RESOLUCION EXENTA Nº 7912

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 GESTIÓN DE INCIDENTE EN LA 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 Gestión de incidente en la seguridad de la información.

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	11-07-2018	Pablo Cona Romero	07-2018		

(*) 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

INTRODUCCIÓN

La Dirección del Servicio Salud Magallanes necesita responder de forma rápida, eficaz y ordenada a las incidencias de seguridad de la información, estableciendo soluciones a corto plazo para eliminar la amenaza y, posteriormente, implantando soluciones duraderas que eviten la repetición del mismo o parecido tipo de incidencia.

OBJETIVO

Este documento tiene por objetivo definir las líneas de actuación a seguir para gestionar los incidentes de seguridad de información de forma que se puedan adoptar las medidas necesarias para su resolución.

Se destaca que estas acciones son de índole organizativa y corresponden a acciones reactivas que se realizan una vez se tiene algún conocimiento de la ocurrencia de un incidente.

AMBITO

El contenido de este documento es de aplicación para toda la Organización y está dirigido al Comité de Seguridad y los Responsables de Seguridad de Información.

GESTIÓN DE UN INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad que se detecten en los sistemas de información, redes o aplicativos de la DSSM deben ser gestionados de forma eficiente y efectiva, asegurando que se establecen contramedidas adecuadas para evitar que se reproduzca de nuevo el incidente.

Tras la resolución de cada incidente, Seguridad de la Información, debe llevar a cabo un análisis cuyo objetivo es adquirir el conocimiento necesario para eliminar la debilidad o vulnerabilidad que lo generó y para mejorar la respuesta ante futuros incidentes relacionados.

1. Incidencias/Incidentes de Seguridad

Se consideran incidentes de seguridad aquellos eventos adversos, reales o sospechados, relativos a los sistemas de información o las redes informáticas (tales como intrusión a través de la red, infección por virus informático o análisis de vulnerabilidades) efectuados desde sistemas externos o internos a la Dirección del Servicio de Salud Magallanes.

De igual forma se entiende por incidencia de seguridad: cualquier anomalía que afecte o pueda afectar a la seguridad de los archivos que contienen datos de producción de la DSSM, así como los incumplimientos de la normativa de seguridad vigente en cada momento.

2. Comunicación

Las incidencias e incidentes de seguridad deben comunicarse de la siguiente forma:

Incidentes de seguridad:

- Desde usuarios a través de su canal de atención (mail de seguridad)
- Desde Seguridad de la Información a través de los contactos que tenga establecido el responsable de seguridad de la organización.

- El circuito que se define en este documento es de aplicación para toda esta tipología, diferenciando los incidentes según su nivel de severidad.

7. Grados de Severidad

Los grados de severidad son:

ALTO: Corresponde a incidentes que afectan o pueden llegar a afectar la reputación de la DSSM, ya sea por las implicancias legales o de confianza. El Oficial de Seguridad llamará a la conformación del Comité de Seguridad en caso de producirse uno de este tipo.

MEDIO: Son incidentes que pueden llegar a comprometer la reputación de la DSSM si es que no son manejados y/o resueltos en un corto tiempo. En ellos puede existir compromiso de sistemas internos que afecten la disponibilidad de los servicios prestados por la Dirección Servicio Salud Magallanes.

BAJO: Se refiere a alertas de vulnerabilidades conocidas que deben ser gestionadas para evitar efectos colaterales.

Algunos ejemplos de incidentes:

- Descubrimiento de webs paralelas.
- Robos de información.
- Fraudes.
- Amenazas.
- Constancia de que un sistema haya sido comprometido.
- Phishing
- Ataques de Malware:
- Malware no detectados por firmas actuales.
- Malwareque estén afectando a una parte importante de los sistemas.
- Malwareque vayan contra un tipo concreto de servidor.
- Malwareque dejen in-operativa la red.

Ante la sospecha razonable de que la organización esté sufriendo un incidente de los tipos mencionados anteriormente, el Encrgdode Seguridad debe evaluar la severidad de éste bajo los parámetros indicados en el punto anterior.

Una vez establecida la severidad se tomarán las siguientes acciones:

Incidentes de categoría BAJA: estos son manejados por el jefe de Seguridad de la Información y por lo tanto actuará como responsable en el caso. Deberá coordinar las respuestas para eliminar vulnerabilidades tecnológicas y establecer los planes a corto plazo

para resolución, coordinando con el Departamento TIC, disponer de un procedimiento de comunicación y soporte definido. Los resultados de estas acciones serán informados al Encargado de Seguridad de la Información.

Incidentes de categoría MEDIA: En el caso de ser incidentes de tipo tecnológico, serán informados al jefe de Seguridad de la Información, quien debe disponer de su equipo de técnico y otros apoyos técnicos necesarios para la pronta resolución, coordinando la respuesta y manteniendo informado al Encargado de Seguridad. Los incidentes de corte no tecnológico serán informados al departamento TIC con una propuesta de planes de acción por parte del Encargado de Seguridad. Una vez aprobado este accionar se procederá a realizar lo establecido, manteniendo informado al jefe de Seguridad de la Información de los resultados. El Encargado de Seguridad coordinará la ejecución del plan.

Incidentes de categoría ALTA: Para estos incidentes se convocará al Comité de Seguridad a fin de establecer los planes de acción con todas las unidades que puedan dar solvencia a la respuesta. El Encargado de Seguridad es el responsable de coordinar todas las acciones.

En las acciones de respuesta, como responsable de establecer las medidas técnicas que permitan resolver los incidentes de corte tecnológico, estará el Encargado de Seguridad de la Información. Este actúa como cabeza del Equipo de Respuesta a Incidentes Informáticos, conformando un equipo para la situación. Para esto solicitará los recursos humanos y de infraestructura necesarios al jefe de Seguridad de la Información quien debe actuar en consecuencia con la severidad del caso.

En todos los casos, siempre es posible coordinar con otras áreas la solicitud de refuerzos y ayudas técnicas según procedimientos ya establecidos y es responsabilidad del Encargado de Seguridad solicitar esta cooperación.

Toda la documentación del proceso de gestión será resguardada por el Encargado de Seguridad solicitar esta cooperación.

8. Tareas Relacionadas con la Detección y Resolución de Incidentes

Relacionado con la comunicación y resolución de incidentes de seguridad, el Encargado de Seguridad de la Información de la DSSM, debe considerar los siguientes aspectos:

- Hay que concienciar a los empleados cuando reciban avisos que puedan estar siendo afectados por un incidente lo comuniquen cuanto antes a Seguridad de la Información de la organización.

En ocasiones, para poder resolver un incidente, será necesario implicar a otras áreas de la organización. Es necesario que en cada entidad tenga identificadas a las personas que, ante un incidente, puede ser necesaria su participación.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

SERVICIO DE SALUD MAGALLANES * DIRECTOR * XII REGIÓN *

MARIA CRISTINA DIAZ MUÑOZ
DIRECTORA (S) SERVICIO SALUD MAGALLANES

MCDM/OPVV/ncr
Nº 3422
DISTRIBUCION:
DEPTO. SUBD. RECURSOS HUMANOS
DEPTO. CONTROL DE GESTIÓN Y TECNOLOGIA DE INFORMACION Y COMUNICACIONES
OFICINA DE PARTES

COPIA