RESOLUCION EXENTA Nº 7908

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 la **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** 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:

Política de Seguridad de la Información.

Preparado por:	Andrés Martínez Chamorro.		
Revisado por	Equipo TIC del Servicio de Salud Magallanes		
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	27-03-2014	Mauricio Díaz Cárdenas	27-03-2014		
2.0	03-2016	Pablo Cona Romero	11-07-2018		Revisión crítica de la 1ra 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. DECLARACION INSTITUCIONAL DSSM.

La información es un recurso que, como el resto de los activos, tiene gran valor para la Dirección del Servicio de Salud Magallanes (DSSM), hoy en día las nuevas tecnologías de la información y de las comunicaciones (TIC) son incorporadas progresivamente en los procesos institucionales y en el que hacer de los funcionarios al ejercer sus labores, esto presenta una serie de beneficios, ventajas y oportunidades de diversa índole, pero conlleva también ciertos riesgos, que pueden eventualmente afectar a los activos de información institucional, por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas, minimizando los riesgos de daño y contribuyendo de esta manera a una mejor gestión de la Organización.

Para que estos principios de la Seguridad de la Información sean efectivos, resulta necesaria la implementación de una Política de Seguridad de la Información que forme parte de la cultura organizacional de la Dirección del Servicio de Salud Magallanes, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

Como consecuencia de lo expuesto, la Dirección del Servicio de Salud ha desarrollado políticas de seguridad de la información, siendo estas 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 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.

En el entendido de que los riesgos que se logren identificar estarán siempre presentes, ya que no se pueden eliminar, la institución se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, a través de un programa de implantación de los que se denominara un "Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma Chilena Oficial NCh- IS027001.Of2009.

Dentro de este Sistema de Gestión de Seguridad de la Información es de gran relevancia homogeneizar los criterios de seguridad, teniendo en cuenta que la **Seguridad de la información** es la preservación de la confidencialidad, integridad y de la disponibilidad de la información, entendiendo por estos:

- **Confidencialidad:** se garantiza que la información sea accesible y/o divulgada sólo a aquellas personas autorizadas y que la requieran para el desarrollo de sus funciones.

- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento, no pudiéndose alterar, ni eliminar, por cambios no autorizados o accidentales.

- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran, de manera oportuna y acorde a sus niveles de autorización.

Las Tecnologías de Información y Comunicaciones (TIC) han sido un aporte importante en los procesos de modernización de la gestión del sector Salud, ya que han permitido mejorar y acelerar todos los procesos, eliminando etapas, mejorando los tiempos de respuesta y la eficiencia de las organizaciones.

Por lo cual es importante considerar adicionalmente otros conceptos:

- **Activo:** es todo aquello que contiene información que sea de vital importancia para la Organización.

- **Autenticidad:** asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad:** todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una

transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Los riesgos que afectan a las plataformas TIC son variados y tienen relación tanto con el correcto funcionamiento del equipamiento, como con la ejecución correcta de procesos informáticos y de procedimientos rutinarios de resguardo de la información y del equipamiento, ejecutado por personas adecuadamente entrenadas.

Con el surgimiento de Internet y de las redes que facilitan la interacción con otras organizaciones dentro y fuera del país, los riesgos asociados a las soluciones de gestión basadas en TIC aumentan en forma considerable ya que cada punto de contacto e intercambio de información es a su vez un punto a través del cual la información de nuestros sistemas puede ser afectada en su integridad, en su confidencialidad y en su disponibilidad entre otros aspectos.

La solución a los temas de riesgos asociados a las plataformas TIC y a su interacción a través de las redes de comunicación no se resuelve prescindiendo de ellas ni aislándolas en su funcionamiento mediante la desconexión de las redes que les permiten interactuar con otras organizaciones, sino en adoptar políticas de seguridad adecuadas a nuestra realidad, ejecutándolas correctamente y manteniéndolas permanentemente actualizadas de acuerdo a la situación actual de nuestra organización y de nuestro entorno.

