Gobierno de Chile

MINISTERIO DE SALUD
GABINETE DE LA MINISTRA
VBG/ JVA / SML/ EAR/RGI/SZV

JEFE GABINETE V°B°

APRUEBA PROCEDIMIENTOS ESPECÍFICOS PARA LA SEGURIDAD DE LA INFORMACIÓN.

EXENTA N° 1566 /

SANTIAGO, 28 DIC. 2016

VISTOS: Lo dispuesto en la ley N° 19.880 que establece Bases de los Procedimientos Administrativos; en el D.F.L N°1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinado y sistematizado del decreto ley N° 2763, de 1979 y 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, firma electrónica y servicios de certificación de dicha firma; la ley 19.628 sobre protección a la vida privada; la ley 20.584 sobre derechos y deberes del paciente; el D.S 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 27001.0f2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos; en el Memorándum A22 N°10 de 16 de noviembre de 2016 de la Jefa de Departamento Gestión Sectorial de TIC; Resolución Exenta N°1161 de 04 de octubre de 2016, conjunta del Subsecretario de Salud Pública y Subsecretario de Redes Asistenciales que aprueba nuevo sistema de seguridad de la información, la Resolución Exenta N°1332 de 14 de noviembre de 2016 que aprueba la Política General de Seguridad de la Información, la Resolución N° 1.600, de 2008, de la Contraloría General de la República; y

CONSIDERANDO:

1°.- Que, las nuevas tecnologías de la información y de las comunicaciones (TIC) al ser incorporadas progresivamente a los procesos institucionales y al quehacer personal de los funcionarios al ejercer sus labores en el Ministerio de Salud, presentan una serie de beneficios, ventajas y oportunidades de diversa índole, pero conlleva también ciertos riesgos, que pueden afectar a los activos de información institucional.

2°.- Que, se oficializó la norma técnica sobre seguridad y confidencialidad del documento electrónico para los órganos de la Administración del Estado a través del Decreto Supremo N°83 de 2004, del Ministerio Secretaria General de la Presidencia.

3°.- Que, por consiguiente, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, tales como: Ley N° 19.799, 2002 sobre documentos electrónicos, firma electrónica y servicios de certificación de firma del Ministerio de economía Fomento y Reconstrucción, Ley N° 19.628, de 1999 sobre protección a la vida privada y datos personales del Ministerio Secretaría General de la Presidencia, Ley N° 19.223, de 1993 sobre delitos informáticos del Ministerio de Justicia, entre otras, con el firme propósito de lograr la protección de los activos relevantes de información y con ello la protección de los derechos de las personas.

4°.- Que, asimismo, el imperativo indicado en el numeral anterior, consiste básicamente o se traduce, entre otras cosas, 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 de integridad, confidencialidad y disponibilidad, con todos sus activos de información relevantes para la institución, como un principio clave en la gestión de procesos.

5°.- Que la seguridad de la información es un tema de suma relevancia para el Ministerio, habida cuenta de la información personal sensible que maneja, existe la necesidad de contar con protocolos claros y exigentes dentro de la organización, que definan los lineamientos y prácticas que deben ser adoptado, siendo una prioridad ministerial, basada en los principios de confidencialidad, integridad y disponibilidad de la información.

6°.- Que internamente han existido procedimientos y políticas anteriores del Ministerio y que en su afán de mejora continua, es necesario modernizar y reemplazar.

7°.- Que, debido a la implementación del sistema de seguridad de la información en conjunto por la Subsecretaría de Redes se ha aprobado por Resolución Exenta N°1332 de 14 de noviembre de 2016 la Política General de Seguridad de la Información.

8°.- Que, en ese contexto se procede a actualizar los procedimientos para la gestión de los derechos de acceso y devolución de activos y el procedimiento monitoreo del uso de los medios de procesamiento de información, y teniendo presente lo anterior, se aprueba la siguiente,

RESOLUCIÓN:

1° APRUÉBENSE los siguientes procedimientos específicos de seguridad de la información de la Subsecretaría de Redes Asistenciales y de la Subsecretaría de Salud Pública, del Ministerio de Salud, cuyos textos se incorporan a la presente Resolución como anexos:

1. Procedimiento para la gestión de los derechos de acceso y devolución de activos.
2. Procedimiento monitoreo del uso de los medios de procesamiento de información

2° ESTABLÉSCAZE la obligación de la División de Tecnologías de la Información del Ministerio de Salud, de difundir la presente política y velar por su estricto cumplimiento.

3° INSTRÚYANSE al Jefe de la División de Tecnologías de Información y Comunicaciones y a los Encargados de Seguridad de la Información que realicen las acciones tendientes a la implementación de la presente Política, en materias de su competencia.

4° DÉJESE SIN EFECTO el procedimiento para la gestión de los derechos de acceso y devolución de activos, aprobado por Resolución 780 de 14 de octubre de 2014 y el procedimiento monitoreo del uso de los medios de procesamiento de información aprobado por Resolución 1124 de 22 de diciembre de 2014.

