RESOLUCION EXENTA Nº 7913

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 ASPECTOS ORGANIZATIVOS DE SEGURIDAD DE LA INFORMACIÓN DIRECCIÓN SERVICIO DE SALUD MAGALLANES** 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:

Aspectos Organizativos de Seguridad de la Información DSSM

Preparado por:	Andrés Martínez Chamorro.		
Revisado por	Equipo TIC del Servicio de Salud Magallanes		
Aprobado por:	Pablos 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			Revisión crítica de la 1ra versión. Todas las secciones.
3.0	10-07-2018	Pablo Cona Romero			**[ISO/IEC 27002:2013. Control 6, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5]**

(*) 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 Pág. 2
2. Organización Interna **(ISO/IEC 27002:2013. Controles 6.1)** Pág. 3
3. Objetivos Pág. 4
4. Alcance. Pág. 4
5. Marco referencial Pág. 5
6. Roles y responsabilidades. **[ISO/IEC 27002:2013. Control 6.1.1]** Pág. 5-6
7. Segregación de tareas. **[ISO/IEC 27002:2013. Control 6.1.2]** Pág. 6
8. Contacto con autoridades. **[ISO/IEC 27002:2013. Control 6.1.3]** Pág. 7
   8.1 Definición de contactos ante incidentes /emergencias. Pág. 7
   - Centralización de la información de contactos Pág. 7
   - Tipos de contactos Pág. 7
     1. Contactos críticos Pág. 7
     2. Contactos operacionales Pág. 7
     3. Contactos particulares Pág. 8
     4. Teléfonos Públicos de Emergencia – Red de Seguridad de Punta Arenas Pág. 8

   Pág. 8
   8.2 Elaboración de listado de contactos con autoridades competentes. Pág. 8
   8.3 Información confidencial de contactos Pág. 8
   8.4 Verificación de contactos Pág. 8
   8.5 Descripción del proceso Pág. 9
   8.5.1 Incidentes que pueden afectar los activos de información. Pág. 9
   8.5.2 Activos de información que pueden ser afectados. Pág. 9
   8.5.3 Acciones frente a incidentes Pág. 9
   8.5.3.1 Acciones genéricas Pág. 10
   8.5.3.2 Acciones frente a Incendios, derrumbes, inundaciones, terremotos u otras catástrofes. Pág. 10
   8.5.3.3 Acciones frente a asalto, robo, hurto u otro delito relacionado. Pág. 11
   8.5.3.4 Acciones frente a accidente Pág. 11
   8.5.3.5 Acciones frente a Interrupción de Servicio (Eléctricos, Internet, sistemas informáticos) Pág. 11
   8.5.4 Ejemplos de tipo de incidentes y contactos. Pág. 12
9. Contacto con grupos de interés especial. **[ISO/IEC 27002:2013. Control 6.1.4]** Pág. 13
10. Seguridad de la información en la Gestión de Proyectos **[ISO/IEC 27002:2013. Control 6.1.5]** Pág. 13
11. Glosario de términos Pág. 13

1. INTRODUCCIÓN

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización.

La Dirección del Servicio Salud Magallanes no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC, es necesaria para garantizar su funcionamiento eficaz.

Se entiende por incidentes de seguridad de la DSSM a todo evento que impida el normal funcionamiento de sus Activos de Información y que afecte a la seguridad Informática.

La gestión de incidentes de seguridad tiene por objeto restaurar la operación normal de los Servicios, con tanta rapidez como sea posible y minimizar el impacto adverso a sus procesos, asegurando así que se mantenga debidamente la confidencialidad, integridad y disponibilidad de la información de la DSSM.

El Comité de Seguridad de la Información definirá los procedimientos a seguir en la gestión de incidentes de seguridad, los que deberán ser implementados por el Departamento TIC, bajo la coordinación del Encargado de Seguridad de Activos de Información.

Asimismo, el Encargado de Seguridad de Activos de Información deberá resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los Activos de Información de la Dirección de Servicio de Salud Magallanes acerca de las Políticas de Seguridad de la Información vigentes, y en particular sobre las obligaciones que les correspondan en relación a la gestión de incidentes de seguridad.

Todo el personal que tenga conocimiento de incidentes de seguridad deberá informarlo en la forma más rápida y expedita posible al Depto. TIC, quienes deberán aplicar el procedimiento de gestión de incidentes dispuesto para estos efectos.

