RESOLUCION EXENTA Nº 7914

PUNTA ARENAS,

09 AGO. 2018

VISTOS: Los antecedentes respectivos: Lo dispuesto en la ley N°19.880 que establece Bases de los Procedimientos Administrativos; en el Decreto con Fuerza de ley N°1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del Decreto Ley N°2763, de 1979 y de 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, forma electrónica y servicios de certificación de dicha firma; en el Decreto Supremo 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 27002 Of.2013; y 10 manifestado en la Resolución Exenta N° 1161 del 04.10.2016 que Aprueba el Sistema de Seguridad de la Información; Resolución Exenta N°4322/26.04.2018 Estructura Orgánica del Servicio de Salud Magallanes; Resolución Exenta N°6440/25.06.2018 que modifica la Resolución Exenta N°4322/26.04.2018; Resolución Exenta N°2888/20.07.2011 de la DSSM, que encomienda como Subdirectora Médica del Servicio de Salud Magallanes a Dra. Maria Cristina Diaz Muñoz; Decreto Exento N°83/12.04.2018 Ministerio de Salud, pone término y establece orden de subrogancia al cargo de Director del Servicio de Salud Magallanes; Decreto Exento N°97/31.05.2018 que modifica Decreto N°83 que establece orden de subrogancia al Cargo de Director del Servicio de Salud Magallanes y en uso de las facultades dicto lo siguiente:

C O N S I D E R A N D O :

La necesidad de contar con adecuadas políticas de seguridad de la información, destinadas a proteger los recursos de información y la tecnología utilizada para su procesamiento. 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,

Memorándum N°15/07.07.2018 de Gestor Regional TI de la Dirección del Servicio de Salud Magallanes, que solicita validar Políticas de Seguridad y Procedimientos,

R E S O L U C I O N

1.- APRUÉBASE a contar del 11 de Julio de 2018 y hasta nueva revisión el **PROCEDIMIENTO ACUERDOS DE CONFIDENCIALIDAD EN CONTRATO CON TERCEROS** del Departamento Control de Gestión y Tecnología de Información y Comunicaciones.

2.- Entiéndase como parte integrante de la presente resolución dicho documento, que a continuación se indica:

Procedimiento Acuerdos de Confidencialidad en Contrato con Terceros

Preparado por:	Andrés Martínez Chamorro.		
Revisado por	Equipo TIC del Servicio de Salud Magallanes		
Revisado por			
Aprobado por:	Pablo Alexis Cona Romero	**Fecha de Aprobación:**	10-07-2018
		Fecha de Publicación:	11-07-2018
		Vigente desde:	11-07-2018
		Vigente Hasta:	Nueva Revisión

Control de versiones

Versión	Fecha de Vigencia	Aprobado por	Fecha publicación	Firma	Comentario
1.0	10-07-2018.	Pablo Cona Romero	11-07-2018		Revisión crítica de la 1era versión. Todas las secciones.

(*) La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

Cualquier pregunta o comentario sobre esta Política de Seguridad de Información dirigirla al Departamento TIC.

ÍNDICE

1. INTRODUCCIÓN

Dentro de la Seguridad de la Información es de vital importancia regular y administrar los contratos con terceros de esta manera garantizar la protección de seguridad de la información.

Es por esto que es imperante que cada vez que se realice un contrato con terceros se genere este acuerdo de confidencialidad o no- divulgación, reflejando la importancia que es para la Dirección de Servicio Salud Magallanes la protección de la información institucional.

PROCEDIMIENTO ACUERDOS DE CONFIDENCIALIDAD EN CONTRATO CON TERCEROS

2. OBJETIVOS

2.1 Objetivo general:

Asegurar el cumplimiento de las políticas, leyes y reglamentos que son aplicables en relación a las cláusulas de seguridad, confidencialidad, propiedad intelectual e integridad de los activos de información de la Dirección Servicio Salud Magallanes, frente a acuerdos y/contratos con terceros.

