MINISTERIO DE SALUD
GABINETE DE LA MINISTRA
AEG/ JVC/ SMI/ EAR/RGI/SZV

JEFE GABINETE V°B°

APRUEBA POLÍTICA DE SEGURIDAD EN LA GESTIÓN DE PROYECTOS Y MONITOREO DE LOS ACUERDOS DE SERVICIO.

EXENTA N° 1565 /

SANTIAGO, 28 DIC. 2016

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, coordinado 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 Orgánico del Ministerio de Salud; en la ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; la ley 19.628 sobre protección a la vida privada; la ley 20.584 sobre derechos y deberes del paciente; la ley 19.886 de bases sobre contratos administrativos de suministro y prestación de servicios y su reglamento; 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 informáticos; en la Norma Chilena NCh-ISO 27001.0f2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos; en el Memorándum A22 N°10 de 16 de noviembre de 2016 de la Jefa de Departamento Gestión Sectorial de TIC; Resolución Exenta N°1161 de 04 de octubre de 2016 conjunta del Subsecretario de Salud Pública y Subsecretario de Redes Asistenciales que aprueba nuevo sistema de seguridad de la información, la Resolución Exenta N°1332 de 14 de noviembre de 2016 que aprueba la Política General de Seguridad de la Información; 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, de 2004 del Ministerio Secretaria General de la Presidencia.

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, tales como: la Ley 19.886 de bases sobre contratos administrativos de suministro y prestación de servicios y su reglamento; Ley N° 19.799, 2002 sobre documentos electrónicos, firma electrónica y servicios de certificación de firma del Ministerio de economía Fomento y Reconstrucción, Ley N° 19.628, de 1999 sobre protección a la vida privada y datos personales del Ministerio Secretaría General de la Presidencia, Ley N° 19.223, de 1993 sobre delitos informáticos del Ministerio de Justicia, entre otras, con el firme propósito de lograr la protección de los activos relevantes de información y con ello la protección de los derechos de las personas.

4°.- Que, asimismo, el imperativo indicado en el numeral anterior, consiste básicamente o se traduce, entre otras cosas, 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

5°.-Que la seguridad de la información es un tema de suma relevancia para el Ministerio, habida cuenta de la información personal sensible que maneja, existe la necesidad de contar con protocolos claros y exigentes dentro de la organización, que definan los lineamientos y prácticas que deben ser adoptado, siendo una prioridad ministerial, basada en los principios de confidencialidad, integridad y disponibilidad de la información.

6°.- Que internamente han existido procedimientos y políticas anteriores del Ministerio y que en su afán de mejora continua, es necesario modernizar y reemplazar.

7°.- Que, debido a la implementación del sistema de seguridad de la información en conjunto por la Subsecretaría de Redes se ha aprobado por Resolución Exenta N°1332 de 14 de noviembre de 2016 la Política General de Seguridad de la Información.

8°.- Que, en ese contexto se procede a actualizar la política de seguridad en la gestión de proyectos y monitoreo de los acuerdos de servicio, y se aprueba la siguiente,

RESOLUCIÓN :

1º APRUÉBESE la siguiente política de seguridad en la gestión de proyectos y monitoreo de los acuerdos de servicio de la Subsecretaría de Redes Asistenciales y de la Subsecretaría de Salud Pública, del Ministerio de Salud, cuyos textos se incorporan a la presente resolución como anexos.

1. PROPÓSITO

Definir las reglas de seguridad para el resguardo de la información personal sensible para la gestión de los proyectos y monitoreo de los acuerdos de servicio, en los procesos relacionados de compra y administración de los servicios al interior de Minsal.

2. ALCANCE

Esta política es aplicable a los proyectos o servicios donde se encuentre involucrado el uso o tratamiento de datos sensibles, según lo declara la Ley 19.628.

Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Se incluyen los datos que se refieran a los estados de salud presente, pasado, futuro o pronosticado de una persona, incluyendo cualquier información o comportamiento que permita identificar alguna situación médica.

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 la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales.

Abarca los siguientes controles definidos en la norma NCh-ISO 27001.Of2013:

- A.06.01.05 Seguridad de la información en la administración de proyectos.
- A.15.02.01 Monitoreo y revisión de los servicios del proveedor.
- A.15.02.02 Administración de cambios en los servicios del proveedor.

3. DOCUMENTOS RELACIONADOS

- NCh-ISO27001.Of2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información.
- Resolución Exenta N° 636 del 12.08.2011 "Aprueba Manual de Procedimientos de Adquisiciones del Ministerio de Salud".
- Resolución Exenta N°1305 del 08.11.2016 "Modifica Manual de Procedimientos de Adquisiciones del Ministerio de Salud, Resolución exenta N°636"

- Política para acuerdos de intercambio de información y software.
- Procedimiento acuerdos de confidencialidad en contratos con terceros.
- Política de Seguridad para las Relaciones con los Proveedores.
- Ley Nº19.628, de 1999, sobre protección de la vida privada.
- Ley N° 20.285, de 2008, sobre acceso a la información pública.
- Ley N° 20.584, de 2012, regula derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud, y sus reglamentos asociados.

