Gobierno de Chile

640

MINISTERIO DE SALUD
DIVISIÓN JURÍDICA
DOC/UVO/FCA/ABG/EDV

V°B° SUBSECRETARÍA DE SALUD PÚBLICA GABINETE

VISADO

APRUEBA POLITÍCA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

EXENTA N° 781 /

SANTIAGO, 14 OCT. 2014

VISTOS: Lo dispuesto en la ley N° 19.880 que establece Bases de los Procedimientos Administrativos; en el D.F.L N°1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del decreto ley N° 2763, de 1979 y las leyes N° 18.933 y N°18.469; en el decreto supremo N° 136, de 2004, del Ministerio de Salud, que aprueba Reglamento Organico del Ministerio de Salud; en la ley N° 19.799 sobre documentos electronicos, forma electronica y servicios de certificación de dicha firma; en el D.S N° 83, de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en la ley N° 19.233 sobre delitos informaticos; en la Norma Chilena NCh-ISO 27001.Of2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos; en el Memorándum A18 N° 285, de 14 de agosto de 2012, del Jefe de Departamento Gestión Sectorial de TIC; en la resolución N° 1.600, de 2008, de la Contraloría General de la República; y

CONSIDERANDO:

1° Que, las nuevas tecnologías de la información y de las comunicaciones (TIC) al ser incorporadas progresivamente a los procesos institucionales y al quehacer personal de los funcionarios al ejercer sus labores en el Ministerio de Salud, presentan una serie de beneficios, ventajas y oportunidades de diversa índole, pero conlleva también ciertos riesgos, que pueden afectar a los activos de información institucional.

2° Que, se oficializó la norma técnica sobre seguridad y confidencialidad del documento electrónico para los órganos de la Administración del Estado a través del Decreto Supremo N°83, del Ministerio Secretaria General de la Presidencia, de 2005.

3° Que, por consiguiente, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, y que consiste básicamente en la realización de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles de integridad, confidencialidad y disponibilidad, con todos sus activos de información relevantes para la institución, como un principio clave en la gestión de procesos.

4° Que, debido a la implementación del sistema de seguridad de la información en conjunto por la Subsecretaría de Redes

Asistenciales y la Subsecretaría de Salud Pública, se ha creado la Política General de Seguridad de Información Res. Exe. Nº 568 del 28.08.2013, según los requisitos de la Norma NCh-ISO 27001 y lo dispuesto por la red de expertos.

5º Que, conforme a lo anterior, resulta necesario contar con una Política General de Seguridad de la Información, y por consiguiente, dicto la siguiente:

RESOLUCIÓN:

1º APRUÉBASE la Política General de Seguridad de la Información, para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales, cuyo texto es el siguiente:

1. DECLARACION INSTITUCIONAL

Las tecnologías de la información y de las comunicaciones (TIC), al ser incorporadas progresivamente a los procesos institucionales y al quehacer de los funcionarios al ejercer sus labores en el Ministerio de Salud, presentan una serie de beneficios, ventajas y oportunidades, pero conllevan, también, ciertos riesgos, que pueden eventualmente afectar a los activos de información institucional.

Por consiguiente, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, por medio de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad, de todos sus activos de información relevantes para la institución, como un principio clave en la gestión de sus procesos.

El Ministerio de Salud, se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, a través de un programa de implantación del tipo "Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma Chilena Oficial NCh-ISO27001.Of2009, con el objetivo de preservar los activos de información institucional con respecto a:

- **Su Integridad:** la información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. Este principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas del negocio, así como evitar fraudes o irregularidades de cualquier índole que haga que la información sea alterada.

- **Su Confidencialidad:** la información sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones. Este principio fundamental de seguridad busca garantizar que toda la información de los ciudadanos, funcionarios y proveedores, y sus medios de procesamiento o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

- **Su Disponibilidad:** La información debe estar disponible para el personal, usuarios y entidades reguladoras de manera oportuna y acorde a sus niveles de autorización. Este principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando ésta es requerida por el proceso de la institución. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en

forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento o equipamiento de procesamiento.

Según lo expuesto anteriormente, el Ministerio de Salud se compromete a:

- Apoyar los objetivos y principios de la seguridad de la información, y a proveer los recursos necesarios para la gestión de actividades en seguridad.

- Desarrollar y ejecutar un plan de acción de mejora continua, con el fin de asegurar una adecuada gestión de la seguridad de la información, según lo dispuesto en la NCh-ISO 27001.Of2009 y otras normativas vigentes que se referencien en el documento "Normativa del Sistema de Gestión de Seguridad de la Información".

2. NORMATIVA APLICABLE

El marco legal para el Sistema de Gestión de Seguridad de la Información se señala en el documento "Normativa del Sistema de Gestión de Seguridad de la Información".

3. OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL MINISTERIO DE SALUD

3.1 Objetivo General

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucionales relevantes, asegurando la continuidad operacional de los procesos.

