resultados.

h) Acceso a la información por parte del regulador.

i) Procedimientos de revisión y actualización de la política de actividades externalizadas, indicando la periodicidad e instancia de la revisión. Estas revisiones deben ser realizadas con una periodicidad de a lo menos una vez al año, debiendo quedar registro de ello.

Los acuerdos de subcontratación deberán formalizarse mediante contratos firmados entre las partes, teniendo presente el acuerdo del nivel de servicio, las cláusulas de penalizaciones, garantías y las responsabilidades del proveedor y de la mutualidad, así como establecer los mecanismos de control y seguimiento que se consideren necesarios.

La política de actividades externalizadas, así como cualquier modificación, deberá ser remitida a la Superintendencia de Seguridad Social en un plazo no mayor a 5 días hábiles, contado desde el día siguiente a su aprobación.