Teniendo en cuenta todo lo anteriormente mencionado a través del presente, el Director(a) del Servicio de Salud Magallanes declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos y principios de la Seguridad de la Información (SI), como también para cumplir con todos los requisitos identificados. Además de desarrollar y ejecutar un plan de mejora

continua asegurando una gestión adecuada de la seguridad de la información según lo dispuesto en todas las normativas vigentes.

2. OBJETIVOS DE LA GESTION DE SEGURIDAD DE LA INFORMACION EN LA DSSM.

2.1 OBJETIVO GENERAL:

Establecer una protección adecuada de los recursos de información de la Dirección del Servicio de Salud Magallanes (DSSM) y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad de la información, a través de un Sistema de Gestión de Seguridad de la Información (SGSI).

2.2 OBJETIVOS ESPECÍFICOS:

- Identificar todos los activos importantes asociados a cada sistema de información de la DSSM, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

- Analizar los riesgos que afectan a los recursos de la información de esta Institución frente a posibles amenazas, ya sean internas o externas.

- Clasificar y valorar los eventos que pueden amenazar la consecución de los objetivos de la Organización y establecer las medidas oportunas para reducir el impacto esperado hasta un nivel aceptable.

- Diseñar e implementar medidas que permitan mitigar los riesgos de procesamiento, conservación y transmisión de la información que sean identificados, del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarla o ponerla en riesgo, sin perder de vista el enfoque de la gestión por procesos institucionales.

- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información, y de esta forma minimizar la ocurrencia de hechos contingentes de posibles amenazas en los medios de almacenamiento y procesamiento.

- Generar planes de continuidad operacional ante hechos contingentes que interrumpan la operación del sistema de seguridad de la información.

- Promover y difundir una cultura organizacional que incorpore la seguridad de la información dentro de la Dirección del Servicio de Salud Magallanes, a través de capacitaciones a los funcionarios a cerca de su responsabilidad en el cuidados de los activos de la institución.

- Mantener la Política de Seguridad de la información del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

- Evaluar y coordinar la implementación de controles específicos de seguridad se la información para los sistemas o servicios de esta organización, sean preexistente o nuevos.

3. ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Para que estos objetivos sean efectivos, resulta necesaria la implementación de esta Política de Seguridad de la Información formando parte activa de la cultura organizacional de la Dirección del Servicio Magallanes, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento con lo cual se ayudará a la preservación y acceso a la información local y la interacción segura con sistemas externos.

La Política General de Seguridad de la Información se aplica a todos los funcionarios de la Dirección del Servicio de Salud Magallanes (planta, contrata, reemplazos y suplencias), personal a honorarios y personal externo que preste servicios, (proveedores, compra de servicios, etc). Que tengan accesos privilegiado a la información, además de contemplar todos los controles contenidos en la NCh-IS027001.0f2009.

4. MARCO NORMATIVO POLITICAS SEGURIDAD DE LA INFORMACIÓN.

La política de la seguridad de la información considera el siguiente marco legal:

- Política de Seguridad de la Información
- Norma ISO/IEC 27001, puntos A.13.2.1, A.13.2.2
- NCh-IS027001.0f2009; Tecnologías de la Información – Técnicas de Seguridad- Sistemas de gestión de seguridad de la información - Requerimientos.
- NCh-IS027002.0f2009; Tecnologías de la Información - Código de prácticas para la gestión de la seguridad de la información.
- Ley N° 17.336, octubre de 1970: Sobre propiedad intelectual. Ministerio de Educación Pública.
- Ley N° 19.223, junio de 1993: Sobre delitos informáticos. Ministerio de Justicia.
- Ley N°19.553, febrero 1998. Concede asignación de modernización y otros beneficios que indica. Ministerio de Hacienda.
- Decreto N°475. Reglamento Ley 19.553 para la aplicación del incremento por desempeño institucional del artículo 6° de la Ley y sus modificaciones.
- Ley N° 19.628, agosto de 1999. Sobre protección de la vida privada y datos personales. Ministerio Secretaria General de la Presidencia.
- Ley N°19.799, abril de 2002. Sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma. Ministerio de Economía.
- Ley N° 19.880, mayo de 2003: Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado. Ministerio Secretaria General de la Presidencia.
- Ley N° 19.927, enero de 2004: Sobre delitos de pornografía infantil. Ministerio de Justicia
- Ley N°20.212, agosto de 2007. Modifica las leyes N° 19.553, N° 19.882, Y otros cuerpos legales, con el objeto de incentivar el desempeño de los funcionarios públicos. Ministerio de Hacienda.
- Ley N° 20.285, agosto de 2008. Regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la administración del Estado. Ministerio Secretaria General de la Presidencia.