3.2 Objetivos Específicos:

- Identificar y catastrar todos los activos de información relevantes que están presentes directa o indirectamente en cada proceso institucional, abarcando tanto los procesos críticos institucionales, como los de soporte.
- Realizar actividades necesarias de análisis de riesgo, según normativas, técnicas y estándares disponibles y aplicables, para diseñar e implantar medidas y controles que permitan mitigar los riesgos que sean identificados, sin perder de vista el enfoque de la gestión por procesos institucionales.
- Proteger la información, sus medios de procesamiento, conservación y transmisión del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarla o ponerla en riesgo.
- Mantener y hacer uso de la estructura y el marco de estándares, políticas y procedimientos en materia de seguridad de la información.
- Minimizar la posibilidad de ocurrencia de hechos contingentes que pudieran interrumpir la operación del negocio y reducir el impacto de los daños a las instalaciones, medios de almacenamiento, equipos de procesamiento y de comunicación.
- Hacer uso de/los plan/es de continuidad operacional ante hechos contingentes que interrumpan la operación del negocio.
- Sensibilizar y capacitar a los funcionarios del MINSAL acerca de su responsabilidad para mantener la seguridad de la información y su adecuado uso, estableciendo una cultura organizacional que incorpore el tema de seguridad de la información como un aspecto relevante en los procesos de negocio del Ministerio.

4. ALCANCE DE LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Esta política es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para las Subsecretarías de Salud Pública y Redes Asistenciales, y contempla los ámbitos de control específicos, contenidos en la NCh-ISO 27001.Of2009.

5. GESTIÓN DE LA POLITICA Y OTROS DOCUMENTOS

La necesidad del desarrollo de nuevas políticas tendrá como fin cubrir las brechas detectadas en los controles específicos contenidos en la norma NCh-ISO 27001.Of 2009.

Las modificaciones de las políticas vigentes deberán ser gestionadas a través del Encargado de Seguridad del Ministerio de Salud, quien, en conjunto con el Comité de Seguridad de la Información, deberá evaluar la factibilidad de aplicarlas.

Para la implementación de las políticas se definirán documentos complementarios, tales como: procedimientos, instructivos, circulares, etc. indicando claramente el o los responsables de su ejecución.

Las nuevas políticas, procedimientos u otros documentos deben ser propuestos al Comité de Seguridad de la Información por el Encargado de Seguridad del Ministerio de Salud, para su aprobación respectiva.

6. ROLES Y RESPONSABILIDADES

6.1. Comité de Seguridad de la Información Sectorial.

a. Responsable del ciclo de vida de las políticas de seguridad de la información del Ministerio.
b. Velar por el cumplimiento y actualización de la Política General de Seguridad de la Información.
c. Validar, aprobar y difundir al interior del Ministerio las políticas del Sistema de Gestión de Seguridad de la Información.
d. Velar por la implementación de los controles de seguridad en la plataforma tecnológica del Ministerio.
e. Monitorear los cambios significativos que pudieran variar los riesgos presentes en la Institución.
f. Monitorear los incidentes de seguridad que pudieran afectar la seguridad al interior de la organización, con el fin de establecer acciones preventivas y correctivas.

6.2. Encargado de Seguridad de la Información.

a. Encargarse del desarrollo inicial de las políticas de seguridad al interior de la organización y el control de su implementación, y velar por su correcta aplicación.
b. Organizar las actividades del Comité de Seguridad de la Información.
c. Coordinar la debida respuesta y priorización del tratamiento de incidentes vinculados a los activos de información de la Institución.
d. Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
e. Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos.
f. Tomar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de seguridad.

6.3. Propietario de la información: Es el Jefe o Encargado de la Unidad Organizacional, responsable de la protección y uso de la información. El propietario de la información es responsable de la clasificación de la misma y es responsable del mantenimiento y actualización de dicha clasificación.

6.4. Usuario de la información: Es el conjunto de personas internas y/o externas que, con la debida autorización del propietario de la información, puede consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos u otros medios de almacenamiento.

Los usuarios sólo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitarán su capacidad en los entornos informáticos de forma que no puedan realizar actividades diferentes a las autorizadas.

Las principales responsabilidades de los usuarios de información son:

a) Utilizar la información sólo para el propósito para el que recibió autorización de uso.
b) Conocer las políticas y procedimientos de Seguridad de la Información que se han institucionalizado.
c) Cumplir con los controles establecidos en las políticas y procedimientos definidos en el SGSI
d) Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.
e) Comunicar los incidentes relativos a la seguridad de la información.

7. REVISIÓN Y MEDICIÓN.

A lo menos una vez al año, el Comité de Seguridad de la Información Sectorial, debe evaluar el cumplimiento de la Política General de Seguridad de la Información, considerando cambios que surjan en el transcurso de este periodo que podrían afectar el enfoque de la organización a la gestión de la seguridad de la información, incluyendo cambios al ambiente de la organización, disponibilidad de recursos, condiciones contractuales, reguladoras, y legales, o cambios al ambiente técnico.

