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

TITULO IV. MEDIDAS DE SEGURIDAD PARA EL OTORGAMIENTO Y TRAMITACIÓN DE LICENCIA MÉDICA ELECTRÓNICA

1. ENROLAMIENTO DE PROFESIONALES QUE OPEREN EN EL SISTEMA DE LICENCIAS MÉDICAS ELECTRÓNICAS

Para efectos de estas instrucciones, se entiende por enrolamiento al procedimiento de registro y habilitación de un profesional en el sistema de licencias médicas electrónicas, y que le permite la emisión de licencias médicas a través del referido sistema.

El enrolamiento para la emisión de licencias, en el sistema de licencias médicas electrónicas, puede ser efectuado presencialmente por el propio Operador del sistema de licencias médicas electrónicas (LME), tratándose de prestadores individuales, o por el prestador institucional que haya suscrito un convenio con el Operador, respecto de aquellos profesionales que presten funciones en dicha entidad. El enrolamiento también puede efectuarse a través de medios remotos, en la medida que se establezcan mecanismos que permitan identificar al profesional que se registra en el sistema.

El Operador, para efectos de la identificación de los profesionales que se enrolen por medios remotos, debe definir mecanismos de autenticación seguros y robustos cuyo objeto es individualizar en forma inequívoca al profesional de la salud, cumpliendo con todos los resguardos para mitigar el riesgo de suplantación de identidad y/o fraude. Asimismo, el Operador debe guardar registro y medios de verificación de dicha gestión, los que pueden ser requeridos por esta Superintendencia u otras entidades competentes.

Adicionalmente, el Operador puede suscribir convenios con la Subsecretaría de Salud Pública, Fondo Nacional de Salud, Secretarías Regionales Ministeriales de Salud, Instituciones de Salud Previsional o Cajas de Compensación de Asignación Familiar, en la medida que dichas instituciones consintieren en ello, para efectuar el proceso de enrolamiento presencial a través de alguna de estas entidades.

El prestador institucional debe designar una o más personas que contarán con el perfil de administrador en el sistema, quienes serán los únicos habilitados para efectuar el procedimiento de enrolamiento de profesionales, los que, en virtud de ese enrolamiento, sólo estarán habilitados para emitir licencias para dicho prestador institucional. Lo anterior, sin perjuicio que, a través de otros enrolamientos, el profesional se encuentre habilitado para emitir licencias para otros prestadores institucionales, o bien como prestador individual.

Para estos efectos, el Operador debe implementar los controles que se le aplicarán a la persona que utilizará el perfil de administrador en el sistema, los que como mínimo, deben consistir en:

a) Formalidad en la designación de la persona que cumplirá el perfil administrador.

b) Autenticar a la persona que cumplirá el perfil de administrador.

c) Formalización de cambios en la designación de las personas con perfil de administrador (cambio de funciones, renuncia, despidos, cambios de trabajo, fallecimientos, u otros).

d) Los profesionales enrolados por este perfil de administrador de sistema serán asociados al mismo prestador institucional.

e) El administrador de sistema debe suscribir un acuerdo de confidencialidad y fiel cumplimiento de sus funciones.

Respecto de los prestadores individuales, el Operador debe individualizar a sus funcionarios habilitados para realizar el procedimiento de enrolamiento en el sistema. En ambos casos, se debe dejar registro histórico de la persona que ha efectuado el enrolamiento de un determinado profesional. En el caso del enrolamiento remoto la responsabilidad de dicho proceso recaerá siempre en el funcionario habilitado para ello.

2. MEDIDAS QUE DEBEN ADOPTAR LOS OPERADORES DE LICENCIA MÉDICA ELECTRÓNICA EN LA FASE DE ENROLAMIENTO

A) REQUISITOS FORMALES PARA EL ENROLAMIENTO

Cada Operador de LME debe exigir, como mínimo, el cumplimiento de los siguientes requisitos formales a los/las profesionales que requieran su enrolamiento en el sistema:

a) El profesional debe contar con cédula de identidad vigente emitida por el Servicio de Registro Civil de Chile. Excepcionalmente, se puede enrolar en el sistema a profesionales con un RUT provisorio, previamente autorizados para desempeñarse por el Ministerio de Salud, circunstancia que debe ser acreditada por el respectivo profesional de forma previa a su enrolamiento en el sistema.

b) El profesional debe estar inscrito en el Registro Nacional de Prestadores Individuales de Salud (RNPI).

c) Comprobante de domicilio (cuenta de luz o agua, teléfono, internet, u otro de similares características) que valide la dirección otorgada por el prestador.

d) Validación de datos de contactabilidad a través de mail y de teléfono, en donde se verifique que dichos datos son válidos y que correspondan al profesional.

