Compendio de Normas sobre Licencias Médicas, Subsidios por Incapacidad Laboral y Seguro SANNA

7. RESPONSABILIDADES DE LOS OPERADORES DE LICENCIA MÉDICA ELECTRÓNICA EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los Operadores de licencia médica electrónica deben 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 sistema de licencia médica electrónica, especialmente en lo referente al enrolamiento de profesionales y en la emisión de licencias médicas electrónicas.

Los Operadores de licencia médica electrónica determinarán 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 los Operadores de licencia médica electrónica considere los siguientes aspectos:

a) Contar con una política de seguridad de la información y ciberseguridad definida al interior del Operador de licencia médica electrónica, establecida por el Directorio o la Dirección Institucional. Para estos efectos puede implementar el estándar para la seguridad de la información ISO/IEC 27001 u otro estándar de análoga naturaleza.

b) Realizar un levantamiento de los activos de información críticos existentes en el Operador 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 la adecuada emisión de licencias médicas electrónicas, con el fin de resguardar la información interna, así como también la de carácter externa.

c) Conocer los riesgos críticos de las tecnologías de la información identificando los que afecten la seguridad de la información y ciberseguridad, pudiendo implementar como buena práctica un sistema de gestión de riesgos y mejora continua.

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

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

f) Adoptar las recomendaciones entregadas, en su caso, 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 Operador por los distintos factores en que se desenvuelve.

h) Identificar las amenazas más relevantes a las que se expone el Operador 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 del Operador, señalando el proceso de negocio que gestiona el área usuaria, identificación de la base de datos y sistema operativo que soporta el aplicativo.