- DS N°77. Norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre éstos y los ciudadanos.
- DS N°81. Norma técnica para los órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos.
- DS N°158. Modifica D.S. N° 81 sobre norma técnica para la interoperabilidad de los documentos electrónicos.
- DS N°83. Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- DS N°93. Norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
- DS N°100. Norma técnica para el desarrollo de sitios web de los órganos de la
- Administración del Estado.
- DS N°181. Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
- Instrucción General N°2, mayo de 2009, del Consejo para la Transparencia: Designación de Enlaces con el Consejo para la Transparencia.
- Instrucción General N°3, mayo de 2009, del Consejo para la Transparencia: índice de Actos o Documentos calificados como secretos o reservados.
- Instructivo Presidencial N°4, junio de 2003: Imparte instrucciones sobre aplicación de la Ley de Bases de Procedimientos Administrativos.
- Instructivo Presidencial N° 05, mayo de 2001: Define el concepto de Gobierno Electrónico. Contiene la mayor parte de las instrucciones referidas al desarrollo de Gobierno Electrónico en Chile.
- Instructivo Presidencial N° 06, junio de 2004: Imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la administración del Estado, para dotar así de un mayor grado de seguridad a las actuaciones gubernamentales que tienen lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos.
- Instructivo Presidencial N°08, diciembre de 2006: Imparte instrucciones sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.
- Circular N°3, enero de 2007: Detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del

instructivo presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado.
- Guía Metodológica del Sistema Gobierno Electrónico.
- Guía Metodológica del Sistema de Gestión de Seguridad de la Información.
- Política de Clasificación de la Información
- Política de seguridad para proveedores

5. MARCO GENERAL DE LAS POLITICAS SEGURIDAD DE LA INFORMACIÓN.

La Política General de Seguridad de la Información ha sido elaborada en concordancia con la legislación vigente en el país, considerando además su compatibilidad con las prácticas sugeridas en la NCh 27002 Of.2009.

La Dirección se compromete a realizar las acciones que estén a su alcance para permitir la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

5.1 DEFINICIONES

Información: la información es la interpretación que se da a un conjunto de datos, pudiendo residir está en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos de la DSSM, así como antecedentes proporcionados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

Información Pública: toda aquella información no catalogada como secreta o reservada, tal como lo establece el ordenamiento jurídico vigente

Información reservada (conocimiento reservado) : son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter, cuando la naturaleza misma de la información requiera ser tratada de manera reservada.

La información secreta (solamente a quien le atañe la información debe conocerlo): son aquellos documentos cuyo conocimiento está circunscrito a las autoridades o personas a las que vayan dirigidos y a quienes deban intervenir en su estudio y resolución, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter. Una norma que establece restricciones claras es la ley de datos personales.

Seguridad de la Información: es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

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

Podemos distinguir 3 tipos de activos:

a) La Información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, etc.).

b) Los Equipos/Sistemas que la soportan.

c) Las Personas que la utilizan. Los activos poseen valor para la organización, y necesitan por tanto ser protegidos adecuadamente, para que no se vea perjudicado.

