JFD/MGL/sam

MODIFICA RESOLUCIÓN EXENTA NÚM. 600, DE 30 DE MARZO DEL 2011, QUE CREA EL COMITÉ DEL SISTEMA SEGURIDAD DE LA INFORMACION, MODIFICADA POR RESOLUCIÓN EXENTA NÚM. 3.154, DE 30 DE DICIEMBRE DE 2011, Y APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN EN EL INSTITUTO DE SALUD PÚBLICA DE CHILE.

RESOLUCIÓN EXENTA Nº_____/

SANTIAGO, 2768 28.12.2012

VISTOS Y CONSIDERANDO:

PRIMERO: Que, a raíz de la publicación de la Ley Núm. 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, en el año 2004 se publicaron una serie de decretos supremos a fin de reglamentar y operativizar distintos aspectos de la mencionada ley, en el marco del concepto de "Gobierno Electrónico" y del proceso de modernización del Estado. Uno de esos instrumentos, el Decreto Supremo Núm. 83/2005, del Ministerio Secretaría General de la Presidencia, planteó un código de prácticas para la gestión de la seguridad de la información en los órganos del Estado.

SEGUNDO: Que, hacia el año 2007 el Ministerio del Interior, Coordinador del Subcomité de Gestión de Seguridad y Confidencialidad del Documento Electrónico, detectó que en las instituciones del sector público persistían algunas falencias respecto de estos temas, entre las cuales se menciona: aplicaciones y sistemas informáticos con configuración inadecuada; sitios Web de gobierno implementados deficitariamente y con vulnerabilidades conocidas; redes informáticas institucionales con debilidades en sus mecanismos de control de acceso y de regulación del tráfico de datos; problemas de continuidad operacional frente a incidentes de índole recurrente, como los cortes de energía eléctrica; e inexistencia de políticas de seguridad institucionales;

TERCERO: Que, a mediados del año 2009 el Comité de Ministros que rige el desarrollo del Programa de Mejoramiento de la Gestión (PMG), en el marco de la Ley Núm. 19.553, toma la decisión de incluir en el PMG, a partir de 2010, al Sistema de "Seguridad de la Información" - dentro del Área de Calidad de Atención a Usuarios - con el fin de enfrentar los problemas de seguridad detectados, y cuya asistencia técnica queda a cargo de la Red de Expertos conformada por analistas de la Secretaría y Administración General del Ministerio del Interior y de la Dirección de Presupuestos del Ministerio de Hacienda, con el fin de darle el debido impulso a la implementación de las normativas de gestión de seguridad.

CUARTO: Que, igualmente, durante el año 2011, en el contexto de la Ley 20.212 se realiza lo propio para las Metas de Eficiencia Institucional, para su ejecución a partir de 2012. En este contexto se incluyó la Norma Chilena ISO 27001 como referente normativo, cuya propuesta incorpora todo tipo de activos de información, complementando al Decreto Supremo Núm. 83 de 2005;

QUINTO: Que, el Documento Requisitos Técnicos y Medios de verificación Programa de Mejoramiento de la Gestión Año 2012, Programa Marco Básico Versión 2.0 de Mayo de 2012, en la Etapa II de los Requisitos Técnicos, señala que la institución debe establecer el marco para su Sistema de Seguridad de la Información, para lo cual deberá considerar la formulación de una "Política General de Seguridad de la información", aprobada por el Jefe Superior del Servicio, a través de una resolución, la que debe contener, al menos:

- Una definición de seguridad de los activos de información, sus objetivos globales, alcance e importancia.
- Los medios de difusión de sus contenidos al interior de la organización.
- La periodicidad de su reevaluación, que debe ser cada 3 años como máximo, y revisión de cumplimiento.
- El nombramiento del Encargado de Seguridad de la Información, mediante resolución.
- La constitución del Comité de Seguridad de la Información.

SEXTO: Que, de acuerdo a lo anterior, es necesario modificar la Resolución Exenta Núm. 600, de 30 de marzo de 2011, que crea el Comité de Seguridad de la Información, con el objetivo de cumplir con los requisitos técnicos de la cuarta etapa del Programa de Mejoramiento de la Gestión, Sistema de Seguridad de la Información, en el sentido de resguardar los activos de información de la Institución.

