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

C. Elementos de la gestión del sistema de seguridad de la información

CAPÍTULO I. Consideraciones

Para una efectiva gestión del sistema de seguridad de la información, éste se deberá integrar a los procesos de los organismos administradores, considerando sus aspectos en el diseño de los procesos y controles establecidos, en base a las obligaciones y responsabilidades derivadas de la administración del Seguro de la Ley N°16.744.

El sistema de gestión de la seguridad de la información debe ser consistente con las definiciones y objetivos de la política de gestión integral de riesgos, establecida en la Letra A, Título IV, de este Libro VII, y la política de seguridad de la información a la que se refiere el número 9, Capítulo I, Letra E, del Título I, de este Libro VII.

CAPÍTULO II. Política de seguridad de la información

Para una eficiente gestión del sistema de seguridad de la información, se estima necesario establecer las políticas internas que entreguen el marco en que el organismo administrador gestionará la seguridad de la información.

En dicho contexto, esta política debiese considerar al menos los siguientes aspectos:

a) Definición de la seguridad de la información, objetivos generales, alcance y la importancia de ésta como un mecanismo que permita compartir y gestionar información de forma segura.

b) Una declaración de la intención de la alta administración, que apoye los objetivos y principios de la seguridad de la información, en concordancia con las metas y estrategias del organismo administrador.

c) Una explicación de los principios, estándares y requisitos de cumplimiento más relevantes para el organismo administrador, tales como, el adecuado otorgamiento de las prestaciones de la Ley N°16.744, cumplimientos normativos de la Seguridad Social, gestión de la continuidad de negocio, consecuencia de una violación de la política de seguridad de la información, entre otros aspectos.

d) Una definición clara respecto de las responsabilidades generales y específicas de la alta gerencia y demás estamentos relevantes dentro del organismo administrador.

e) Considerar un registro de incidentes de seguridad de la información.

f) Referencia de documentos complementarios a la política de seguridad de la información, si corresponde, tales como procedimientos o manuales detallados con reglas o estándares asociados a actividades específicas.

La política de seguridad de la información debiese ser comunicada y difundida a toda la organización, de forma clara y comprensible para el usuario final. Se recomienda considerar, como parte de este proceso, que al momento de la contratación de un colaborador, éste firme que ha tomado conocimiento de dicha política.

La política de seguridad de la información debiese ser revisada y actualizada anualmente, para asegurar que se encuentre en concordancia con las metas y estrategias de los organismos administradores. Este hecho debiese quedar documentado con la correspondiente firma en el control de cambios del referido documento.

CAPÍTULO III. Gestión de riesgos de las tecnologías de la información

La gestión de los riesgos de las tecnologías de la información implica identificar, analizar, evaluar, tratar, monitorear y comunicar el impacto de los riesgos de las tecnologías de la información sobre los procesos de los organismos administradores.

Una vez que se identifiquen los riesgos y se determine el apetito de riesgo, se recomienda especificar la estrategia de gestión de riesgos, asignando un responsable por cada riesgo identificado y, dependiendo de su importancia e impacto, definir cómo

tratar el riesgo, es decir, evitar, mitigar, transferir o aceptar dicho riesgo.

Por otra parte, se recomienda que los criterios de tratamiento del riesgo estén especificados y formalizados, y que éstos sean revisados anualmente por la alta administración y el directorio, dejándose registro de dicha actividad.

La identificación y formalización de los riesgos de tecnologías de la información y actividades que contemplan el uso, transporte o almacenamiento de activos de información que impiden cumplir con el objetivo de mantener la confiabilidad, integridad y disponibilidad de los datos, continuidad de servicios y protección de dichos activos de información se realizará en la correspondiente matriz de riesgo y controles, contenida en el número 2, Capítulo V, Letra B, del Título IV, del presente Libro VII, identificando claramente los riesgos que los organismos administradores asocian a los riesgos de seguridad de la información.

De igual forma, se recomienda que los organismos administradores adopten las medidas adecuadas para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten la seguridad de sus redes, equipos y sistemas, con el objeto de garantizar su continuidad operativa, así como la continuidad de la seguridad de la información. En todos los casos, se podrá diseñar, implementar, practicar y evaluar un plan de respuesta que otorgue adecuada cobertura a sus redes, equipos y sistemas, en conformidad con estándares internacionales o nacionales, de amplia aplicación y, a su vez, desde el punto de vista de los grupos de interés, garantizar la integridad, disponibilidad y confidencialidad de la información.

