MINISTERIO DE SALUD
SUBSECRETARIA DE SALUD PÚBLICA
SUBSECRETARIA DE REDES ASISTENCIALES
DIVISIÓN JURÍDICA

JEFE GABINETE V°B°

AEG / JVC / SML / EAR / MPS

APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARÍA DE SALUD PÚBLICA Y PARA LA SUBSECRETARIA DE REDES ASISTENCIALES

EXENTA Nº 1332 /

SANTIAGO, 14 NOV. 2016

VISTO: Lo dispuesto en la ley Nº19.880 que establece Bases de los Procedimientos Administrativos; en el Decreto con Fuerza de ley Nº1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del Decreto Ley Nº2763, de 1979 y de las leyes Nº18.933 y Nº18.469; en el Decreto Supremo Nº136, de 2004, del Ministerio de Salud, que aprueba Reglamento Organico del Ministerio de Salud; en la ley Nº19.799 sobre documentos electronicos, forma electronica y servicios de certificación de dicha firma; en el Decreto Supremo Nº83, 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 Nº19.233 sobre delitos informáticos; en la Norma Chilena NCh-ISO 27002 Of.2013; en la Resolución Exenta Nº1231, de 21 de octubre de 2016, que crea la División de Tecnologías de Información y Comunicaciones; y en la Resolución Exenta Nº1161, de 4 de octubre de 2016, conjunta de las Subsecretarías de Salud Pública y de Redes Asistenciales, que aprueba el Sistema de Seguridad de la Información para dichas Subsecretarías, las Secretarías Regionales Ministeriales y los Servicios de Salud.

CONSIDERANDO:

1. Que, las nuevas tecnoclogías de la información y de las comunicaciones (TIC) al ser progresivamente incorporadas a los proceso institucionales y al quehacer personal de los funcionarios en el ejercicio de sus funciones, presentan una serie de beneficios, ventajas y oportunidades de diversa indole. Sin embargo, también conlleva ciertos riesgos que pueden afectar a los activos de información institucional.

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

3. Que, siendo la seguridad de la información un tema de suma relevancia en el Ministerio de Salud habida cuenta del volumen de información sensible con la que se trabaja, existe la necesidad de contar con una estructura de organización sectorial, que considere la definición de lineamientos y prácticas de seguridad de la información a ser aplicadas a todos los organismos relacionados. En este sentido, es una prioridad para el Ministerio de Salud implementar, mantener y mejorar continuamente la gestión de la seguridad de la Información con una mirada sectorial, basada en preservar los principios de confidencialidad, integridad y disponibilidad de la información.

4. Que, a la fecha, existen una serie de normas en materias de seguridad de la información entre las que se encuentra el Decreto Supremo Nº83, de 2005, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos y la Normas Chilenas NCh-ISO 27001 Of.2013 y NCh-ISO 27002 Of.2013 que proporcionan un marco de gestión de Seguridad de la Informacion utilizable por cualquier tipo de organización, pública o privada.

5. A su vez, internamente, han existido varias normas como la Resolución Exenta Nº781, de 14 octubre de 2014, que aprueba la política general de seguridad de la información; la Resolución Exenta Nº782 de misma fecha que actualiza Comité de Seguridad de la Información Sectorial del Ministerio de Salud; y otras que aprueban políticas y procedimientos particulares de seguridad de la información y que tienen por alcance la Subsecretaria de Salud Pública y Subsecretaria de Redes Asistenciales.

6. Que, sin embargo, en el Ministerio de Salud existe la intención de actualizar y mejorar dicha normativa; y el interés de crear una instancia sectorial que coordine la seguridad de la información no solo a nivel ministerial sino que incluya a los servicios dependientes y relacionados.

7. Que, en ese contexto, a través de la Resolución Exenta N°1161, de 4 de octubre de 2016, conjunta del Subsecretario de Salud Pública y la Subsecretaria de Redes Asistenciales aprobaron un nuevo Sistema de Seguridad de la Información para dichas Subsecretarías, las Secretarías Regionales Ministeriales y los Servicios de Salud.

8. Que, conforme a lo dispuesto en el número 3, del artículo 1°, de la referida Resolución Exenta, la estructura documental del sistema de seguridad de la información estará conformado, entre otros documentos, por una política general de seguridad de la información, definida como la política que establece el enfoque de la organización para administrar sus objetivos de Seguridad de la Información.

