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

7. Actividades de control

Las mutualidades deberán llevar a cabo actividades de control que les permitan asegurar el cumplimiento de las directrices administrativas de control de los riesgos y adoptar las acciones mitigadoras que se estimen necesarias.

Respecto de lo anteriormente expuesto, cabe señalar que cada actividad de control se deberá diseñar con el fin de cumplir con un objetivo de control específico. En la letra a) siguiente se detallan algunos ejemplos de objetivos de control.

Por otra parte, las actividades de control se deben realizar en todos los niveles jerárquicos de las mutualidades y en todas aquellas funciones que conlleven un riesgo. En la letra b) se detallan algunas actividades de control.

a) Ejemplos de objetivos de control

   i) Existencia/Validación: sólo transacciones válidas y debidamente autorizadas son procesadas.

   ii) Ocurrencia: sólo las transacciones que ocurrieron en un determinado período son procesadas (cortes documentales).

   iii) Integridad: todas las transacciones que deben ser procesadas lo son.

   iv) Validación de cálculos: los saldos se valúan con procedimientos adecuados y los cálculos están correctos.

   v) Activos y pasivos: la entidad tiene derechos efectivos sobre los activos, y los pasivos que representan adecuadamente las obligaciones de la entidad.

   vi) Clasificación y presentación: los componentes de los estados financieros son apropiadamente clasificados.

   vii) Razonabilidad: los resultados y/o saldos aparecen como razonables en relación al resto de la información y las tendencias históricas.

b) Ejemplos de actividades de control

   i) Segregación de tareas y responsabilidades

      Las tareas y responsabilidades esenciales relativas a la autorización, ejecución, registro, custodia y revisión de las transacciones y operaciones de la mutualidad deben ser asignadas a personas diferentes.

   ii) Registro oportuno y adecuado de las transacciones y operaciones

      Las transacciones y operaciones que afectan a una mutualidad deben registrarse inmediatamente y ser debidamente clasificadas.

   iii) Requerimiento de respaldos contables y su disponibilidad

      Los registros contables deben quedar respaldados con la documentación de soporte respectiva. Esta documentación tiene que quedar adecuadamente disponible para permitir y facilitar las revisiones internas y externas, incluida la revisión de la Superintendencia de Seguridad Social. El acceso a estos respaldos no debe depender de la presencia o ausencia de las personas.

   iv) Niveles definidos de autorización

      Los actos y transacciones relevantes sólo pueden ser autorizados y ejecutados por funcionarios y trabajadores que actúen dentro del ámbito de su autoridad. La conformidad de las autorizaciones y poderes deben estar en línea con la dirección, la misión, estrategia, planes, programas y presupuesto de la mutualidad.

      Las autorizaciones y poderes otorgados en la mutualidad deben encontrarse documentados formalmente y ser comunicados explícitamente tanto al directorio como a las personas o sectores autorizados. Estos últimos deberán ejecutar las tareas que se les han asignado, de acuerdo con las directrices, y dentro del ámbito de competencias establecidas por la normativa existente.

   v) Acceso restringido a los recursos, activos y registros

      La mutualidad debe proteger y limitar el acceso a los recursos, activos, registros y comprobantes. Las personas

autorizadas deben estar obligadas a rendir cuenta de su custodia y utilización.

Todo activo de valor debe ser asignado a un responsable de su custodia y, por otra parte, es responsabilidad de la administración superior velar porque se cuente con adecuadas protecciones, mediante el uso de seguros, almacenaje, sistemas de alarma, claves de acceso, sistemas de respaldo, etc., según sea aplicable.

Los activos deben estar debidamente registrados y periódicamente, pero sin previo aviso, se deben cotejar las existencias físicas con los registros contables para verificar su coincidencia. La frecuencia de la comparación debe ser definida por la dirección dependiendo del nivel de vulnerabilidad del activo.

vi) Rotación del personal en determinadas funciones

Ningún trabajador debiera tener a su cargo durante un tiempo prolongado tareas críticas que presenten un alto potencial de llegar a cometer irregularidades. Los trabajadores a cargo de dichas tareas debieran periódicamente abocarse a otras funciones. La administración superior de la mutualidad debe velar por establecer medidas mitigadoras suficientes cuando lo anterior no pueda cumplirse.

vii) Revisiones gerenciales

La gerencia general de la mutualidad debe controlar periódicamente el desempeño de las diversas áreas por la vía de indicadores de desempeño de las operaciones, los que deben desarrollarse para todas las áreas de riesgo.

Asimismo, el directorio debe controlar el rendimiento comparado, entre otros, con los planes, presupuestos, el resultado de años anteriores, los resultados de los competidores y del mercado como un todo.

viii) Control de los sistemas de información

Los controles a los sistemas de información deberán, en primer lugar, estar referidos a los controles generales, esto es, controles sobre las operaciones de centro de procesamiento de datos y su seguridad física, sobre contratación y mantenimiento del hardware y software, sobre controles de acceso físico y lógico, y controles sobre desarrollo y mantenimiento de las aplicaciones. Se encuentran dentro de esta categoría los procesos de respaldo de datos y recuperación de caídas. Estos controles aplican a todos los sistemas, sistemas principales, redes de comunicación y computadores personales.

También pueden considerarse controles de aplicación en los procesos que conlleven riesgos significativos, contribuyendo con ello al aseguramiento de la integridad y exactitud de tales procesos, prestando especial atención a las interfaces entre aplicaciones.

Los controles de aplicación se deben extender también a las aplicaciones de usuarios finales relacionadas eventualmente a riesgos en los ámbitos de control interno.