CAPÍTULO IV. Acceso a programas y datos

En atención a que los procesos de otorgamiento de las prestaciones de los organismos administradores se encuentran vinculados a un sistema de información, el que se compone por un sistema operativo, una base de datos y el aplicativo en sí, para una correcta gestión de la seguridad de la información es recomendable considerar los siguientes aspectos mínimos en la seguridad de acceso a programas y datos:

a) Seguridad de acceso físico tanto a los servidores como a la inmediación o a cualquier centro sobre el que se encuentre información sensible del organismo administrador, empresas adheridas o afiliadas, trabajadores protegidos y otros beneficiarios, emplazando y protegiendo los equipos para reducir las amenazas y peligros ambientales.

b) Identificación y autenticación de reglas de accesos a los sistemas de información mediante usuarios individualizados y contraseñas encriptadas.

c) La administración de accesos a las cuentas de usuarios con privilegios de administrador debe estar formalmente definida e identificada, tanto en la base de datos, sistema operativo que soporta el aplicativo y el aplicativo en sí.

d) Existencia de un procedimiento de creación de cuentas de usuarios con acceso a los sistemas formalmente documentado, que considere las autorizaciones necesarias y perfiles de accesos para los sistemas de información.

e) Monitoreo de accesos periódicos a los sistemas de información, con el objeto de identificar accesos no autorizados o sospechosos.

f) Implementación de controles para garantizar el acceso autorizado a los usuarios, evitando el acceso no autorizado a los sistemas, aplicaciones y servicios.

Los aspectos señalados precedentemente deben ser formalmente documentados en el procedimiento de administración de accesos a los sistemas críticos para las prestaciones del Seguro de la Ley N°16.744. Asimismo, se recomienda que dicho procedimiento sea revisado y actualizado anualmente, y que se someta a aprobación de la alta gerencia.

CAPÍTULO V. Cambios a programas y datos

Los sistemas utilizados por los organismos administradores para el otorgamiento de las prestaciones del Seguro de la Ley N°16.744, pueden corresponder a desarrollos internos o externos y, de la misma manera, su administración puede ser propia o tercerizada. Dichos sistemas no deben permitir cambios directos en los ambientes productivos, y éstos deben encontrarse autorizados tanto por el área de tecnología como por el dueño del proceso.

Para el cumplimiento de lo señalado en párrafo anterior, se recomienda que los organismos administradores consideren al menos los siguientes aspectos:

a) Implementar ambientes de desarrollo y prueba separados del ambiente productivo para los sistemas de información que soportan procesos críticos.

b) Formalizar y documentar los hitos de conformidad y autorización frente a un cambio en los sistemas, tanto del área dueña del proceso como del área de tecnología.

c) Considerar como parte del proceso de cambios a los sistemas, la documentación de las pruebas de usuario y la respectiva conformidad.

Los aspectos antes señalados deben ser formalmente documentados en el procedimiento de gestión de cambio de los sistemas críticos para las prestaciones del Seguro de la Ley N°16.744, considerando una revisión y actualización anual.

Conjuntamente con lo anterior, se deberá garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida de los datos, incluyendo a los sistemas que proporcionan servicios en redes públicas.

CAPÍTULO VI. Respaldo y restauración de los sistemas

Se recomienda que los organismos administradores implementen medidas de respaldo de la información, restauración de los sistemas, plan de continuidad operacional, además de considerar otras acciones destinadas a mantener el funcionamiento óptimo de los sistemas, y el adecuado otorgamiento de las prestaciones del Seguro de la Ley N°16.744.

En relación con lo anterior, los organismos administradores debiesen considerar al menos los siguientes documentos:

a) Procedimiento de respaldo y restauración de los sistemas críticos para las prestaciones del Seguro de la Ley N°16.744. En este documento se deberá contemplar al menos, la definición del medio de respaldo, la frecuencia en que éstos se llevarán a cabo según el sistema asociado, el lugar de resguardo de dicha información y el responsable de ejecutar el respaldo. Asimismo, se deberá incluir la definición del responsable y la frecuencia de las pruebas de restauración de la información para los sistemas críticos de dicho seguro.

b) Plan de continuidad operacional, considerando lo instruido en el número 4, Capítulo V, Letra B, Título IV, del presente Libro VII.

c) Plan de administración de incidentes, en el que se detalle paso a paso cómo se debe proceder frente a una contingencia o desastre asociado a los servidores o sistemas. Éste debe contener los responsables de iniciar el plan de acción, cargo y datos de contacto, y el procedimiento para documentar y respaldar el evento, así como las condiciones que darán conformidad para finalizar el plan.

CAPÍTULO VII. Responsabilidad y seguridad de los datos

Los organismos administradores deben contar con mecanismos de control que aseguren la exactitud y calidad de los datos y reportes generados, incluida la reportería a los sistemas de información de administración de la Superintendencia de Seguridad Social.

Es responsabilidad de los organismos administradores asegurar que los datos reportados a los sistemas de la Superintendencia de Seguridad Social, sean consistentes, asegurando su totalidad, exactitud e integridad.

Los organismos administradores deberán incorporar en el plan anual de auditoría interna, la revisión sobre la consistencia de los datos reportados a los sistemas de información de la Superintendencia de Seguridad Social.

Por otra parte, se recomienda que, como parte de sus actividades preventivas, los organismos administradores apliquen técnicas de hacking ético, para encontrar vulnerabilidades o fallas de seguridad en el sistema y, de esta manera, adoptar todas las medidas necesarias que posibiliten prevenir una catástrofe cibernética, en función del alcance y periodicidad definidos por el organismo administrador.

Respecto a los activos de la organización que se encuentran accesibles a los proveedores, se deberá acordar con éstos un nivel de seguridad de la información y prestación de servicios conforme a la importancia de dichos activos.