ANÓTESE Y COMUNÍQUESE.

MINISTERIO DE SALUD SUBSECRETARIA DE REDES ASISTENCIALES

DRA. GISELA ALARCÓN ROJAS
SUBSECRETARIA DE REDES ASISTENCIALES

REPUBLICA DE CHILE SUBSECRETARIA DE SALUD PUBLICA MINISTERIO DE SALUD

DR. JAIME BURROWS OYARZÚN
SUBSECRETARIO DE SALUD PÚBLICA

Distribución:
- Jefe de Gabinete Ministra.
- Gabinete Ministra de Salud.
- Jefe de Gabinete Subsecretaría de Redes Asistenciales.
- Jefe de Gabinete Subsecretaría de Salud Pública.
- Jefes de División Subsecretaría de Salud Pública.
- Jefes de División Subsecretaría de Redes Asistenciales.
- Secretarios Regionales Ministeriales de Salud.
- División Jurídica.
- Departamento de Tecnologías de Información y Comunicaciones.
- Oficina de partes.

Contenido

1 PROPÓSITO

Definir las actividades para monitorear el uso de las instalaciones de procesamiento de la información de Minsal en el Nivel Central.

2 ALCANCE

Subsecretarías de Salud Pública y de Redes Asistenciales.

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

Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27001.Of2013:

- A.12.01.03 Administración de capacidad.
- A.12.04.01 Registro de eventos.
- A.12.04.03 Registros del administrador y del operador.
- A.12.04.04 Sincronización con los relojes.

3 TERMINOLOGÍA

MINSAL: Ministerio de Salud.
SGSI: Sistema de Gestión de Seguridad de Información.
DNS: Sistema de nombres de dominio.
CPU: unidad central de procesamiento.

Streaming: es la distribución digital de contenido multimedia a través de una red de computadoras, de manera que el usuario utiliza el producto a la vez que se descarga.
ID: cuenta de usuario, identificador.
Gateway: puerta de enlace, dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más computadoras.
Firewall: cortafuegos, dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.
Cloud computing: es un modelo para permitir el acceso adecuado y bajo demanda a un conjunto de recursos de cómputo configurables (p.e. redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos y puestos a disposición del cliente con un mínimo esfuerzo de gestión y de interacción con el proveedor del servicio.
RAM: memoria de acceso aleatorio.

4 DOCUMENTOS APLICABLES

- NCh-ISO27001.Of2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
- NIST Special Publication 800-92 Guide to Computer Security Log Management.
- Procedimiento gestión de incidentes de seguridad de la información.
- Política de Desarrollo de Sistemas.

5 ROLES Y RESPONSABILIDADES

Departamento de Operaciones de la División TIC

Es responsable del monitoreo de la capacidad de los servidores, servicios y aplicaciones existentes en producción y además el monitoreo del uso de los Equipos de comunicación.

6 PROCEDIMIENTO

6.1 Monitoreo y gestión de la capacidad de los medios de procesamiento de información.

6.1.1 Monitoreo de Servidores

El Departamento de Operaciones de la División TIC debe contar con herramientas para monitorear, a lo menos una vez a la semana, los servidores que tenga bajo su administración, y mantener el registro electrónico de los resultados a lo menos dos años.

El monitoreo a los servidores debe incluir como mínimo:

- Porcentaje de uso de la CPU
- Espacio disponible en Disco Duro
- Memoria RAM

Cuando cualquiera de las tres variables mencionadas sobrepase el 80% de su capacidad, el Jefe del Departamento de Operaciones utilizará la información histórica del uso del(os) servidor(es), para evaluar el aumento de la capacidad o la reducción de la demanda. Algunas medidas para la reducción de la demanda son:

a) eliminación de datos obsoletos (espacio en el disco);
b) sacar de servicio a las aplicaciones, sistemas, bases de datos o entornos;
c) eliminación de los procesos y programaciones de parches;

d) optimización de las consultas de lógicas de aplicaciones o bases de datos;
e) otras alternativas de almacenamiento, como Hosting o VPS (Virtual Private Server).

6.1.2 Monitoreo del estado de los servicios y aplicaciones

El Departamento de Operaciones de la División TIC debe contar con herramientas para monitorear a lo menos una vez a la semana los servicios que tenga bajo su administración, y mantener el registro electrónico de los resultados a lo menos dos años.

Los servicios mínimos que se deben monitorear son:
- DNS (Domain Name Service)
- Video conferencia
- Internet
- Telefonía
- Wireless
- Firewall
- Aplicativos críticos.

6.1.3 Monitoreo de vulnerabilidades

El Departamento de Operaciones de la División TIC deberá contar con herramientas para monitorear de forma aleatoria las vulnerabilidades tanto en le infraestructura tecnológica como en los aplicativos que tenga a su cargo, y mantener el registro electrónico de los resultados a lo menos por dos años.