2. ORGANIZACIÓN INTERNA [ISO/IEC 27002:2013. Control 6.1]

La Dirección del Servicio de Salud Magallanes a través del dpto. TIC manifiesta su real compromiso y apoyo a través de las políticas que se implementan frente a la Seguridad de la Información, teniendo en cuenta que son el pilar fundamental en la seguridad de todos los activos de la institución, posibilitando una estructura de gestión que permita iniciar y controlar la implementación de Seguridad de la Información en el seno de la DSSM.

Así mismo se compromete a fomentar y desarrollar con un enfoque multidisciplinario de la seguridad de la información, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros y la gestión de riesgos.

Se trabajará en el acceso a fuentes especializadas de consulta en seguridad de la información, externos, con objeto de mantenerse actualizado en las tendencias, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad.

3. OBJETIVOS

3.1. Objetivo general:

Asegurar el cumplimiento de las políticas, leyes y reglamentos que son aplicables en situaciones de ocurrencia de incidentes identificados en la seguridad de la información, con el objeto de realizar los enlaces adecuados y oportunos para la resolución de los incidentes de seguridad de los activos de información de la Dirección Servicio Salud Magallanes.

3.2. Objetivos específicos:

- Establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información dentro de las entidades de la DSSM.
- Fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos a la información propiedad de las entidades de la DSSM.
- Mantener un registro digital, actualizado, con información de los funcionarios de la Dirección del Servicio Salud Magallanes.
- Mantener un registro actualizado de las autoridades nacionales (Ministros, Subsecretario, Intendencias, Poder Legislativo y Poder Judicial) que sean relevantes para el manejo de emergencias mayores en la DSSM.
  - Mantener un registro actualizado de los teléfonos públicos de emergencia.
  - Especificar cuáles autoridades deben ser contactadas oportunamente en caso de incidentes de seguridad de la información.
  - Difundir internamente a quienes corresponda la información de los contactos.

4. ALCANCE

- Este procedimiento se aplica a todos los usuarios de la Dirección del Servicio Salud Magallanes, en relación con otras autoridades que pudieran intervenir en la Seguridad de la Información, sean estas autoridades gubernamentales, entidades públicas, servicios de emergencia con los cuales se mantendrá conexión continua.

5. MARCO REFERENCIAL

- Normá ISO/IEC 27002:2013
- NCh-ISO27001.Of2009 Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información- Requisitos, puntos: A.6.1.6
- Resolución exenta n° 6665, Plan de Emergencias, Dirección Servicio Salud Magallanes, octubre 2014.

6. ROLES / RESPONSABILIDADES [ISO/IEC 27002:2013. Control 6.1.1]

- **Comité Seguridad de la información**

1. Asegurar que las metas de la seguridad de información sean identificadas, relacionarlas con las exigencias organizacionales y que sean integradas en procesos relevantes.
2. Formular, revisar y aprobar la política de seguridad de información.
3. Revisión de la efectividad en la implementación de la política de información.
4. Proveer direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad.
5. Proveer los recursos necesarios para la seguridad de información.
6. Aprobar asignaciones de roles específicos y responsabilidades para seguridad de información a través de la DSSM.
7. Iniciar planes y programas para mantener la conciencia en seguridad de información, asegurando la implementación de los controles de la seguridad de información coordinada a través de la DSSM.

- **Encargado de Seguridad de la Información:**

1. Asegurar que las actividades de seguridad sean ejecutadas en cumplimiento con la política de seguridad.
2. Aprobar metodologías y procesos para seguridad de información, como por ejemplo la evaluación del riesgo y la clasificación de información.
3. Identificar cambios significativos de amenazas y exposición de información.
4. Evaluar la adecuación, coordinación e implantación de los controles de seguridad de la información.
5. Promocionar efectivamente educación, entrenamiento y concientizar en seguridad de información, a través de la organización.

6. Evaluar información de seguridad recibida de monitorear y revisar los incidentes de seguridad de información y recomendar acciones apropiadas en respuesta para identificar incidentes de seguridad de información.
7. Velar por la correcta actualización de los contactos críticos ante eventos de seguridad. Mantener contacto con las autoridades pertinentes.

- **Funcionarios:**

1. Participar e interiorizarse en las políticas de seguridad de la información que rigen a la Dirección Servicio Salud Magallanes.
2. Ante un incidente de seguridad de la información, será de responsabilidad del funcionario que detecte dicho incidente, reportar en forma inmediata a su superior directo, y al encargado de seguridad de la información de la DSSM.