9. En este contexto, y habiendose dejado sin efecto Resolución Exenta N°781, de 14 octubre de 2014 mediante la citada Resolución Exenta N°xxx, venimos a actualizar la política general de seguridad de la información para las Subsecretarías de Salud Pública y Redes Asistenciales, para lo aprobamos la siguiente:

RESOLUCIÓN:

ARTÍCULO 1°.- APRUÉBESE la siguiente Política General de Seguridad de la Información para la Subsecretaría de Salud Pública y para la Subsecretaría de Redes Asistenciales:

1. DECLARACION INSTITUCIONAL

El Ministerio de Salud (MINSAL) se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, 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. Para estos efectos, el Minsal se basará 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.

Para la gestión de la Seguridad de la Información al Interior del MINSAL se ha decidido contar con un programa de implantación del tipo "Sistema de Gestión de Seguridad de la Información" (SGSI), basado en los requisitos de la Norma NCh-ISO27001:2013, y las prácticas para los controles de seguridad de la Norma NCh-ISO27002:2013, 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, la dirección del 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.

- Promover 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 27001:2013 y otras normativas vigentes que, conforme a lo dispuesto en el número 7 de esta política general, estarán disponibles permanentemente en el sitio web de MINSAL[1].

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

2.1 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.

2.2 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 planes 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.

3. 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, en el Nivel Central.

Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27001.Of2013:

- A.5.1.1 Políticas para la seguridad de la información.
- A.5.1.2 Revisión de las políticas de seguridad de la información.
- A.8.1.2 Propiedad de los activos.

4. GESTIÓN DE LA POLITICA Y OTROS DOCUMENTOS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

Conforme a lo dispuesto en el número 3, del artículo 1º, de la Resolución Exenta Nº1161, de 4 de octubre de 2016, que aprueba el Sistema de Seguridad de la Información para las Subsecretarías de Salud Pública y Redes Asistenciales, las Secretarías Regionales Ministeriales y los Servicios de Salud, la estructura documental de ese sistema está compuesto por una Política General de Seguridad de la Información, políticas específicas de seguridad de la información, procedimientos de operación, instructivos y registros.

[1] http://web.minsal.cl/seguridad_de_la_informacion/

La referida estructura documental aplicable a las Subsecretarías de Salud Pública y de Redes Asistenciales deberá ser aprobada por los respectivos Subsecretarios y será revisada (a lo menos cada dos años) por el Encargado de Seguridad del Nivel Central y el Comité de Seguridad del Nivel Central a que se refieren los números 4 y 5 de la citada Resolución Exenta Nº1161, de 4 de octubre de 2016.

La documentación aplicable a las Subsecretarías de Salud Pública y de Redes Asistenciales debe asegurar:

- Integren el modelo de seguridad con las metodologías y políticas existentes para ambas Subsecretarias.
- Cumplan con la normativa definida en la Resolución Exenta Nº1161, de 4 de octubre de 2016, que aprueba el Sistema de Seguridad de la Información para las Subsecretarías de Salud Pública y Redes Asistenciales, las Secretarías Regionales Ministeriales y los Servicios de Salud.
- 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.

Las versiones vigentes de la normativa del SGSI y los documentos de apoyo, serán publicados en el sitio web de MINSAL (http://web.minsal.cl/seguridad_de_la_informacion/), además de otros sitios o lugares de fácil acceso a los funcionarios.

5. ROLES Y RESPONSABILIDADES

La estructura organizacional para la gestión de la seguridad de la información en la Subsecretaría de Salud Pública y de Redes Asistenciales, estará compuesta por:

a) El **Comité de Seguridad de la Información Nivel Central** a que se refiere la Resolución Exenta Nº1161, de 4 de octubre de 2016, que aprueba el Sistema de Seguridad de la Información para las Subsecretarías de Salud Pública y Redes Asistenciales, las Secretarías Regionales Ministeriales y los Servicios de Salud; y tendrá los roles y responsabilidades que se definen en el número 4.2 de dicha resolución.

b) El **Encargado de Seguridad de la Información Nivel Central**, a que se refiere la Resolución Exenta Nº1161, de 4 de octubre de 2016, que aprueba el Sistema de Seguridad de la Información para las Subsecretarías de Salud Pública y Redes Asistenciales, las Secretarías Regionales Ministeriales y los Servicios de Salud; y tendrá los roles y responsabilidades que se definen en el número 5 de dicha resolución y en la resolución que lo nombre.