5.2 ROLES Y RESPONSABILIDADES

5.2.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI): es el cuerpo integrado por representantes de todas las áreas sustantivas del DSSM, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

El Comité de Seguridad de la Información (CSI), mediante la Resolución Exenta Nº1581/04.04.2012, tiene los siguientes objetivos:

- Revisar y proponer al Director(a) del Servicio de Salud, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información

que fueran convenientes y apropiadas elaboradas por el Encargado de Seguridad de la Información para la Dirección del Servicio de Salud Magallanes.

- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de esta Institución frente a posibles amenazas, sean internas o externas.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de esta Organización.

- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada sector, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Recomendar roles y responsabilidad específicos que se relacionen con la Seguridad de la Información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de esta Organización, sean preexistente o nuevos.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Dirección del Servicio de Salud Magallanes, como así, coordinar el proceso de administración de la continuidad de las actividades.

La creación del Comité de Seguridad de la Información se corresponde en un todo con el espíritu y la letra, expresados en el Modelo de las Política de Seguridad de la Información para Organismos de la norma ISO 27001 y controles de la norma ISO 27002.

5.2.2 ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

Se describe a modo de resumen algunas de las funciones del cargo actual:

- **Políticas de Seguridad:**
  - Tener a su cargo el desarrollo de las políticas de seguridad al interior de la organización y el control de su implementación, y velar por su correcta aplicación.
  - Generar en conjunto con el Comité de Seguridad de la Información, los controles, registros e indicadores que implementen las políticas.
  - Verificar el cumplimiento de estas políticas.

- **Organización de Seguridad:**
  - Establecer responsabilidades asociadas a la protección de los activos y procesos específicos:
  - Identificar y definir claramente los activos y procesos asociados a cada sistema individual.
  - Debe definirse el administrador responsable por cada activo o proceso de seguridad y los detalles de esta responsabilidad deben estar documentados.
  - Los niveles de autorización deben estar claramente definidos y documentados
  - Crear el equipo de respuesta ante incidentes y comité de Seguridad que de soporte a las políticas establecidas.
  - Establecer la estrategia y promoción para la realización de planes de difusión y concientización de seguridad.
  - Establecer y desarrollar relaciones con organismos externos, como servicios de emergencias, entes reguladores, foros, con el fin de establecer las coordinaciones necesarias de apoyo.

- **Gestión de Activos:**
  - Inventariar y clasificar de acuerdo a su grado de sensibilidad los activos que desean ser protegidos.
  - Establecer medidas apropiadas para su protección.

5.2.3 PROPIETARIO DE LA INFORMACIÓN: Es el Jefe o Encargado de la Unidad Organizacional o apoyo correspondiente, responsable de la protección y uso de la información. El propietario de la información es responsable de clasificación de la misma y es responsable del mantenimiento y actualización de dicha clasificación.

También debe participar en la definición de los lineamientos y controles necesarios, así como de su monitoreo con el apoyo del Jefe Regional TIC, en especial con el encargado de la información, para estar en cumplimiento con las normativas y objetivos de la DSSM.

5.2.4 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 solo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitaran 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 solo para el propósito para el que recibió autorización de uso.
  - Conocer las políticas y procedimiento de Seguridad de la Información que se han institucionalizado.
  - Cumplir con los controles establecidos en las políticas y procedimientos definidos en el SGSI y que están relacionadas a su quehacer habitual.
  - Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.

5.2.5 RECURSOS HUMANOS.

La gestión de la Seguridad de la información, al igual que la mayoría de los ámbitos de las gestiones, depende principalmente de las personas que componen la Organización, ya que son estas, quienes en último término, deben gestionar adecuadamente este importante recurso. Es por esto la gran importancia de este departamento en el reclutamiento, formación, capacitación y selección de los funcionarios de la DSSM, como así también de la gestión de la salida, empleados que abandonan la Organización o la implementación de la normativa interna. Dos grandes puntos fundamentales en el ciclo de vida de todo empleado: el inicio de su actividad profesional y la finalización de la misma.

6. ACEPTACIÓN POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DSSM.

Las políticas de seguridad de la información será aprobada por el (la) Director(a) Dirección Salud Magallanes, reflejando claramente su compromiso, apoyo e interés en el desarrollo de una cultura de seguridad de la información en la institución.