2.2 Objetivos específicos:

- Este procedimiento define las reglas básicas para la protección de la información en la Dirección Servicio de Salud Magallanes donde entregue y/o traspase a terceros con ocasión de un contrato, acuerdo o negociación.

- Mantener el control y la gestión de los contratos y servicios con terceros celebrados por la DSSM que tienen relación con Informática.

- Incorporar dentro de los contratos con terceros, cuando sea pertinente, las cláusulas relacionadas a la: seguridad de la información institucional, confidencialidad, propiedad intelectual e integridad.

3. ALCANCE

- Este procedimiento se aplica a todos los contratos y servicios de terceros celebrados por la Dirección Servicio de Salud Magallanes y que tienen relación con Tecnología e Informática.

4. ROLES/RESPONSABILIDADES

- Departamento Administración y Finanzas: incorpora en los requerimientos de contratación las cláusulas de Seguridad de la información en los contratos celebrados por Dpto. TIC, con terceros proveedores de servicio.
- Departamento TIC: se encarga de realizar el control de cumplimiento sobre las cláusulas de seguridad.
- Encargado de Seguridad de la Información: revisar, a lo menos una vez al año, que los requerimientos de confidencialidad y no divulgación definidos en este procedimiento reflejen las necesidades de la DSSM para proteger la información.
- Asesores legales: Velar para que los acuerdos de confidencialidad cumplan con los requisitos legales vigentes. Asesorar en la revisión de las cláusulas de confidencialidad.

5. MARCO REFERENCIAL

- Ley 19.886, Ley de bases sobre contratos administrativos de Suministro y prestaciones de servicios.
  - Documento Cláusulas de Confidencialidad y protección de la información en el link *http://web.minsal.cl/seguridad_de_la_informacion*.
  - Decreto Supremo N° 250, del Ministerio de Hacienda, del 9 de marzo 2004, Aprueba reglamento de la ley n° 19886 de bases sobre contratos administrativos de suministro y prestaciones de servicios.
  - Decreto Supremo N° 83, del Ministerio Secretaria General de la Presidencia, del 3 de junio 2004, Aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
  - Política General de Seguridad de la Información.
  - NCh-ISO27001:2009 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos Cláusulas 6.1.5. – 10.6.2.
  - Norma ISO/IEC 27001, capítulos A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
  - Metodología de evaluación y tratamiento de riesgos
  - Informe de evaluación y tratamiento de riesgos
  - Política de control de acceso
  - Declaración de confidencialidad

6. DEFINICIONES

- Información confidencial: Toda aquella que en virtud de lo establecido en la leyes sobre el Acceso a la Información Pública (n° 20.285) y de Protección de Datos Personales (n° 19.628), pueda estar sujeta a restricciones para su divulgación o entrega al público.
- Acuerdo de confidencialidad: Toda cláusula, contrato o convenio que establezca la obligación de proteger la divulgación por terceros, el uso permitido de la información confidencial y la posterior auditoria o supervisión de esta obligación por parte de la Dirección del Servicio de Salud Magallanes

7. DESCRIPCIÓN DEL PROCESO

7.1 SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS

IDENTIFICACIÓN DE RIESGOS DEL ACCESO DE TERCERAS PARTES

Cuando exista la necesidad de otorgar acceso a terceros a la información de la Dirección del Servicio de Salud Magallanes, el Encargado de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información del Organismo.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Dirección del Servicio de Salud Magallanes, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

7.2 REQUERIMIENTOS DE SEGURIDAD EN CONTRATOS O ACUERDOS CON TERCEROS

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de seguridad de la información de la Dirección del Servicio de Salud Magallanes.

b) Protección de los activos de la Dirección del Servicio de Salud Magallanes, incluyendo:

- Procedimientos para proteger los bienes de la Dirección del Servicio de Salud Magallanes, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.

g) Existencia de Derechos de Propiedad Intelectual.

h) Definiciones relacionadas con la protección de datos.

i) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario credencial o logo que a simple vista se detecte a que empresa externa pertenece.
- Proceso de autorización de accesos.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

n) Proceso claro y detallado de administración de cambios.

p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

r) Controles que garanticen la protección contra software malicioso.

s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

t) Relación entre proveedores y subcontratistas.