7. SEGREGACIÓN DE TAREAS [ISO/IEC 27002:2013. Control 6.1.2]

Toda tarea en la cual los funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

En concordancia:

• Todos los sistemas de disponibilidad crítica o media de la Institución, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

8. CONTACTO CON AUTORIDADES [ISO/IEC 27002:2013. Control 6.1.3]

8.1 DEFINICIÓN DE CONTACTOS ANTE INCIDENTES / EMERGENCIAS.

Es necesario contar con una base de datos, que sea fácilmente accesible, en caso de una contingencia mayor, para establecer contacto con las autoridades pertinentes, este procedimiento entrega la base para la creación y actualización permanente de este recurso, y los datos que debiera contener, para activarla en el caso mencionado.

Centralización de la información de contactos

- Debe mantenerse una base de datos de contactos críticos para ser utilizados en situaciones de emergencia y/o desastre (operacional, tecnológico).
- El Encargado de Seguridad de la Información será el responsable de su mantención, garantizando su integridad, accesibilidad y actualización.

Tipos de contactos Se definen 4 tipos de contactos:

- Contactos Críticos
- Contactos Operacionales
- Contactos Particulares
- Teléfonos Públicos de Emergencia.

Debiera considerar los siguientes campos:

Departamento/Área/Sección, Cargo, Nombre contacto, Números fijo y celular, Correo electrónico.

1. **Contactos críticos**
   - Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o eventos de seguridad de la Información. Para cada rol, se debe mantener como mínimo un contacto suplente.

2. **Contactos Operacionales**
   - Corresponden al nivel de contacto que se debe mantener en forma centralizada y actualizada para la continuidad en el tiempo de los procesos críticos de la institución.

3. **Contactos Particulares**
   - Se definen como aquellos contactos que pueden ser utilizados en las operaciones normales de la institución, no son obligatorios y pueden mantenerse en bases independientes.

4. **Teléfonos Públicos de Emergencia – Red de Seguridad de Punta Arenas:** Corresponden a números telefónicos públicos de servicios de emergencia, que en este caso particular, no referencian la identificación de una persona.

8.2 ELABORACIÓN DE LISTADO DE CONTACTOS CON AUTORIDADES COMPETENTES

- Toda normativa de seguridad debe identificar los tipos de contactos o roles pertinentes que sean necesarios y lugar donde ubicar la información necesaria para su contacto.
- Es responsabilidad del Encargado de Seguridad confeccionar anualmente, durante el primer trimestre, el listado de las autoridades competentes a contactar.
- Este listado se actualiza de manera semestral o cuando sea necesario.
- El listado con los contactos contiene para cada uno de estos los datos descritos en el **Anexo 1: hoja planilla Excel 1: Contactos Críticos, Contactos Operacionales, Contactos Particulares, Teléfonos Públicos de Emergencia – Red de Seguridad de Punta Arenas.**
- Distribución del Listado de Contactos. Este Listado de Contactos y sus actualizaciones se presentan al Comité de Seguridad de la Información para su validación.
- Una vez validado, se distribuye a través de correo electrónico y resolución.

8.3 INFORMACIÓN CONFIDENCIAL DE CONTACTOS los atributos que se consideran confidenciales son los contactos críticos y están regidos por las Políticas de Seguridad de la Información, por lo cual su divulgación y/o mal uso de estos sean sancionados.

8.4 VERIFICACIÓN DE CONTACTOS

- Los contactos críticos se deben verificar mensualmente.
- Los contactos operacionales, cada 6 meses.

8.5 DESCRIPCIÓN DEL PROCESO

Para el buen funcionamiento de la Dirección Servicio Salud Magallanes es necesario tener el contacto con autoridades tanto internas como externas, con el fin de recurrir a ellos en casos fortuitos en donde se necesite de su ayuda.

Los incidentes de seguridad que pueden estar relacionados con activos de información, son muchos y variados. Se indica a continuación una lista de los más recurrentes. En el caso de producirse otro evento no considerado, éste será incorporado, en la medida que afecte los activos de información de la DSSM.

8.5.1 Incidentes que pueden afectar los activos de información:

- Incendio, humo o situación que genere excesivo calor.
- Inundaciones o anegamientos.
- Ataque a instalaciones.
- Extravío, robo o hurto.
- Daños intencionales.
- Accidentes por caída o impacto de estructuras.
- Accidentes en traslados, instalaciones o reinstalaciones.
- Daños a la infraestructura que deje los activos a la intemperie, o expuesto a los efectos de la naturaleza.
- Daños producidos por eventos de la naturaleza.