Para ello debe considerar los siguientes aspectos:

- Retroalimentación de las partes interesadas.
- Resultados de las revisiones efectuadas por terceras partes.
- Estado de acciones preventivas y correctivas.
- Cambios en los procesos institucionales, nueva legislación, tecnología etc.
- Alertas ante amenazas y vulnerabilidades.
- Información relacionada a incidentes de seguridad.
- Recomendaciones provistas por autoridades relevantes.
- Medición de los indicadores del Sistema.

Por otro lado, deberá revisar el estado del Sistema de Gestión de Seguridad de la Información, a lo menos cada tres años mediante auditorías internas o externas.

8. MARCO GENERAL PARA LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

La estructura documental del Sistema de Gestión de Seguridad de la Información, estará conformado por la presente Política General sustentada en políticas particulares, procedimientos de operación e instructivos, los que se generarán según lo siguiente:

- Que integren el modelo de seguridad con las metodologías y políticas existentes para ambas Subsecretarias.
- Que cumplan con la normativa definida en el documento Normativa del Sistema de Gestión de Seguridad de la Información.
- Que se cumplan las normas legales y reglamentarias referidas a seguridad, tanto para la información, como para los medios que la contienen.
- Que la información cumpla con los niveles de autorización y responsabilidad correspondientes para su utilización, divulgación, administración, seguimiento y custodia.

- Que la información, sus medios de procesamiento, conservación y transmisión estén protegidos del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotajes, espionaje, violación de la privacidad y otras acciones que pudieran perjudicarla.
- Que los medios de procesamiento, conservación y comunicación de la información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.
- Que los derechos de propiedad sobre la información y sistemas estén establecidos.
- Que las comunicaciones internas y externas cuenten con mecanismos que protejan la integridad, disponibilidad y confidencialidad en la transmisión de información.
- Que se delimiten los ámbitos físicos de acción de las políticas de seguridad, dependiendo de los distintos niveles de riesgo que presentan los medios de procesamiento, conservación y comunicación.
- Que el acceso a los servicios de ambas Subsecretarias, ya sea por medios internos o externos, se realice de acuerdo con las atribuciones de las personas o entidades que las utilicen.
- Que las actividades y uso de recursos críticos, relacionados con productos y servicios, sean monitoreados y su información sea conocida en forma oportuna por los niveles correspondientes.

9. DIFUSION.

El Ministerio de Salud, deberá establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos generados en el marco del Sistema de Gestión de Seguridad de la Información (algunos de los canales accesibles y formales de difusión son: correo electrónico, intranet, comunicación impresa, charlas y/o capacitaciones).

Todas las políticas, procedimientos y documentos relacionados, serán publicados en la página web de MINSAL a través de la web http://web.minsal.cl/seguridad_de_la_informacion

Adicionalmente, las políticas, procedimientos y documentos relacionados se informarán a cada funcionario a través de correos masivos, boletines informativos u otras actividades de difusión que se definan para tal efecto.

Será responsabilidad del Departamento de Recursos Humanos, incorporar la aplicación y observancia de las políticas de seguridad de la información, en su plan de capacitación institucional, junto con velar por la correcta inducción de los funcionarios nuevos en materias de seguridad de la información.

10. ACEPTACION

Todos los usuarios del Ministerio de Salud, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deberán aceptar ésta Política General de Seguridad de la Información, las Políticas específicas y Procedimientos relacionados.

Para el caso de terceros y por el solo hecho de participar en algún proceso de compras del servicio, el oferente deberá dar cumplimiento a las Políticas y Procedimientos vigentes de seguridad de la información del Ministerio de Salud, publicadas en el link http://web.minsal.cl/seguridad_de_la_informacion, y sus correspondientes modificaciones, las cuales se presumen conocidas por el contratista o adjudicatario, para todos los efectos legales.

11. SANCIONES

El incumplimiento de las obligaciones emanadas de esta Política, de las Políticas específicas del Sistema, Procedimientos u otros documentos que se deriven de éstos, serán sancionadas en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del Ministerio de Salud. Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, se procederá al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

2º ESTABLÉZCASE la obligación del Departamento de Recursos Humanos de la Subsecretaría de Salud Pública, de difundir la política fijada en este instrumento y al Departamento de Gestión Sectorial TIC, de velar por su estricto cumplimiento.

3º INSTRÚYASE al Jefe del Departamento de Gestión Sectorial TIC y a los Encargados de Seguridad de la Información, que realicen las acciones tendientes a la implementación de la presente Política en materias de su competencia.

ANÓTESE Y COMUNÍQUESE

REPUBLICA DE CHILE ★ SUBSECRETARIA DE SALUD PUBLICA ★ MINISTERIO DE SALUD

DR. JAIME BURROWS OYARZÚN
Subsecretario de Salud Pública

REPUBLICA DE CHILE ★ SUBSECRETARIA DE REDES ASISTENCIALES ★ MINISTERIO DE SALUD

DRA. ANGÉLICA VERDUGO SOBRAL
Subsecretaria de Redes Asistenciales

Distribución:
- Gabinete Sra. Ministra de Salud
- Subsecretaría de Salud Pública
- Subsecretaría de Redes Asistenciales
- Departamento de Gestión Sectorial de Tecnologías y Comunicaciones
- División Jurídica
- Oficina de Partes