7.3 CLAUSULAS DE SEGURIDAD

- **Contratos:** "El proveedor se obliga al cumplimiento de lo establecido en las Políticas y Procedimientos de Seguridad de la Información, publicados también por el Ministerio de Salud en su página web, las que deben ser consultadas en el link *http://web.minsal.cl/seguridad_de_la_informacion*."

- **Bases o Términos de referencia:** "Por el solo hecho de participar en el presente procedimiento de compras el oferente deberá dar cumplimiento a las Políticas y Procedimientos vigentes de seguridad de la información, publicados también por el Ministerio de Salud en el link *http://web.minsal.cl/seguridad_de_la_informacion*. Las cuales se presumen conocidas por el oferente, para todos los efectos legales".

7.4 TERCERIZACIÓN
REQUERIMIENTOS DE SEGURIDAD EN CONTRATOS DE TERCERIZACIÓN

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC de la Dirección del Servicio de Salud Magallanes, contemplarán además de los puntos especificados en ("Requerimientos de Seguridad en Contratos o Acuerdos con Terceros", los siguientes aspectos:

a) Forma en que se cumplirán los requisitos legales aplicables.
b) Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del Organismo.
d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del Organismo.
e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.
g) Derecho a la auditoría por parte del Organismo sobre los aspectos tercerizados en forma directa.

Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

7.5 REVISIÓN ACUERDOS DE CONFIDENCIALIDAD

El encargado de Seguridad de la Información, al menos una vez al año, asesorado por el Dpto. Jurídico, debe revisar los requerimientos de confidencialidad y no divulgación definidos en el presente procedimiento.

7.6 FINIQUITO DE LOS ACUERDOS

A los acuerdos de confidencialidad podrá ponérsele término de común acuerdo entre las partes, sin perjuicio de la subsistencia de las demás cláusulas del acuerdo, convenio o contrato.

Sin perjuicio de lo anterior, el acuerdo de confidencialidad cesare conjuntamente con el acuerdo, convenio o contrato a que accede, salvo que se haya estipulado que dicho acuerdo tenga duración indefinida.

EI finiquito del acuerdo, convenio y/o contrato respectivo, deberá indicar la forma de destrucción o devolución de la información una vez finalizados los mismos, de acuerdo a lo establecido en el Procedimiento de destrucción de Activos de Información.

La Dirección de Servicio Salud Magallanes podrá ejercer todas las acciones legales tendientes a reparar el daño que sea provocado por la infracción de cualquier acuerdo de confidencialidad.

7.7 SANCIONES

Los acuerdos de confidencialidad deben ser acatados por todos los funcionarios de la institución y los terceros con los cuales la DSSM se relacione y establezca dichos acuerdos.

La infracción a lo señalado en los acuerdos de confidencialidad, dará lugar a las responsabilidades administrativas y legales que correspondan.

8. METODOLOGIA DE EVALUACIÓN DE PROVEEDORES

La evaluación de los proveedores se debe realizar a través de un cuestionario el que permite obtener un conocimiento general del nivel de madurez del modelo de Seguridad de la Información implementada en la empresa proveedora, el cual debe asegurar la disponibilidad de los servicios que se otorgan a la Dirección Servicio Salud Magallanes, frente a amenazas que podrían interrumpir su normal funcionamiento, por ejemplo, virus, fuga de información, fraude, etc.

El cuestionario mencionado debe ser completado por el responsable de Seguridad de la Información del negocio de la empresa proveedora.