SÉPTIMO: Que, para tales efectos se debe incorporar facultades adicionales al Comité en cuanto a la validación de documentos técnicos considerados en el Sistema de Gestión de Seguridad de la Información.

OCTAVO: Que, este Comité del Sistema Seguridad de la Información debe responder eficaz y oportunamente cuando sea requerido por Dirección.

NOVENO: Que, la Norma Chilena ISO 27001 señala en la letra b) de su cláusula 4.2.1, que este Instituto debe "Definir una política del Sistema de Gestión de la Seguridad de la Información en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, que:

1) Incluya un marco de trabajo para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información;
2) Tenga en cuenta los requisitos del negocio, los legales, regulatorios, y las obligaciones de seguridad contractuales;
3) Esté alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI;
4) Establezca los criterios contra los cuales se valorará el riesgo; y
5) Haya sido aprobada por la Dirección; y

TENIENDO PRESENTE las facultades que me confieren los artículos 5 y 11 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado; los artículos 60 y 61 letra a) del Decreto con Fuerza de Ley Núm. 1, de 2005, que fija el texto refundido, coordinado y sistematizado del Decreto Ley Núm. 2.763, de 1979 y de las Leyes Núm. 18.933 y Núm. 18.469; en los artículos 7 y 10 letra a) del Decreto Supremo Núm. 1.222, de 1996, del Ministerio de Salud, que aprueba el Reglamento del Instituto de Salud Pública de Chile; así como lo establecido en la Resolución Núm. 1.600, de 2008, de la Contraloría General de la República; y en el Decreto Supremo Núm. 122, de 28 de diciembre de 2010, del Ministerio de Salud, dicto la siguiente;

R E S O L U C I Ó N

1. MODIFICASE la Resolución Exenta Núm. 600, de 30 de marzo del 2011, en lo siguiente;

a) **INCORPÓRASE** en el numeral uno de la parte resolutiva de la Resolución Exenta Núm. 600, de 30 de marzo del 2011, el siguiente numeral: **"7.- Jefatura de la Unidad de Calidad Institucional o quien ésta designe".**

b) **INCORPÓRASE** en el numeral cuatro de la parte resolutiva de la Resolución Exenta Núm. 600, de 30 de marzo del 2011, los siguientes numerales:

"12. Validar documentos técnicos del Sistema de Gestión de Seguridad de la Información y generar proyectos de desarrollo para el cumplimiento de los requisitos técnicos y normativos, dentro del marco presupuestario vigente.

13. Aprobar las actualizaciones anuales a la Política de Seguridad de la información y documentos asociados".

2. Se deja constancia que los funcionarios realizaran las tareas que le sean asignada, sin perjuicio del cumplimiento de las funciones inherentes a sus cargos.

3. APRUEBASE la Política General de Seguridad de la Información del Instituto de Salud Pública de Chile, cuyo tenor es el siguiente:

a) Objeto

Esta política general define los criterios institucionales relevantes para la administración y gestión del Sistema de Seguridad de la Información.

Del mismo modo la administración, custodia y utilización de la información como también los bienes asociados.

b) Declaración Institucional

El Instituto de Salud Pública de Chile reconoce expresamente la importancia de la información, así como los activos de información, lo anterior por constituir una decisión estratégica de Dirección, ya que puede representar un peligro para la continuidad del negocio o al menos suponer daños importantes por pérdida irreversible de datos, equipos e infraestructura.

Del mismo modo los accesos y usos de la información, deben ser considerados como las demás políticas anexas, en las normas, reglas, estándares y procedimientos que se deriven de ella.

