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

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.