B) OBLIGACIÓN DE VERIFICACIÓN DE LA IDENTIDAD DEL PROFESIONAL QUE SE ENROLA Y DE SUS DATOS BIOMÉTRICOS

Los Operadores de LME tendrán la obligación de verificar la identidad del profesional que se enrola en el sistema, así como también que los datos biométricos que se registran para acceder y firmar la licencia médica electrónica, corresponden a dicho profesional.

Para lo anterior, los Operadores deben implementar un mecanismo que permita verificar que los datos biométricos del profesional, así como también validar que los datos civiles que se registran al momento del enrolamiento corresponden al profesional registrado en el Registro Nacional de Prestadores Individuales. En caso de no contar con dicho mecanismo, o bien cuando éste no cuente con información para validar los datos biométricos del profesional, el enrolamiento debe efectuarse presencialmente, siendo responsabilidad de la persona habilitada para efectuar dicha gestión, la verificación de la identidad del profesional.

Tratándose del registro de huella dactilar, los Operadores deben contar con un protocolo para gestionar aquellas solicitudes en que se requiere la atenuación para facilitar el acceso al sistema. Adicionalmente, los Operadores deben mantener un registro con el listado de profesionales que hayan efectuado esta solicitud, incluyendo la identificación del profesional, la fecha de la solicitud y la fecha en que se concretó la gestión en el sistema.

C) OBLIGATORIEDAD DE CAMBIAR LA CLAVE DE ACCESO AL SISTEMA DE LME

En los casos en que el acceso al sistema sea con clave, los profesionales que tengan la calidad de enrolados en el sistema de licencia médica electrónica, por motivos de seguridad, tendrán la obligación de cambiar dicha clave de acceso al momento de ingresar al sistema por primera vez, debiendo, además, establecerse un procedimiento de actualización obligatoria de la clave a lo menos cada seis meses.

D) RESPALDO DE ANTECEDENTES QUE DEBEN REALIZAR LOS OPERADORES DE LME

Los Operadores de LME deben establecer como mecanismo obligatorio, que los sistemas utilizados, junto con permitir el registro y seguimiento íntegro de las operaciones realizadas, generen archivos que permitan respaldar los antecedentes de cada operación, necesarios para efectuar cualquier examen o certificación posterior, los que, como mínimo, deben considerar la certificación del médico y paciente que actúan en la emisión de la LME, con la fecha y hora en que se realizó la emisión, el registro de las novedades involucradas en el procesamiento de la LME, señalando fecha y hora en que ocurrió y el usuario que lo generó, contenido de los mensajes e identificación de mecanismos de verificación o cotejo posterior.

En todo caso, el Operador de LME debe emitir, cuando corresponda, el respectivo certificado de indisponibilidad que permita dejar registro de las caídas que experimente el sistema.

E) EXIGENCIA DE PROTOCOLOS

Los Operadores de LME deben establecer el proceso de enrolamiento remoto y reenrolamiento, en su caso, mediante un protocolo que especifique los pasos, requisitos y responsables del referido proceso.

F) MECANISMOS DE AUTENTICACIÓN Y PERFIL DE SEGURIDAD

Los Operadores deben contar con mecanismos de autenticación seguros, que permitan individualizar en forma inequívoca al profesional que se adscribe al sistema, se enrola o registra y emite LME.

Asimismo, el sistema debe proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio.

Además, los procedimientos deben impedir que las personas que intervengan en el flujo desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse métodos de autenticación seguros para el acceso al sistema y al tipo de operación, que permitan velar por su autenticidad e integridad.

G) CANAL DE COMUNICACIÓN

Los Operadores deben mantener permanentemente abierto y disponible un canal de comunicación que permita al usuario o al prestador institucional ejecutar o solicitar el bloqueo de cualquier operación que intente efectuarse utilizando sus medios de acceso o claves de autenticación. Cada sistema que opere en línea y en tiempo real, debe permitir dicho bloqueo también en tiempo real.

3. GESTIÓN DEL RIESGO DE FRAUDE

Los Operadores de LME deben contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar, en el menor tiempo posible, aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deben establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos de estos y comportamientos que no estén asociados al cliente.

Estos sistemas o mecanismos deben permitir tener una vista integral y oportuna de las operaciones del profesional enrolado, de personas no enroladas (por ejemplo, en los intentos de acceso), de los puntos de acceso (por ejemplo, direcciones IP), de frecuencia de emisión, de control de sesiones únicas, de mecanismos que impidan utilización de robots o procesos automatizados que simulen acciones humanas. En concreto, los Operadores de LME deben hacer el seguimiento y correlacionar eventos y/o fraudes a objeto de detectar otros fraudes, puntos en que estos se cometen, manera en que se realizan estas operaciones, y puntos de compromisos, entre otros.