La responsabilidad de la seguridad de la información es de la Dirección, de la Encargada Institucional de Seguridad de la Información y del Comité de Seguridad de la Información.

c) Objetivos del Sistema de la Seguridad de la Información

El presente Sistema de Gestión de Seguridad declara y establece la consecución de los siguientes objetivos:

I. Cumplir la legislación y reglamentación vigente aplicable, y cumplir con los requisitos establecidos voluntariamente.

II. Mantener las políticas de seguridad actualizadas, para asegurar su vigencia y nivel de eficacia.

III. Asegurar la implementación de la seguridad de esta política, identificando los recursos correspondientes.

IV. Se reconoce la seguridad de la información como un atributo necesario en los servicios y productos ofrecidos por el Instituto de Salud Pública.

V. Proteger los recursos de información del Instituto de Salud Pública y la tecnología utilizada para su procesamiento de cualquier amenaza, ya sea interna o externa, deliberada o

accidental, para poder asegurar el cumplimiento de la integridad, confidencialidad, legalidad, disponibilidad y confiabilidad de la información.

VI. Garantizar un ambiente de trabajo que reconozca y valore la actividad en seguridad desarrollada por los equipos técnicos, apoyar además a la generación de una cultura general de trabajo seguro y procedimentado que no aumente los riesgos.

VII. Minimizar el riesgo a que está expuesto el Instituto de Salud Pública con el debido tratamiento y control de riesgo.

VIII. Todo trabajador, proveedor o personal externo que preste sus servicios al Instituto de Salud Pública tiene la obligación de notificar cualquier incidente de seguridad de la información, actividad o situación que afecte la seguridad de los activos de la información.

IX. La información es clasificada de acuerdo a criterios de valoración en relación a la importancia que posee para el Instituto de Salud Pública.

X. La información del Instituto de Salud Pública solo puede ser accedida por personas o entidades externas autorizadas en las situaciones y formas expresamente establecidas en las normativas y decretos vigentes cumpliendo con los controles que garanticen su protección.

XI. El Encargado de la Seguridad de la Información tendrá a su cargo los temas de seguridad, planes, proyectos y programas de capacitación para su implantación y control.

d) Alcance de la Política General de Seguridad de la Información

d.1) Alcance General

La presente Política de Seguridad de la Información del Instituto de Salud Pública de Chile es aplicable a toda la estructura funcional y a todos sus trabajadores, independiente de la calidad jurídica de su contratación.

La Política General de la información del Instituto de Salud Pública, define los lineamientos y criterios que determinan la administración, protección, transmisión y utilización de la información como así mismo los bienes utilizados para producirla, procesarla y almacenarla.

La Política de Seguridad de la Información es parte de la cultura organizacional, y asegura un compromiso de la Dirección y de todas las unidades de la organización para la difusión, consolidación y cumplimiento de la presente política.

d.2) Definición de Activos de Información

Se entiende por Activos de Información todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para Instituto de Salud Pública.

Los niveles básicos de los activos de información son:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los Equipos, Sistemas, Infraestructura que soportan esta información.
- Las Personas que utilizan la información y que tienen el conocimiento de los procesos institucionales.

Los activos de información poseen valor para el Instituto de Salud Pública, y por tanto, deben ser protegidos adecuadamente para que la misión institucional no sea perjudicada. Esto implica identificar riesgos, detectar vulnerabilidades y establecer los controles de seguridad que sean necesarios, tanto a nivel institucional y de gestión de procesos, como a nivel de tecnologías de la información utilizadas.

d.3) Definición de Seguridad de la Información

La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del servicio y minimizar los daños, procurando la Preservación de la confidencialidad, integridad y disponibilidad de la información.

La información es un activo que es esencial para una organización y requiere en consecuencia una protección adecuada.

e) Estructura del Marco de Políticas, Normas y Procedimientos

e.1) Estructura General de la Política

En la Política General de Seguridad de la Información se define una estructura marco para garantizar e implementar una serie de políticas específicas, normas y procedimientos coherentes en materia de la Seguridad de la Información, basada en la Norma NCh-ISO 27001.0f2009, que incluyen los siguientes dominios:

