MINISTERIO DE SALUD
SUBSECRETARIA DE SALUD PÚBLICA
SUBSECRETARIA DE REDES ASISTENCIALES
DIVISIÓN JURIDICA

RBG / JVC / SMB / EAR / MPS

APRUEBA POLÍTICA DE PROTECCIÓN DE SOFTWARE MALICIOSO PARA LA SUBSECRETARÍA DE SALUD PÚBLICA Y PARA LA SUBSECRETARIA DE REDES ASISTENCIALES

EXENTA Nº 1329

SANTIAGO, 14 NOV. 2016

VISTO: Lo dispuesto en la ley Nº19.880 que establece Bases de los Procedimientos Administrativos; en el Decreto con Fuerza de ley Nº1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del Decreto Ley Nº2763, de 1979 y de las leyes Nº18.933 y Nº18.469; en el Decreto Supremo Nº136, de 2004, del Ministerio de Salud, que aprueba Reglamento Orgánico del Ministerio de Salud; en la ley Nº19.799 sobre documentos electrónicos, forma electrónica y servicios de certificación de dicha firma; en el Decreto Supremo Nº83, 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 Nº19.233 sobre delitos informáticos; en la Norma Chilena NCh-ISO 27002 Of.2013; en la Resolución Exenta Nº1231, de 21 de octubre de 2016, que crea la División de Tecnologías de Información y Comunicaciones; y en la Resolución Exenta Nº1161, de 4 de octubre de 2016, conjunta de las Subsecretarías de Salud Pública y de Redes Asistenciales, que aprueba el Sistema de Seguridad de la Información para dichas Subsecretarías, las Secretarías Regionales Ministeriales y los Servicios de Salud.

CONSIDERANDO:

1. Que, las nuevas tecnoclogías de la información y de las comunicaciones (TIC) al ser progresivamente incorporadas a los proceso institucionales y al quehacer personal de los funcionarios en el ejercicio de sus funciones, presentan una serie de beneficios, ventajas y oportunidades de diversa indole. Sin embargo, también conlleva ciertos riesgos que pueden afectar a los activos de información institucional.

2. Que, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente y que consiste basicamente en la realización de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basandose para ello en metodologías y técnicas estándares en estas materias. 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.

3. Que, siendo la seguridad de la información un tema de suma relevancia en el Ministerio de Salud habida cuenta del volumen de información sensible con la que se trabaja, existe la necesidad de contar con una estructura de organización sectorial, que considere la definición de lineamientos y prácticas de seguridad de la información a ser aplicadas a todos los organismos relacionados. En este sentido, es una prioridad para el Ministerio de Salud implementar, mantener y mejorar continuamente la gestión de la seguridad de la Información con una mirada sectorial, basada en preservar los principios de confidencialidad, integridad y disponibilidad de la información.

4. Que, a la fecha, existen una serie de normas en materias de seguridad de la información entre las que se encuentra el Decreto Supremo Nº83, de 2005, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos y la Normas Chilenas NCh-ISO 27001 Of.2013 y NCh-ISO 27002 Of.2013 que proporcionan un marco de gestión de Seguridad de la Informacion utilizable por cualquier tipo de organización, pública o privada.

5. A su vez, internamente, han existido varias normas como la Resolución Exenta Nº781, de 14 octubre de 2014, que aprueba la política general de seguridad de la información; la Resolución Exenta Nº782 de misma fecha que actualiza Comité de Seguridad de la Información Sectorial del Ministerio de Salud; y otras que aprueban políticas y procedimientos particulares de seguridad de la información y que tienen por alcance la Subsecretaria de Salud Pública y Subsecretaria de Redes Asistenciales.

6. Que, sin embargo, en el Ministerio de Salud existe la intención de actualizar y mejorar dicha normativa, y el interés de crear una instancia sectorial que coordine la seguridad de la información no solo a nivel ministerial sino que incluya a los servicios dependientes y relacionados.

7. Que, en ese contexto, a través de la Resolución Exenta N°1161, de 4 de octubre de 2016, conjunta del Subsecretario de Salud Pública y la Subsecretaria de Redes Asistenciales aprobaron un nuevo Sistema de Seguridad de la Información para dichas Subsecretarías, las Secretarías Regionales Ministeriales y los Servicios de Salud.

8. Que, conforme a lo dispuesto en el número 3, del artículo 1°, de la referida Resolución Exenta, la estructura documental del sistema de seguridad de la información estará conformado, entre otros documentos, por políticas específicas de la información, definidas como aquellas que estipulan la implementación de controles de seguridad de la información y que típicamente se estructuran para abordar las necesidades de ciertos grupos objetivo dentro de la organización para abarcar ciertos temas.