4. ROLES Y RESPONSABILIDADES

Jefe de División o Departamento
Definir a un funcionario o equipo, responsable de la administración de proyectos y los acuerdos de servicios.

Funcionario o equipo responsable
Dar cumplimiento a los requisitos definidos en esta política en la administración de proyectos y los acuerdos de servicio.

5. POLÍTICA

a. Seguridad de la información en la administración de proyectos

En todo proyecto donde esté relacionado el uso o tratamiento de datos de carácter sensible, se debe abordar la seguridad de la información en el diseño, y administración del proyecto, sin importar el tipo de proyecto (proceso comercial, TI, administración de instalaciones, procesos de apoyo, etc.). Se debe identificar y abordan los riesgos de seguridad de la información como parte del proyecto.

Dentro de la administración del proyecto se debe incluir:

a) Dentro de los objetivos del proyecto se deben incluir objetivos de seguridad de la información en concordancia con la información personal sensible tratada.

b) Una evaluación de los riesgos[1] de para la protección de los datos sensibles[2] para identificar los controles necesarios.

c) Una evaluación de los riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios;

d) La seguridad de la información debe ser parte de todas las etapas del proyecto, independiente de la metodología utilizada.

En este tipo de proyectos, la Jefatura responsable debe definir un funcionario que actuará como responsable para la seguridad de la información (puede ser el Jefe de proyecto o parte del equipo del proyecto), quien será el responsable que el proyecto incluya los objetivos y requerimientos de seguridad de la información.

En los proyectos que requieran compras se deben seguir las pautas de seguridad de la información definidas en el punto 5.2 de la presente política.

b. Seguridad de la información en los Proceso de compras

Los procesos de compra se llevarán a cabo de acuerdo a lo definido en la Resolución Exenta N° 636 del 12.08.2011 "Aprueba Manual de Procedimientos de Adquisiciones del Ministerio de Salud" y sus modificaciones, a saber, compras a través de:
- Convenio Marco

---

[1] Se trata de un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

- Licitación o Propuesta Pública
- Licitación o Propuesta Privada
- Trato o Contratación Directa.

Además de incluir las cláusulas de confidencialidad establecidas en el "Procedimiento de acuerdos de confidencialidad en contratos con terceros". Se deberán para aquellos procesos de compras asociados a proyectos donde se encuentre involucrado el manejo o tratamiento de datos personales, incluir cláusulas que permitan proteger la información, dependiendo del tipo de compra:

Convenio Marco

Compras Menores a 1.000 UTM:

Antes de la compra debe existir una revisión del bien o servicio para asegurar que cumple con los requisitos de seguridad de la información definidos en las etapas tempranas del proyecto.

Grandes compras Mayores a 1.000 UTM

Además de la revisión de los bienes y servicios, se deben definir los requisitos de seguridad de la información para resguardar la integridad, confidencialidad y disponibilidad de la información asociada al proyecto y deben ser establecidos en:

- Especificaciones técnicas y administrativas.
- Acuerdo complementario.

Compras a través de Licitación o Propuesta Pública

Antes de la compra debe existir una revisión del bien o servicio para asegurar que cumple con los requisitos de seguridad de la información definidos en las etapas tempranas del proyecto.

Además, se deben definir los requisitos de seguridad de la información para resguardar la integridad, confidencialidad y disponibilidad de la información en:

Licitación o Propuesta Pública Menor a 100 UTM

- Términos de referencia.

- Licitación o Propuesta Pública entre 100 y 1.000 UTM
  - Bases de Licitación.
  - Contrato.

- Licitación o Propuesta Pública entre 1.001 UTM y 4.999 UTM
  - Bases de Licitación.
  - Contrato.

- Licitación o Propuesta Pública mayor o igual a 5.000 UTM
  - Bases de Licitación.
  - Contrato.

Compras a través de Trato o Contratación Directa

Antes de la compra debe existir una revisión del bien o servicio para asegurar que cumple con los requisitos de seguridad de la información definidos en las etapas tempranas del proyecto.

Además, se deben definir los requisitos de seguridad para resguardar la integridad, confidencialidad y disponibilidad de la información en:

- Compras Menores a 1.000 UTM a través de Trato Directo
  - Resolución que aprueba el trato directo.

- Compras Mayores a 1.000 UTM a través de Trato Directo
  - Resolución que aprueba el trato directo.
  - Contrato.

c. Monitoreo y revisión de los servicios del proveedor

En los servicios de proveedores donde se vea involucrado el uso o tratamiento de datos sensibles la División o Departamento encargada de la administración del acuerdo, debe mantener el control y la visibilidad suficientes en todos los aspectos de seguridad para la información o las instalaciones de procesamiento de información personal sensible y crítica que evalúa, procesa o administra un proveedor.