- Organización de la Seguridad de la Información: Orientado a administrar la seguridad de la información dentro del Instituto de Salud Pública y establecer un marco gerencial para controlar su implementación.
- Gestión de Activos: Destinado a mantener una adecuada protección de los activos de información del Instituto de Salud Pública.
- Seguridad de Recursos Humanos: Orientado a reducir los riesgos de error humano, prevención de ilícitos contra del Instituto de Salud Pública o uso inadecuado de los activos de información e instalaciones.
- Seguridad Física y Ambiental: Destinado a impedir accesos no autorizados, daños e interferencia a las unidades y de la información del Instituto de Salud Pública.
- Gestión de las Comunicaciones y las Operaciones: Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.
- Control de Acceso: Orientado a controlar el acceso lógico a los activos de Información
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información: Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su adquisición, desarrollo o implementación y durante su mantenimiento.
- Gestión de Incidentes de Seguridad: Orientado a llevar una gestión acuerda a los incidentes de seguridad de la información que se presenten en el Instituto de Salud Pública.
- Gestión de la Continuidad del Servicio: Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.
- Cumplimiento: Destinado a impedir infracciones y violaciones a las disposiciones legales, reglamentarias, estatutarias o contractuales vigentes que digan relación con los requisitos de seguridad de la información.

e.2) Difusión de la Política

Para la difusión de los contenidos de la política de seguridad de la información al interior de la institución se deberán utilizar los medios de difusión que disponga Instituto de Salud Pública (intranet, boletín, etc.), así como también instancias de capacitación llevadas a cabo para este efecto.

Los principales medios utilizados deben ser los siguientes:

- Intranet institucional
- Folletería o circulares informativas
- Inducción a personal (planta, contrata y honorarios) que ingresen al servicio.
- Comunicaciones a través de charlas y reuniones
- Web institucional

Para el caso de terceros que presten servicios en la institución y a las entidades externas relevantes la difusión se llevara a cabo a través de inducción y entrega de ejemplares de las políticas.

La difusión de las políticas de seguridad de la información estará a cargo del Comité de Seguridad de la Información en coordinación con la Unidad de Comunicaciones e Imagen Institucional, cuando corresponda.

e.3) Evaluación del Cumplimiento de la Política

El cumplimiento de esta política deberá ser monitoreada periódicamente, al menos semestralmente, por el Comité del Sistema Seguridad de la Información de este Instituto, mediante los indicadores establecidos en el Sistema de Seguridad de la Información, los que serán difundidos a la comunidad institucional.

Así como mediante auditorías internas al sistema de seguridad de la información, a intervalos planeados para verificar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

e.4) Revisión de la Política

La política de seguridad de la información será revisada anualmente o cuando ocurran cambios significativos, por el Comité del Sistema Seguridad de la Información de este Instituto, para asegurar su continua idoneidad, eficiencia y efectividad. Los cambios a las políticas de seguridad de la información serán propuestos a la Dirección por el Comité de Seguridad de Información.

f) Roles y Responsabilidades

f.1) La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de Instituto de Salud Pública, cualquiera sea su situación contractual, el área al cual afecta y el nivel de las tareas que desempeñe.

f.2) El Director del Instituto, los Jefes de Departamentos, los Jefes de Subdepartamentos y los Jefes de Unidades del Instituto de Salud Pública, independientes de su nivel jerárquico, son responsables de la implementación de esta Política de Seguridad de la Información, dentro de sus áreas de responsabilidad, y de promover las competencias necesarias para el cumplimiento de dicha Política, por parte de su equipo de trabajo, de acuerdo al alcance definido.

f.3) El Comité de Seguridad de la Información del Instituto de Salud Pública, deberán elaborar y proponer al Director la Política General y Específicas de Seguridad de la Información para su aprobación; Proponer las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, Asegurar que se establezcan, implementen y mantengan los procesos necesarios para el funcionamiento del Sistema de Seguridad de la Información, en concordancia a sus requisitos técnicos; Informar a la Dirección sobre el funcionamiento del Sistema de Seguridad de la Información y de las necesidades de mejoramiento; Velar porque se promueva la toma de conciencia de los requisitos del Sistema Seguridad de la Información; Estudiar, revisar y proponer la documentación que se genere en ámbito de acción del Sistema Seguridad de la Información; Promover la difusión de la seguridad de la información dentro de la institución.