9. En este contexto, venimos a aprobar la siguiente política de protección de software malicioso:

RESOLUCIÓN:

ARTÍCULO 1°.- APRUÉBESE la siguiente Política de Protección de Software Malicioso para la Subsecretaría de Salud Pública y para la Subsecretaría de Redes Asistenciales:

1. PROPOSITO

Proteger la información y las instalaciones de procesamiento de la información contra software maliciosos (virus, troyanos, phishing, gusanos, spyware, key loggers y otros).

2. ALCANCE

Esta política es aplicable en MINSAL Nivel central y establece los requisitos de protección contra software malicioso para; estaciones de trabajo (fijas o móviles), servidores y aplicaciones.

Esta política es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para las Subsecretarías de Salud Pública y de Redes Asistenciales.

Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27001.Of2013:
- A.12.02.01 Controles contra código malicioso.
- A.12.06.02 Restricciones sobre la instalación de software.

3. DOCUMENTOS RELACIONADOS

- Política General de Seguridad de la Información, aprobado mediante Resolución Exenta N°xxx, de fecha xxx, de las Subsecretarias de Salud Pública y de Redes Asistenciales.
- Política para la gestión de Hardware y software, aprobada mediante Resolución Exenta N°13, de 7 de enero de 2016, de las Subsecretarias de Salud Pública y de Redes Asistenciales.
- NCh-ISO27001.Of2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información

4. ROLES Y RESPONSABILIDADES

Jefe División de Tecnologías de Información y Comunicaciones
- Proveer los medios para administrar las herramientas contra software malicioso.
- Validar y autorizar las herramientas contra software malicioso.

Departamento de Operaciones, de la División de Tecnologías de Información y Comunicaciones
- Controlar las aplicaciones de MINSAL, respecto a posible inyección de software malicioso.
- Definir formalmente los estándares de los productos de software y hardware para prevenir, contener, detectar y recuperar la introducción de un software malicioso.

- Disponer de medidas de protección adecuadas para la prevención de software malicioso.
- Mantener actualizado los computadores personales y servidores de propiedad del MINSAL y que se conectan a u su red interna, con la última versión de las herramientas contra software malicioso.

Encargado de Seguridad de la Información
- Gestionar los incidentes de seguridad por software malicioso.

Soporte TIC
- Recibir y canalizar cualquier aviso de software malicioso.
- Dar respuesta técnica a los incidentes por software malicioso.

Usuarios
- Reportar cualquier evento que implique software malicioso.
- Cumplir con las reglas y prohibiciones definidas en esta política.

5. POLITICA

5.1 Consideraciones

Las Subsecretarías de Salud Pública y de Redes Asistenciales establecen que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, anti spam, antispyware y otras aplicaciones que brindan protección contra código malicioso.

Será responsabilidad del Departamento TIC, autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

5.2 Protección en estaciones de trabajo (estacionales y portátiles)

Toda estación de trabajo debe contar con una herramienta de protección contra software malicioso instalado y permanentemente actualizado (tanto en su versión de software como en su base de amenazas).

La herramienta debe permitir:

- Activación toda vez que se inicie sesión en el dispositivo y debe permanecer siempre activo.
- Escanear en busca de amenazas cualquier medio removible (pendrive, discos duros, etc.), cuando sea conectado a alguna estación de trabajo. Que la notificación ante la detección de un código malicioso, sea notificada automáticamente.
- Programación automática de busca de bases de nuevas amenazas y escaneo de los equipos donde se encuentra instalado.

Todo equipo que no cuente con una herramienta de protección contra software malicioso, no podrá ser conectado a la red de datos del MINSAL (ver puntos 5.2.1, 5.2.2 y 5.2.3).

5.2.1 Equipos Propiedad de MINSAL
La Unidad de Infraestructura Telecomunicaciones y Seguridad será la responsable de instalar, configurar y dar soporte a la herramienta de protección contra software malicioso.

5.2.2 Equipos en Arriendo
Todo contrato de arriendo debe incluir el requisito de una herramienta de protección contra software malicioso, con una administración centralizada y que cumpla con los requisitos definidos en esta política.

5.2.3 Equipos personales
El dueño del equipo es responsable de tener instalado y actualizado una herramienta de protección contra software malicioso, el uso de estos dispositivos se encuentra normado por la Política de Gestión de Hardware y Software, disponible en http://web.minsal.cl/seguridad_de_la_informacion/.