8.5.2 Activos de información que pueden ser afectados con ocasión de los incidentes descritos anteriormente:

- Equipos computacionales de escritorio, computadores portátiles, impresoras, escáneres.
- Equipos de comunicaciones, antenas, cables telefónicos o de red de datos.
- Documentación y expedientes de los usuarios y/o funcionarios.
- Archivadores, listados, libros en general, documentación contable.
- Respaldo de información en forma de CD, DVD, cintas, pendrive, discos duros.
- Documentación en general.

8.5.3 Acciones frente a incidentes:

En caso de presentarse un incidente que afecte la Seguridad de la Información, provocando el extravío de documentos por daño parcial o total de la información contenida en ellos debido a un evento inesperado, se deberán ejecutar las siguientes acciones:

8.5.3.1 Acciones genéricas:

1. Cuando un funcionario detecte o visualice la ocurrencia de un incidente, después de aplicar los procedimientos de emergencia establecidos para las respectivas situaciones, y en el caso que dicho incidente afecte a activos de información, o esté relacionado con éstos, deberá comunicarlo al Encargado de Seguridad de la Información y a su jefatura directa.
2. El Encargado de Seguridad de la Información se comunicará con la autoridad que corresponda (Jefe Dpto. TIC, Soporte Informático, etc), según la evaluación que se efectúe del incidente, para coordinar las medidas paliativas y/o correctivas de tratamiento del incidente.
3. El Encargado de Seguridad de la Información registrará en la planilla correspondiente el incidente y emitirá un informe respecto del incidente acaecido, su naturaleza y las medidas adoptadas.
4. En caso de ausencia del Encargado de Seguridad de la Información, le corresponderá al subrogante u otro miembro previamente designado del Dpto. TIC del DSSM, dar aviso a la institución, empresa o servicio que corresponda.

8.5.3.2 Acciones frente a: Incendio, derrumbes, Inundaciones, Terremotos u otras catástrofes:

1. Cuando un funcionario detecte la ocurrencia o inicio en cualquier dependencia o área que amerite una evacuación, deberá dar la alarma en forma inmediata, a través del sistema disponible en ese momento.
2. El Coordinador General designado en el Plan de Emergencias, o bien la persona que detecta la emergencia, procederá a solicitar la concurrencia de las entidades pertinentes (Cuerpo de Bomberos, Carabineros, ONEMI, SAMU, Gasco Magallanes, Edelmag, Aguas Magallanes y/u otros) según la evaluación que se efectúe del incidente.
3. Luego que los Coordinadores Generales apliquen los procedimientos de emergencia establecidos, ante la ocurrencia de una emergencia de estos tipos y en el caso que dicho incidente afecte a activos de información, o esté relacionado con éstos, deberá comunicarlo al Encargado de Seguridad de la Información y a su jefatura directa.
4. El Encargado de Seguridad de la Información se comunicará con la autoridad que corresponda según la evaluación que se efectúe del incidente, para coordinar las medidas de tratamiento del incidente.
5. El Encargado de Seguridad de la Información registrará en la planilla correspondiente el incidente y emitirá un informe respecto del incidente acaecido, su naturaleza y las medidas adoptadas.
6. En caso de ausencia del Encargado de Seguridad de la Información, le corresponderá al subrogante u otro miembro previamente designado del Dpto. TIC del DSSM, dar aviso a la institución, empresa o servicio que corresponda.

8.5.3.3Acciones frente a asalto, robo, hurto u otro delito relacionado:

1. La persona que sea testigo o el mismo afectado debe dar aviso a su Jefatura Directa, al Personal de Seguridad e inmediatamente llamar Carabineros de Chile, informando de lo sucedido y especificar la dirección exacta.
2. Luego de solucionar el problema, el Comité de Seguridad de la Información debe dejar registrada la situación y en el caso de verse comprometida información relevante para la DSSM debe dejarse constancia de aquello.
3. El Encargado de Seguridad de la Información se comunicará con la autoridad que corresponda según la evaluación que se efectúe del incidente, para coordinar las medidas de tratamiento del incidente.

8.5.3.4 Acciones frente a accidente:

1. La persona que presencie esta situación o el mismo afectado debe llamar al Servicio de Ambulancias, informando de lo sucedido, especificando el tipo de accidente y la dirección del lugar, para llevar al afectado al Centro Asistencial más próximo y/o pertinente.