Asimismo, para reducir la probabilidad de materialización de riesgos debido a fraudes, los Operadores deben establecer un programa de gestión del riesgo de fraude, que comprenda las siguientes actividades:

A) ACTIVIDADES DE PREVENCIÓN

Los operadores deben contar con una política de prevención de fraude, sujeta a un proceso de mejora permanente, debiendo incorporar una metodología de fortalecimiento del control interno y definir actividades de monitoreo que midan su aplicación y efectividad. La política debe establecer quién es el responsable de gestionar el riesgo de fraude en la entidad, las actividades de prevención, detección e investigación y respuesta del fraude y las responsabilidades que el personal de todos los niveles de la entidad debe tener respecto a la gestión del riesgo de fraude.

Adicionalmente, los Operadores deben establecer instancias de gestión y monitoreo del riesgo de fraude, además de controles para prevenir, detectar y responder ante eventos de fraudes. De la misma manera, los Operadores deben asumir las siguientes responsabilidades en relación con la gestión del riesgo de fraude:

a) Propiciar un ambiente laboral positivo, con el objetivo de evitar incentivos, presiones o motivaciones que puedan inducir a los empleados al fraude.

b) Identificar riesgos de fraude, con el objetivo de establecer controles que permitan mitigarlos.

c) Desarrollar una política y procedimiento de gestión de personas que contemple la contratación, inducción y finiquito de personal, con un enfoque alineado en la prevención del fraude.

d) Implementar procedimientos y mecanismos para monitorear áreas de riesgo.

e) Implementar un sistema de control interno robusto con el objetivo de evitar las oportunidades o condiciones que faciliten la comisión de fraudes.

f) Establecer sistemas que permitan la generación de información completa, fiable y oportuna para efectuar análisis preventivos.

g) Evaluar los eventuales riesgos que se generen cada vez que el Operador realice cambios en su estructura, sistemas, procesos, procedimientos, personas y proveedores de servicios externos.

B) ACTIVIDADES DE DETECCIÓN

a) Detección temprana

Los Operadores deben implementar mecanismos de detección de fraudes en los procesos que desarrollan, lo que comprende mecanismos tales como:

- Análisis de datos que permitan la identificación de patrones o esquemas de comportamientos anómalos, a través de sistemas informáticos adecuados, especializados en el análisis de datos masivos y sus relaciones.
- Pruebas de cumplimiento de controles.
- Mecanismos anónimos de comunicación de potenciales fraudes.

A partir de lo anterior, los Operadores deben generar una base de conocimientos con información de los profesionales registrados en su base de datos y desarrollar indicadores o alertas de fraude.

A su vez, los Operadores deben desarrollar, cada seis meses, procedimientos de actualización de la información personal de los profesionales registrados en el sistema de licencias médicas electrónicas, considerando para ello a lo

menos el domicilio, datos de contacto, correo electrónico, número telefónico y actualización de la clave. Este procedimiento tendrá el carácter de obligatorio y su omisión impedirá a los profesionales continuar operando en el sistema.

b) Auditoría interna

Los Operadores deben desarrollar un plan anual de auditoría interna, que considere la evaluación de la eficiencia de los controles implementados en los procesos con mayor riesgo de fraude.

c) Responsable de la gestión del riesgo de fraude.

Los Operadores deben contar con un responsable de la administración del riesgo de fraude, quien debe asumir las siguientes funciones:

- Administrar el canal de denuncias.
- Comunicar la información recibida de acuerdo a los protocolos y políticas de escalamiento establecidos en la entidad.
- Llevar adelante la investigación del potencial fraude.
- Diseñar medidas o protocolos de acción tendientes a tratar situaciones anómalas que puedan ser indicios de fraude.
- Participar en la planificación del programa de prevención de fraude y efectuar su seguimiento.
- Registrar y clasificar las denuncias o reclamos cuyo análisis pueda revelar señales o indicios de fraude.
- Evaluar la efectividad de los procedimientos para recepcionar y tratar las denuncias o reclamos.
- Proponer medidas correctivas en los controles antifraude.

El responsable de la administración del riesgo de fraude debe contar con la capacitación y los conocimientos necesarios para llevar a cabo las funciones antes señaladas.

d) Canal de denuncias

Los Operadores deben implementar un canal de denuncias o línea ética para registrar eventos, que permita alertar oportunamente, detectar e investigar un posible fraude. El canal de denuncias o línea ética, debe garantizar el anonimato y seguridad en la entrega de información.