Tópicos del cuestionario de evaluación de proveedores

8.1 Documentos de Políticas de Seguridad de la Información

En este tópico se consulta la existencia de documentación de general de Seguridad de la Información con preguntas tales como:

- Si el proveedor cuenta con una política y documento formal de Seguridad de la Información implementada.
- Si el proveedor cuenta con una política y referencias específicas de Seguridad de la Información implementada.

8.2 Revisión y Evaluación de la Política de Seguridad de la Información

En este tópico se consultan por los planes de Seguridad de la Información con preguntas tales como:

- Si la empresa proveedora cuenta con planes de Seguridad de la Información formalmente documentados para los procesos y servicios críticos que proporciona a la DSSM.

8.3 Administración de Seguridad de la Información al interior de la Organización

En este tópico se consultan por los planes de Seguridad de la Información con preguntas tales como:

- Si la empresa proveedora formula, revisa y aprueba los planes de Seguridad de la Información.
- Si la empresa proveedora tiene procedimientos disciplinarios de Seguridad de la Información en caso de producirse un acceso no autorizado

8.4 Reducir el Riesgo de Errores Humanos, Robos, Fraudes o Mal Uso de las Instalaciones

En este tópico se consultan por los planes de Seguridad de la Información con preguntas tales como:

- Si la empresa proveedora da a todos los usuarios (contratistas, 3ras. partes y empleados) la adecuada educación en seguridad.
- Si la empresa proveedora tiene procedimientos disciplinarios formales para tratar las situaciones en las que un empleado presuntamente ha violado las políticas de seguridad o los procedimientos de la compañía.

8.4 Consideraciones de la evaluación:

- La evaluación de los proveedores es llevada a cabo por el Área Requirente, de acuerdo a la siguiente periodicidad:
- Evaluación Anual: para proveedores críticos, con un contrato de servicios con vigencia superior a 12 meses.
- Cada Área Requirente es responsable de mantener un inventario actualizado de proveedores (realizar un ciclo de actualización, clasificación y evaluación anual de proveedores).

ANEXO 1: CUESTIONARIO DE EVALUACIÓN DE PROVEEDORES DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de este cuestionario es obtener un conocimiento general del nivel de madurez del modelo de Seguridad de la Información implementada en la empresa proveedora, el cual debe asegurar la disponibilidad de los servicios que se otorgan a la DSSM, frente a amenazas que podrían interrumpir su normal funcionamiento, por ejemplo, virus, fuga de información, fraude, etc.

Para tales efectos se ha elaborado el presente cuestionario el que debe ser completado por el responsable de Seguridad de la Información de su empresa y devuelto a través de correo electrónico al Dpto. TIC de la Dirección Servicio Salud Magallanes (Al correo electrónico que se indicará cuando le sea enviado este cuestionario). Si tiene dudas respecto de las preguntas y materias incluidas en este cuestionario, también deberá canalizarlas a través de esta misma dirección de correo.

CUESTIONARIO DE EVALUACIÓN DE PROVEEDORES DE SEGURIDAD DE LA INFORMACIÓN

Fecha de Respuesta:	
Razón Social:	
Nombre:	
RUT Proveedor:	
Dirección de Proveedor:	
Breve descripción de servicio(s) provisto(s) a DSSM:	
Nombre de ejecutivo que responde el cuestionario:	
Cargo:	
Teléfono de Contacto:	

Correo Electrónico:	

Instrucciones de Llenado: Responda "Sí" o "No", o el valor requerido, en el espacio proporcionado después de cada pregunta. Utilice la columna "Observaciones" para fundamentar o complementar sus respuestas.