8.5.3.5Acciones frente a Interrupción de Servicio (Eléctricos, Internet, Sistemas Informáticos)

1. Ante la Interrupción de Servicios, principalmente de electricidad, se deberá dar inicio a los procedimientos definidos como importantes, en forma manual para la gestión, los cuales no pueden ser detenidos.
2. Se tomarán las medidas correspondientes para que se pueda operar permanentemente y mantener el suministro a las dependencias.
3. Si el corte de suministro eléctrico abarca un espacio geográfico que impide el uso de los sistemas o si el servicio de Internet entregado por el proveedor se corta o se produce una caída de los sistemas Informáticos a nivel central, los jefes de cada departamento involucrado, deberán aplicar los procedimientos manuales para la atención de usuarios.
4. El encargado de seguridad de la información dará aviso correspondiente a su jefatura directa en caso de que dicho incidente haya afectado a activos de información. Según la evaluación que se efectúe deberá contactarse con las respectivas entidades (Edelmag, Entel, Soporte Minsal), para coordinar las medidas a seguir.

8.5.4 Ejemplos de tipos de incidentes y contactos.

Tipo de Incidente	Contacto
Fuego, incendio, humo o situaciones que consideren alguna alteración por temperaturas altas	Cuerpo de bomberos
Corte de energía eléctrica	Compañía Eléctrica
Inundaciones o anegamientos	ONEMI
Modificación no autorizada del sitio institucional	Departamento TIC
Ataques a instalaciones, motines, protestas, sabotajes, vandalismo, violencia	Carabineros / Jefe Dpto. Tic
Robos y/o pérdidas de información	Departamento TIC
Robos y/o hurtos	Jefe de Área
Daños intencionales: Modificación o eliminación no autorizada de datos. Amenaza o acoso por medio electrónico Ataque o infección por código malicioso (virus, gusano, troyanos, etc) Uso prohibido de un recurso informático Divulgación y/o destrucción no autorizada de Información Intrusión física Acceso o intento de acceso no autorizado a un sistema informático Modificación, instalación o eliminación no autorizada de software	Departamento TIC
Anomalía o vulnerabilidad técnica de software	Departamento TIC
Interrupción prolongada en un sistema o servicio de red	Departamento TIC
Uso indebido de información crítica	Comité de Seguridad de la Información
Eliminación insegura de información	Departamento TIC

9. CONTACTO CON GRUPOS DE INTERÉS ESPECIAL [ISO/IEC 27002:2013. Control 6.1.4]

Se instaurará dentro de las necesidades establecer contacto con grupos o foros de seguridad de la información, especializados y/o asociaciones profesionales.

Con el Objetivo de:

a) Mejorar el conocimiento sobre mejores prácticas y estar actualizado con información relevante de seguridad.
b) Asegurar que el entendimiento del ambiente de seguridad de información es actual y completo.
c) Recibir alertas de detección temprana, advertencias y parches que para los ataques y a las vulnerabilidades.
d) Ganar acceso a consejos especializados de seguridad de información.
e) Compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades.
f) Proveer puntos de enlaces convenientes cuando se trata con información de incidentes de seguridad.

10. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS [ISO/IEC 27002:2013. Control 6.1.5]

La Dirección Servicio de Salud Magallanes cuenta con la Unidad de Proyectos, por lo tanto se establece que las políticas que rigen la Seguridad de la Información también son contempladas en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la DSSM.

11. GLOSARIO DE TÉRMINO

- **Incidente:** Un incidente es aquello que sucede en el curso de un asunto y que tiene la fuerza, por las implicancias que conlleva, de cambiar por completo su curso.
- **Incidente de Seguridad:** Es una amenaza inminente de violación a una política de Seguridad de la Información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad).
- **Activos de Información:** Son aquellos datos o información que tiene valor para una organización.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

SERVICIO DE SALUD MAGALLANES * DIRECTOR * REGION

MARIA CRISTINA DIAZ MUÑOZ
DIRECTORA (S) SERVICIO SALUD MAGALLANES

MCDM/OPVV/ncr
N°3423
DISTRIBUCION:
DEPTO. SUBD. RECURSOS HUMANOS
DEPTO. CONTROL DE GESTIÓN Y TECNOLOGIA DE INFORMACION Y COMUNICACIONES
OFICINA DE PARTES

COPIA