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

B. Responsabilidades del organismo administrador en la gestión de la seguridad de la información

Los organismos administradores deberán implementar medidas técnicas y de organización para gestionar los riesgos de seguridad de la información y ciberseguridad de las redes, equipos y sistemas que utilizan para la administración del Seguro de la Ley N° 16.744, especialmente en lo referente al otorgamiento de las prestaciones médicas, económicas y preventivas a los trabajadores, pensionados y entidades empleadoras adheridas y afiliadas.

El organismo administrador determinará las medidas de gestión que garanticen la disponibilidad, integridad y confidencialidad de la información, de conformidad con la complejidad de sus operaciones, los riesgos asociados, la tecnología disponible y la normativa vigente.

Para establecer un adecuado sistema de gestión de seguridad de la información, se recomienda que el organismo administrador, considere los siguientes aspectos:

a) Contar con una política de seguridad de la información y ciberseguridad definida al interior del organismo administrador, establecida por el Directorio o la Dirección Institucional.

b) Realizar Realizar un levantamiento de los activos de información críticos existentes en el organismo administrador asegurando que la información reciba el nivel de protección adecuado de acuerdo con su importancia para la organización. En particular aquellos sistemas relevantes para el soporte de las operaciones y procesos críticos que involucran el adecuado otorgamiento de las prestaciones de seguridad social, con el fin de resguardar la información interna, así como también la de carácter externa relacionada a los trabajadores protegidos, a las entidades empleadoras adheridas o afiliadas, pensionados, entre otros.

c) Conocer los riesgos críticos de las tecnologías de la información identificando los que afecten la seguridad de la información y ciberseguridad.

d) Establecer anualmente el nivel de riesgos aceptado por el organismo administrador en materia de tecnologías de información, considerando además los niveles de disponibilidad mínimos para asegurar la continuidad operacional.

e) Informar al directorio y a toda la organización respecto a los lineamientos principales de la entidad frente a la seguridad de la información.

f) Adoptar las recomendaciones entregadas por auditores externos e internos respecto de esta materia.

g) Contar con el apoyo del área de riesgos existente, procurando que dicha área se involucre en materia de valorización, identificación, tratamiento y tolerancia de los riesgos propios del ambiente de tecnologías de la información a los que se expone el organismo administrador por los distintos factores en que se desenvuelve.

h) Identificar las amenazas más relevantes a las que se expone el organismo administrador ante eventuales ciberataques y evaluar el impacto organizacional que conlleva la vulnerabilidad e indisponibilidad de estos activos de información.

i) Mantener un registro formalmente documentado de los sistemas de información existentes al interior de la organización, señalando el proceso de negocio que gestiona el área usuaria, identificación de la base de datos y sistema operativo que soporta el aplicativo.