Para lo anterior, el Jefe de la División o Departamento debe definir un funcionario o equipo responsable de administrar las relaciones con el proveedor[3], quienes deberán monitorear, revisar y auditar la prestación de servicios del proveedor de manera regular.

Este monitoreo y revisión de los servicios debe garantizar que se incluyan términos y condiciones de seguridad de la información en los acuerdos definidos en los procesos de compra, y que estos se respeten y que los incidentes y los problemas de seguridad de la información se gestionen correctamente, esto incluye:

a) Monitorear los niveles de desempeño del servicio con el fin de verificar la adherencia a los acuerdos;

b) Revisar los informes de servicio producidos por el proveedor y organizar reuniones de avance de manera regular según lo requieren los acuerdos;

c) Realizar auditorías de los proveedores, en conjunto con la revisión de informes de auditores independientes, en caso de estar disponibles y, un seguimiento de los problemas identificados (para llevar a cabo esta acción se deberían incluir en los contratos que Minsal se reserva el derecho de auditar los servicios prestados, software o producto);

d) Proporcionar información sobre los incidentes de seguridad y revisar esta información según sea necesario conforme a los acuerdos y a cualquier pauta o procedimiento de apoyo;

e) Revisar los seguimientos de auditoría del proveedor y los registros de eventos de seguridad de la información, los problemas operacionales, seguimiento de todas las fallas e interrupciones relacionadas con el servicio entregado;

f) Resolver, gestionar y/o escalar cualquier problema, incidente o evento de seguridad de la información, identificados en los puntos anteriores; así como monitorear la realización de las acciones inmediatas y acciones correctivas / preventivas que permita la resolución de los mismos;

g) Asegurar que el proveedor cumple con las prohibiciones del uso secundario de la información sensible definidos en la compra del servicio, los procedimientos y controles específicos, la criticidad de la información, los sistemas y procesos involucrados.

h) Asegurarse de que el proveedor mantiene una capacidad de servicio suficiente junto con planes de trabajo diseñados para garantizar que se mantienen los niveles de continuidad en el servicio luego de grandes fallas o desastres en el servicio.

d. Administración de cambios en los servicios del proveedor

Cuando existan cambios en la provisión de los servicios, estos deben ser administrados por el funcionario o equipo asignado para el monitoreo, y revisión de los servicios del proveedor. Esta administración de los cambios se debe realizar considerando la mantención y/o mejora de los requisitos de seguridad de la información definidos en la compra del servicio, los procedimientos y controles específicos, la criticidad de la información, los sistemas y procesos involucrados, junto con la reevaluación de los riesgos. Además de lo mencionado se deben considerar los siguientes aspectos:

a) Cambios a los acuerdos del proveedor;
b) Los cambios realizados por la organización por implementar:

- mejoras a los servicios que se ofrecen actualmente;

[3] El administrador del acuerdo no debe ser necesariamente la contraparte técnica para el acuerdo.

- desarrollo de cualquier nueva aplicación y sistemas
- las modificaciones o actualizaciones de las políticas y procedimientos de la organización;
- controles nuevos o cambiados para resolver incidentes de seguridad de la información y mejorar la seguridad;

c) Cambios en los servicios del proveedor a implementarse;

- cambios y mejoras en las redes;
- uso de nuevas tecnologías;
- adopción de nuevos productos o nuevas versiones;
- nuevas herramientas y entornos de desarrollo;
- cambios en la ubicación física de las instalaciones de servicios;
- cambio de proveedores;
- cambios en el equipo del proveedor;
- subcontratación a otro proveedor.

6. DEFINICIONES

UTM: Unidad Tributaria Mensual.

7. DIFUSIÓN

La comunicación de la presente política, se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, 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. REVISIÓN Y MEDICIÓN

La presente política deberá ser revisada a lo menos cada dos años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

2° ESTABLÉSCAZE la obligación de la División de Tecnologías de la Información del Ministerio de Salud, de difundir la presente política y velar por su estricto cumplimiento.

3° INSTRÚYANSE al Jefe de la División de Tecnologías de Información y Comunicaciones 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.

MINISTERIO DE SALUD SUBSECRETARIA DE REDES ASISTENCIALES

DRA. GISELA ALARCÓN ROJAS
SUBSECRETARIA DE REDES ASISTENCIALES

REPUBLICA DE CHILE SUBSECRETARIA DE SALUD PUBLICA MINISTERIO DE SALUD

DR. JAIME BURROWS OYARZÚN
SUBSECRETARIO DE SALUD PÚBLICA

Distribución:
- Jefe de Gabinete Ministra.
- Gabinete Ministra de Salud.
- Jefe de Gabinete Subsecretaría de Redes Asistenciales.
-Jefe de Gabinete Subsecretaría de Salud Pública.
- Jefes de División Subsecretaría de Salud Pública.
- Jefes de División Subsecretaría de Redes Asistenciales.
- Secretarios Regionales Ministeriales de Salud.
- División Jurídica.
- Departamento de Tecnologías de Información y Comunicaciones.
- Oficina de partes.