Cuestionario de Seguridad de la Información			
#	Pregunta	Respuesta (SI/ NO)	Observaciones
1.0	**Documento de Políticas de Seguridad de la Información**		
1.1	¿Hay un documento escrito con la política de seguridad, disponible a TODOS los empleados de la Compañía, responsables de la seguridad de información?		
1.2	¿Contiene la política una definición de la seguridad de información, sus objetivos y alcances generales y su importancia como un mecanismo que facilita el compartir la información?		
1.3	¿Contiene la política una declaración con la intención de la administración de respaldo a las metas y principios de la seguridad de información, así como una definición de responsabilidades generales de la administración y responsabilidades específicas de la Compañía para todos los aspectos de seguridad de información?		
1.4	La política debe contener una referencia a políticas específicas de seguridad de Compañía, los principios, los requisitos de estándares y conformidad. ¿Cuáles de las siguientes áreas están consideradas en la Política? -Requerimientos legislativos y contractuales. -Requerimientos de educación en seguridad. -Prevención y detección de virus. - Consecuencias del incumplimiento.		
2.0	**Revisión y Evaluación de la Política de SI**		

2.1	¿Hay un proceso de revisión definido, incluyendo fechas y responsabilidades, para el mantenimiento de las políticas?		
2.2	La revisión definida, ¿incluye lo siguiente? - Efectividad de políticas - Costo e impacto de los controles - Cambios tecnológicos.		
2.3	¿Tiene la política un propietario claramente definido?		
3.0	**Administrar la Seguridad de la Información al Interior de la Organización**		
3.1	¿La Política de Seguridad Información se formula, revisa y aprueba?		
3.2	¿La administración proporciona una dirección visible y clara que apoyan las iniciativas de seguridad?		
3.3	¿Se asegura que la implantación de los controles de SI se coordina para toda la organización?		
3.4	¿Está explícitamente definida la responsabilidad por la protección de los bienes y la realización de los procesos de seguridad?		
3.5	¿Se incluye la fecha de expiración, incluyendo aquellos casos en donde la confidencialidad debe ser mantenida indefinidamente?		
3.6	¿Se consideran las responsabilidades y acciones de las personas para evitar acceso no autorizado a la información?		
3.7	¿Se consideran los derechos para auditar y monitorear el uso dado a la información confidencial?		
3.8	¿En los contratos con 3ras.partes se considera los requerimientos de seguridad para los accesos, procesamiento, comunicación o administración de la información de la organización o la incorporación de productos o facilidades de servicio de procesamiento de información?		
4.0	**Reducir el Riesgo de Errores Humanos, Robos, Fraudes o Mal Uso de Facilidades**		
4.1	¿Todos los roles y responsabilidades de cargo en la organización incorporan las responsabilidades relevantes en relación con la política de SI?		
4.2	¿Se considera la protección de activos de accesos no autorizados, divulgación, modificación, destrucción de información?		

4.3	¿Se da a todos los usuarios (contratistas, 3ras. partes y empleados) la adecuada educación en seguridad y entrenamiento técnico de acuerdo a lo establecido en los procedimientos y política de seguridad de la organización?		
4.5	¿Existe un procedimiento disciplinario formal para tratar las situaciones en las que un empleado presuntamente ha violado las políticas de seguridad o los procedimientos de la compañía?		
5.0	**Prevenir Acceso Físico No Autorizado**		
5.1	¿Están las facilidades de TI, que soportan actividades críticas o sensibles de la organización, protegidas de accesos no autorizados o de interferencias externas, al estar ubicadas en zonas seguras?		
5.2	¿Se ubican los equipos de forma de reducir el riesgo de amenazas y peligros ambientales y reducir el riesgo de acceso no autorizado?		
5.3	¿Se eliminan los derechos de acceso de 3as.partes, contratistas, usuarios que termina contrato?		

Firma y Timbre del Responsable de la Empresa
Nombre:
Rut:

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

SERVICIO DE SALUD MAGALLANES * DIRECTOR * XII REGIÓN *

MARIA CRISTINA DIAZ MUÑOZ
DIRECTORA (S) SERVICIO SALUD MAGALLANES

MCDM/OPVV/ncr
N° 3424
DISTRIBUCION:
DEPTO. SUBD. RECURSOS HUMANOS
DEPTO. CONTROL DE GESTIÓN Y TECNOLOGIA DE INFORMACION Y COMUNICACIONES
OFICINA DE PARTES

COPIA