f.4) El Encargado de Seguridad de la Información: será el responsable de tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de. Instituto de Salud Pública; el control de su implementación y velar por su correcta aplicación; coordinar la respuesta a incidentes informáticos o aquellos que afecten a los activos de información institucionales; 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 y finalmente coordinar las acciones del Comité de Seguridad de la Información.

f.5) El Jefe del Subdepartamento de Recursos Humanos al momento de ingresar un nuevo funcionario a la Institución, deberá informar e instruir los derechos y obligaciones que el personal tiene respecto de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo por mandato de la Dirección, tendrá a

su cargo la difusión de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad y las tareas de capacitación permanente en materia de seguridad. Finalmente también se deberá implementar procedimientos o cláusulas de seguridad de activos de la información para difundir y controlar estas medidas a todo personal externo que realice trabajos al interior de las unidades del Instituto de Salud Pública.

f.6) La Jefe de Recursos Humanos, verificará el cumplimiento de la presente Política en la gestión de los contratos de personal; el Jefe del Subdepartamento Abastecimiento será responsable del cumplimiento de la presente política en los contratos que gestione; el Jefe de Asesoría Jurídica verificará el cumplimiento de la presente Política en la gestión de los contratos que le corresponda, asimismo, asesorará en materia legal al Instituto de Salud Pública, en lo que se refiere a la seguridad de los activos de información.

f.7) El Jefe del Subdepartamento Tecnologías de Información y Comunicaciones, cumplirá la función de coordinar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación, tanto de los sistemas como de los recursos de tecnologías de la información de Instituto de Salud Pública. Por otra parte tendrá la función de gestionar las tareas de uso, desarrollo, adquisición y mantenimiento de sistemas institucionales, siguiendo una metodología apropiada al ciclo de vida, que contemplen la inclusión de medidas de seguridad en todas sus etapas.

7.- Glosario de Términos

Para el propósito de los documentos asociados a la seguridad de la información, se aplican los siguientes términos y definiciones.

Activo de Información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para Instituto de Salud Pública.

Seguridad de la Información: La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del servicio y minimizar los daños, procurando la preservación de la confidencialidad, integridad y disponibilidad de la información.

Control: Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Medios de procesamiento de la información: Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

Confidencialidad: Es la necesidad de que la información este en poder de quien corresponda para el desarrollo de las funciones respectivas, con la oportunidad e integridad requerida.

Integridad: Asegurar que la información y sus métodos de procesos son exactos y completos.

Disponibilidad: asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Evento de seguridad de la información: Ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones relativas a las funciones de la institución y amenazar la seguridad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): Parte del sistema de gestión global, basada en un enfoque de riesgo; cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
Evaluación de Riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, con análisis de probabilidad de que ocurran y su potencial impacto en la operatoria del Instituto de Salud Pública.

4. NOTIFIQUESE la presente Resolución a todo el personal de Instituto de Salud Pública, a terceros que presten servicios en la institución y a las entidades externas relevantes.

Anótese, comuníquese y publíquese en la página Web Institucional.

DRA. MARÍA TERESA VALENZUELA BRAVO
DIRECTORA
INSTITUTO DE SALUD PÚBLICA DE CHILE

Resol. A1/N°1066
27/12/2012

Distribución:
- Dirección
- Dpto. ANAMED.
- Dpto. Salud Ocupacional.
- Dpto. Administración y Finanzas.
- Dpto. Salud Ambiental.
- Dpto. Laboratorio Biomédico Nacional y de Referencia.
- Dpto. Asuntos Científicos.
- Subdpto. Recursos Humanos
- Subdpto. Tic.
- Subdpto. Servicios Generales.
- Planificación Estratégica y Control de Gestión.
- Asesoría Jurídica.
- Comunicaciones e Imagen Institucional.
- Sección Mantención de Equipos.
- SALPRI.
- Encargada de la Seguridad de la Información.
- Coordinador de Riesgo Institucional.
- Encargado de Vigilancia y Seguridad Institucional.
- SIAC
- Oficina de Partes.

INSTITUTO DE SALUD PÚBLICA DE CHILE
MINISTRO DE FE

Transcrito fielmente
Ministro de fe