c) El **Propietario de la información**, entendiéndose por tal 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.

d) **Usuario de la información**. entendiéndose por tal, la persona -internas y/o externa al Minsal- 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:

- Utilizar la información sólo para el propósito para el que recibió autorización de uso.
- Conocer las políticas y procedimientos de Seguridad de la Información que se han institucionalizado.
- Cumplir con los controles establecidos en las políticas y procedimientos definidos en el Sistema de Seguridad de la Información aprobado mediante Resolución Exenta Nº1161, de 4 de octubre de 2016, de los Subsecretarios de Salud Pública y de Redes Asistenciales, o el texto que lo reemplace.
- Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.
- Comunicar los incidentes relativos a la seguridad de la información.
- Responder por el uso de cualquier recurso de procesamiento de la información y cualquier uso desarrollado bajo su responsabilidad.

Todos los funcionarios, personal a honorarios y terceros tienen la responsabilidad de utilizar la información y activos de información a los que tienen acceso sólo para el uso específico al que se ha destinado y no comunicar, diseminar o de alguna forma hacer pública la información a ninguna persona, firma, compañía o terceros. En particular, el ejercicio de funciones en el Ministerio de Salud, se debe realizar en el contexto de las siguientes normas:

a) Ley 19.628 Sobre la protección de la vida privada, Ministerio Secretaría General de la Presidencia.
b) Ley 20.285 Sobre acceso a la información pública, Ministerio Secretaría General de la Presidencia.
c) D.F.L. Número 29 Fija texto refundido, coordinado y sistematizados de la Ley N° 18.834, sobre estatuto Administrativo.
d) Ley 19.653 ministerio Secretaría General de la Presidencia, Sobre Probidad Administrativa aplicable a los Órganos de la Administración del Estado.

6. IDENTIFICACION DE RIESGOS

En cumplimiento de lo dispuesto en la letra d), del número 4.2, del Sistema de Seguridad de la Información aprobado mediante Resolución Exenta Nº1161, de 4 de octubre de 2016, de los Subsecretarios de Salud Pública y de Redes Asistenciales, a lo menos cada dos años el Comité de Seguridad de la Información Nivel Central, debe gestionar la actualización de los riesgos de seguridad de la información del Nivel Central, que debe ser construido a partir del análisis de las amenazas y vulnerabilidades a los que se encuentran expuestos los activos de la información relevantes. La metodología de análisis y gestión de riesgos debe estar enfocado en los procesos de provisión institucional, sus actividades, actores y activos, siendo referente:

- CAIGG, apartado Líneas de Acción / Gestión de Riesgos, en el sitio web http://www.auditoriainternadegobierno.cl/.
- Norma NCh-ISO 31000:2012 – Principios y directrices para la Gestión de Riesgos.
- Marco COSO ERM – www.coso.org.
- DIPRES, Guía Metodológica Sistema de Seguridad de la Información.

En el caso de los riesgos residuales, deben ser relevados por el Comité de Seguridad de la Información Nivel Central, al Comité de Riesgos de la Institución para su análisis.

7. DIFUSION

Sin perjuicio de lo señalado en párrafo final del número 4 de esta Política General de Seguridad de la Información, la comunicación de los documentos que componen el Sistema de Seguridad de la Información se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios; y, a lo menos, se deberá hacer difusión mediante los siguientes canales:

- Publicación en la página web de MINSAL http://web.minsal.cl/seguridad_de_la_informacion
- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

8. CUMPLIMIENTO

Todos los usuarios del Ministerio de Salud, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deberán dar complimiento, en lo que les corresponda, a esta Política General de Seguridad de la Información, las políticas específicas y los procedimientos relacionados que se aprueben al efecto.

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.

9. 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 MINSAL. 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.

ANÓTESE Y COMUNÍQUESE

DRA. GISELA ALARCÓN ROJAS
SUBSECRETARIA DE REDES ASISTENCIALES

DR. JAIME BURROWS OYARZÚN
SUBSECRETARIO DE SALUD PÚBLICA

Distribución:

1. Gabinete Ministra de Salud.
2. Gabinete Subsecretario de Salud Pública.
3. Gabinete Subsecretario de Redes Asistenciales.
4. División de Tecnologías de Información y Comunicaciones.
5. Oficina de Partes.