Para lo anterior se realizarán pruebas de seguridad, las que se podrán determinar usando herramientas especializadas o de manera manual. Junto con ello, la generación de un informe detallado con los resultados obtenidos durante todo el proceso de ejecución de las pruebas, con el correspondiente análisis de dicha información para poder ser interpretada de manera correcta y entender las implicaciones a nivel de seguridad sobre la infraestructura o aplicativos analizados, con las recomendaciones necesarias para solucionar dichos problemas.

6.1.4 Gestión de eventos o incidentes de seguridad:

Durante el monitoreo pueden surgir eventos que pongan en riesgo la seguridad de la información, en esto casos se debe reportar el incidente de acuerdo a lo definido en el "Procedimiento gestión de incidentes de seguridad de la información". Algunos eventos que podrían requerir investigación adicional son:

- Pérdida de servicio, de equipos o de instalaciones.
- Mal funcionamiento o sobrecargas del sistema.
- Errores humanos.
- No cumplimiento con políticas o pautas.
- Cambios de sistema no controlados.
- Mal funcionamiento de software o hardware.
- Violaciones de acceso.
- Exposición de información sensible

Algunos elementos que pueden ser investigados en estos casos son:

a) Acceso no autorizado:
   - identificación (ID) de usuario.
   - fecha y hora de acontecimientos claves.
   - tipos de eventos.

- archivos accedidos.
- programa/utilitario utilizado.

b) Operaciones privilegiadas, tales como:
- empleo de cuentas privilegiadas, por ejemplo, supervisor, raíz (root), administrador.
- arranque y apagado del sistema.
- conexión/desconexión de dispositivos de entrada-salida (I/O).

c) Intentos de acceso no autorizados, tales como:
- acciones de usuario fallidas o rechazadas.
- acciones fallidas o rechazadas que implican datos y otros recursos.
- violaciones de política de acceso y notificaciones para puertas de enlace (Gateway) y cortafuego (firewall) de red.
- alerta de sistemas de detección de intrusión propietarios.

d) Alertas o fallas del sistema, tales como:
- alarmas o mensajes de consola.
- excepciones del registro del sistema.
- gestión de alarmas de red.
- alarmas levantadas por el sistema de control de acceso.

e) Cambios o intentos de cambiar, configuraciones y controles de seguridad del sistema.
f) Descargas masivas de información.
g) Barrido de puertos.
h) Accesos fuera de horario habitual.
i) Accesos con derechos de administrador.
j) Frecuencias anormales de uso del sistema.
k) Envío de información a servidores externos.
l) Tráfico cifrado.
m) Descargas de servidores externos.

6.2 Registros del administrador y del operador

Dado que los usuarios con privilegios pueden manipular los registros en las instalaciones de procesamiento de información bajo su control directo, éstas cuentas deberán ser revisadas al menos cada 12 meses mediante alguna de las siguientes:

- Auditorías internas.
- Auditorías externas.
- Revisión de la Unidad de Control de Gestión, Presupuesto y Aseguramiento de Calidad de la División TIC.

6.3 Sincronización con los relojes

El Departamento de Operaciones de la División TIC, es responsable de la sincronización de los relojes de los sistemas de procesamiento de información que tiene bajo su administración, esta sincronización se realizará a través de las siguientes herramientas:

- Parche de hora de Microsoft.
- Active Directory.

- De forma "manual" para el equipamiento que posea otro sistema operativo.

La hora de referencia que se utilizará será la proporcionada por el Servicio Hidrográfico y Oceanográfico de la Armada.

7 REGISTROS

- Registro Monitoreo de Servidores.
- Registro Monitoreo del estado de los servicios y aplicaciones.
- Registro Monitoreo de vulnerabilidades.

8 DIFUSION

La comunicación del presente procedimiento, 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.

9 REVISION Y MEDICION

El presente procedimiento deberá ser revisado a lo menos cada dos años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

10 CONTROL DE VERSIONES

Versión	Fecha de Aprobación	Motivo del cambio	Secciones modificadas
01	Diciembre 2013	Creación del documento	Todas
02	Octubre 2014	Actualización de los roles y responsabilidades en el monitoreo	6.1 Supervisión 6.2 Revisión
03	Noviembre 2016	Actualización de la normativa de referencia. Se incluyen los controles de registros de administrador y sincronización de relojes.	6.1 Monitoreo y gestión de la capacidad de los medios de procesamiento de información 6.2 Registros del administrador y del operador 6.3 Sincronización con los relojes

ELABORADO POR	Rodrigo Vidal / Control de Gestión TIC
REVISADO POR	José Villa / Encargado de Seguridad de la Información Rodrigo Zamorano / Departamento de Operaciones División TIC Claudio Barra / Departamento de Operaciones División TIC
APROBADO POR	Soledad Muñoz / Presidenta Comité de Seguridad de la Información