5.3 Protección a nivel de red

La plataforma de comunicaciones de Minsal debe contar con equipamiento de seguridad que otorgue la protección necesaria ante amenazas, inspeccionando y controlando el tráfico de entrada y de salida para cada una de las LAN de la red.

El equipamiento de seguridad debe permitir:

- Analizar el tráfico de entrada y de salida de internet.
- Controlar las aplicaciones de los usuarios.
- Revisión de correos spam.
- Filtrado de contenidos y control de uso de internet.
- Administración y gestión centralizada de contenidos en la Red Minsal.
- Facilidad e Independencia en la generación de política de filtrado de contenidos.
- Detección de amenazas y control P2P y Mensajería Instantánea.
- Acceso seguro vía VPN.

5.4 Protección en Aplicaciones

Cualquier aplicación que sea desarrollada de forma interna como externa, debe ser controlada durante su desarrollo, paso a producción y operación, para asegurar que no contiene código malicioso.

5.5 No está permitido

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por MINSAL
- Instalar y ejecutar programas, ya sean propios u obtenidos a través de internet, correo u otro medio, en los equipos de la Institución sin la debida autorización del Departamento TIC.
- Modificar los parámetros de configuración de los equipos, así como el software y/o sistemas informáticos instalados.
- Efectuar cambios en la configuración o deshabilitar la(s) herramienta(s) de protección contra software malicioso.
- El uso de cualquier tipo de herramienta que impida o bloquee el normal funcionamiento de la(s) herramienta(s) de protección contra software malicioso.
- Conectar equipos a la red Minsal, que no cuenten con una herramienta de protección contra software malicioso.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Copiar o descargar archivos de medios de almacenamiento externos (pendrive, discos duros, celulares, etc.), sin antes analizarlos con la(s) herramienta(s) de protección contra software malicioso.
- Agregar, borrar o modificar el hardware o software instalado en los equipos sin la autorización del Departamento TIC.

Las presentes reglas serán difundidas a todos los funcionarios según los mecanismos definidos en el punto 7. Difusión de la presente política.

5.6 Controles contra código móvil

En caso de que se autorice el uso de código móvil, la configuración debe asegurar que el código móvil autorizado opera de acuerdo a un procedimiento de seguridad claramente definido y se debe prevenir la ejecución de código móvil no autorizado.

Se deben considerar las siguientes acciones para protegerse contra acciones no autorizadas realizadas por el código móvil:

- Ejecutar código móvil en un ambiente lógicamente aislado.
- Bloquear en forma general, cualquier uso de código móvil.
- Bloquear la recepción de código móvil.
- Activar medidas técnicas disponibles en los sistemas para asegurar que el código móvil es controlado.
- Controlar los recursos disponibles a través del acceso de código móvil.

6. DEFINICIONES

- Virus: Programas maliciosos (**malwares)** que "infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo "víctima" (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y, por tanto, una nueva fuente de infección.
- Gusanos: Son un sub-conjunto de malware. Su principal diferencia con los virus radica en que no necesitan de un archivo anfitrión para seguir vivos. Los gusanos pueden reproducirse utilizando diferentes medios de comunicación como las redes locales, el correo electrónico, los programas de mensajería instantánea, redes P2P, dispositivos USBs y las redes sociales.
- Código Móvil: Software de transferencia entre sistemas, por ejemplo, transferidas a través de una red o mediante una unidad flash USB, y ejecutado en un sistema local sin necesidad de instalación o ejecución explícita por parte del beneficiario. Ejemplos de código móvil incluyen secuencias de comandos (JavaScript, VBScript), Java applets, controles ActiveX, animaciones Flash, películas Shockwave (y Xtras), y macros incrustadas en documentos de Office.
- Spyware: El spyware o software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas.
- Keylogger: Aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado (Capturadores de Teclado). Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.
- Phishing: Consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante.

7. DIFUSION

La comunicación de la presente política, se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la página web de MINSAL http://web.minsal.cl/seguridad_de_la_informacion
- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

8. REVISION Y MEDICION

La presente política deberá ser revisada por el Comité de Seguridad de la Información del Nivel Central, a lo menos cada dos años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

ANÓTESE Y COMUNÍQUESE

DRA. GISELA ALARCON ROJAS
SUBSECRETARIA DE REDES ASISTENCIALES

DR. JAIME BURROWS OYARZÚN
SUBSECRETARIO DE SALUD PÚBLICA

Distribución:
1. Gabinete Ministra de Salud.
2. Gabinete Subsecretario de Salud Pública.
3. Gabinete Subsecretario de Redes Asistenciales.
4. Departamento de Gestión Sectorial de Tecnologías y Comunicaciones.
5. Oficina de Partes.