C) ACTIVIDADES DE RESPUESTA

Los Operadores deben desarrollar protocolos de investigación interna o externa, escalamiento del fraude, resguardo de las pruebas para posteriores procedimientos judiciales, aplicación de sanciones, así como un plan de respuesta antifraude. Dicho protocolo debe contener al menos los niveles jerárquicos a ser notificados, los plazos máximos de notificación, las sanciones y los mecanismos de respaldo de la información.

Los Operadores deben informar a esta Superintendencia, los hechos potencialmente constitutivos de fraude que detecten y que afecten al sistema de licencias médicas electrónicas, dentro de las 24 horas siguientes a su detección.

A su vez, los Operadores deben evaluar la aplicación de sanciones internas y comunicarlas al personal cuando se hayan aplicado, sin perjuicio de efectuar la denuncia al Ministerio Público, en su caso, y evaluar la interposición de las acciones judiciales que resulten pertinentes.

Respecto de los posibles fraudes detectados, los Operadores deben analizar los controles que se hayan vulnerado y aplicar las medidas correctivas que procedan.

4. CONSULTA AL REGISTRO NACIONAL DE PRESTADORES INDIVIDUALES

Los Operadores de LME deben implementar un procedimiento de consulta al Registro Nacional de Prestadores Individuales, al menos una vez al día cuando el profesional se loguee para operar en el sistema de LME, a fin de verificar que mantiene registro vigente.

En caso que no cuente con registro vigente en el señalado Registro, se debe inhabilitar temporalmente el acceso al sistema hasta que el profesional regularice dicha situación.

Si por cualquier causa no imputable al Operador, éste se encontrare impedido de consultar el Registro Nacional de Prestadores Individuales, se permitirá la emisión de licencias médicas sin la verificación antes señalada, dejando constancia de la fecha y hora en que realizó la consulta y del respaldo que acredite que ésta no se pudo efectuar por una causal no imputable al Operador.

5. INHABILITACIÓN PREVENTIVA DEL REGISTRO

Si el Operador observa cualquier anomalía respecto de la autenticidad de la información registrada por el profesional o bien cuando éste presente un comportamiento inhabitual en la emisión de licencias médicas, ya sea por su cantidad, frecuencia de emisión o anulación, o lugar desde el que se otorga, el Operador debe inhabilitar preventivamente al profesional, debiendo comunicarle dicha circunstancia a éste y, en caso de corresponder, al prestador institucional, y requerirle que efectúe un nuevo proceso de enrolamiento presencial, bajo el apercibimiento de mantener la inhabilitación del registro mientras no cumpla con esta obligación.

El Operador debe mantener un registro de las inhabilitaciones preventivas que hubiere efectuado, en el que se indique, como mínimo, la identificación del profesional, la fecha y hora en que se efectuó la inhabilitación, la fecha y hora en que se rehabilitó el acceso al profesional, la causa por la que se efectuó la inhabilitación preventiva y el mecanismo utilizado para validar la identidad del profesional y rehabilitar su acceso.

El referido registro debe disponibilizarse para consulta de la Superintendencia de Seguridad Social.

6. BLOQUEO DEL REGISTRO POR APLICACIÓN DE LAS SANCIONES ESTABLECIDAS EN LA LEY N°20.585

Sin perjuicio de las instrucciones contenidas en el Título II de este Libro VI, los Operadores deben dar cumplimiento a la suspensión de la facultad de emitir licencias médicas que se imponga a un profesional como resultado de la aplicación de los procedimientos establecidos en la Ley N°20.585.

Para estos efectos, la Superintendencia de Seguridad Social o la Comisión de Medicina Preventiva e Invalidez, según corresponda, comunicarán a los Operadores el periodo por el cual se debe aplicar la referida suspensión. A su vez, el o los Operadores en los cuales se encuentre registrado el profesional, procederán a bloquear su registro por el periodo en que se extienda la suspensión, comunicando dicha circunstancia, además, al prestador institucional.

Por su parte, aquellos Operadores en los que el profesional no se encuentre registrado, deben establecer los resguardos necesarios para impedir que el profesional se enrole en el sistema durante el periodo en que se encuentre suspendido.

Los Operadores deben disponer un mecanismo que permita a la Superintendencia de Seguridad Social y a las Comisiones de Medicina Preventiva e Invalidez, según corresponda, verificar que la suspensión de la facultad de emitir licencias médicas se ha materializado en tiempo y forma, a través del bloqueo del registro en el sistema de licencias médicas electrónicas.

Además, el Operador debe disponibilizar mecanismos para que los bloqueos y desbloqueos puedan ser gestionados directamente por las Comisiones de Medicina Preventiva e Invalidez o la Superintendencia de Seguridad Social, según corresponda, respecto de los profesionales que éstas hayan sancionado.

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.