Todos los funcionarios de la DSSM, deberán aceptar esta Política de Seguridad de la Información, así también las políticas específicas y/o procedimientos relacionados.

7. DIFUSIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DSSM.

Resulta clave para que la presente política se integre en la cultura organizacional, la existencia de un plan formal de difusión, capacitación y sensibilización en torno a la seguridad de la información.

La Dirección del Servicio Salud Magallanes a través del Encargado de la Seguridad de la Información debe asegurarse de que todos los empleados de la Dirección del Servicio de Salud Magallanes, como también los participantes externos correspondientes, estén familiarizados con esta Política a través de canales accesibles para la comunicación continua de todas las políticas generadas en el marco del Sistema de Gestión de Seguridad de la información, medios tales como, Capacitación, Charlas, Intranet, Correo electrónico, documentos impresos, etc.

Toda la información pertinente sobre esta Política de Seguridad de la Información, procedimientos, documentos, serán debidamente informadas a cada funcionario a través de correos masivos, boletines informativos u otras actividades de difusión que sean diseñadas para tal efecto.

8. REVISIÓN Y MEDICIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Las directrices y alcances contenidos en esta política son susceptibles de mejorar continuamente, factibles de realizar modificaciones, actualizaciones de modo de mantener una vigencia actual.

La Dirección Servicio Salud Magallanes debe procurar revisar el SGSI al menos cada dos años o cada vez que se produzca una modificación significativa; y debe elaborar minutas de dichas reuniones, el objetivo de las verificaciones por parte de la dirección, es establecer la conveniencia, educación y eficacia del SGSI.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información en el cargo de "Promotor" realizará revisiones independientes sobre la vigencia e implementación de las Políticas de Seguridad de la Información, a efectos de garantizar que las prácticas de la Dirección del Servicio de Salud Magallanes reflejan adecuadamente sus disposiciones.

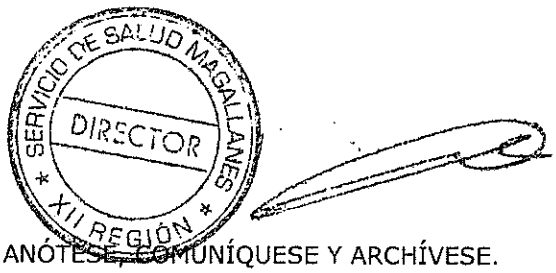
Al menos una vez cada tres años el Comité de Seguridad de la Información Sectorial debe evaluar y revisar el cumplimiento de la Política General de Seguridad de la Información, para esto se debe considerar lo siguiente:

- Retroalimentación de partes interesadas.
- Resultados de las revisiones efectuadas por terceras partes.
- Estado de acciones preventivas y correctivas.
- Cambios en los procesos institucionales, directiva, 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.

9. SANCIONES PREVISTAS POR INCUMPLIMIENTO

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad y de las Políticas específicas del Sistema, Procedimientos y documentos que se deriven de estos, todo esto conforme a lo dispuesto por las leyes y normas vigentes y aplicables bajo el Estatuto Administrativo que rigen al personal de la Dirección del Servicio de Salud Magallanes, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.

Se procederá al término anticipado del contrato cuando el incumplimiento sea por parte de personas que no tengan responsabilidad administrativa o empresas que se encuentre dentro del alcance de esta política, sin perjuicio de las responsabilidades civiles y/o penales que surjan de tales infracciones.



ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

MARIA CRISTINA DIAZ MUÑOZ
DIRECTORA (S) SERVICIO SALUD MAGALLANES

MCDM/OPVV/ncr
Nº 3418
DISTRIBUCION:
DEPTO. SUBD. RECURSOS HUMANOS
DEPTO. CONTROL DE GESTIÓN Y TECNOLOGIA DE INFORMACION Y COMUNICACIONES
OFICINA DE PARTES

COPIA