Servicio de Salud Metropolitano Sur Oriente
Región Metropolitana
Ministerio de Salud

UNIDAD DE CONTROL INTERNO
DR.FBV. /JTF. /HPR. /clf.

APRUEBA POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DE LA DIRECCIÓN DEL SERVICIO DE SALUD METROPOLITANO SUR ORIENTE

5201 *31.12.2018

RESOLUCION EXENTA N° _____/

PUENTE ALTO,

VISTOS:

Lo dispuesto en la ley N° 19.880 que establece bases de los procedimientos administrativos; 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 2005, 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 del 7 de junio de 1993 del Ministerio de Justifica sobre tipificación de figuras penales relativas a la informática; Resolución N° 1.161 de 4 de octubre de 2016 Subsecretaría de redes y Subsecretaría de Salud, que aprueba el Sistema de Seguridad de la información, en la Norma Chilena NCh-ISO 27002 Of. 2013. Que, de acuerdo a lo dispuesto en el Decreto con fuerza de ley N°1 de 2005 de salud, que fija el texto refundido, coordinado y sistematizado del Decreto de Ley N° 2.763/79 y de las leyes N° 18.933 y N° 18.469; Resolución N° 1600 de 2008, de la Contraloría General de la República y las facultades que me confiere el Decreto Afecto N° 53 de 12 de julio de 2018, de Salud.

CONSIDERANDO:

1.Que, las nuevas tecnologías de la información y de las comunicaciones (TIC) al ser progresivamente incorporadas a los procesos institucionales y al quehacer personal de los funcionarios en el ejercicio de sus funciones, presentan una serie de beneficios, ventajas de diversa índole. Sin embargo, también conlleva 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 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. 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 Servicio de Salud metropolitano sur oriente, por el alto volumen de información sensible con la cual se trabaja, existe la necesidad de contar con una estructura 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 la Dirección del Servicio de Salud implementar, mantener y mejorar continuamente la gestión de la seguridad de la información, basada en 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 N° 83, de 2005, del Ministerio Secretaría 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 las Normas Chilenas NCh- ISO 27001 Of. 2013 y NCh-ISO 27002 Of. 2013 que proporcionan un marco de gestión de Seguridad de la información utilizable por cualquier tipo de organización, pública o privada.

5.Que, conforme a los principios de eficiencia, eficacia y coordinación reconocidos en el artículo N°3 de la ley N° 18.575, orgánica constitucional de bases generales de la administración del Estado, se justifica que la Dirección del Servicio de Salud Metropolitano Sur Oriente, adopte las medidas que estime pertinente para resguardar la seguridad de la información.

6. Que, la Dirección del Servicio de Salud Metropolitano Sur Oriente comprende la importancia de un Sistema de Seguridad de la Información estándar y replicado en los Establecimientos Hospitalarios de la red Sur Oriente, con el objetivo de gestionar la seguridad de la información de forma homogénea en la Dirección del Servicio y red de salud.

7. En este contexto, y por todas las consideraciones expuestas, la Dirección del Servicio de Salud Metropolitano Sur Oriente, define y formaliza la Política de Gestión de incidentes de Seguridad de la información de la Dirección del Servicio de Salud Metropolitano Sur Oriente, dictando lo siguiente:

RESOLUCIÓN

ARTICULO N°1- APRUEBASE Política de Gestión de incidentes de Seguridad de la información, de la Dirección del Servicio de Salud Metropolitano Sur Oriente, que se encuentra descrita en el documento adjunto, como anexo, es parte integrante de la presente Resolución.

ARTÍCULO 2. La presente Resolución surtirá sus efectos a contar de esta fecha

ANOTESE, COMUNIQUESE Y ARCHIVESE

SERVICIO SALUD SUR ORIENTE
DIRECTOR

DR. FERNANDO BETANZO VALLEJOS

DIRECTOR

SERVICIO DE SALUD

METROPOLITANO SUR ORIENTE

DISTRIBUCION:

- Dirección S.S.M.S.O.
- Subdirección Administrativa del S.S.M.S.O
- Subdirección de Gestión Asistencial S.S.M.S.O
- Subdirección de Gestión y Desarrollo de las Personas S.S.M.S.O
- Establecimientos Hospitalarios de la Red Sur Oriente
- Unidad de Control Interno S.S.M.S.O
- Asesoría Jurídica S.S.M.S.O
- Departamento de Auditoría Interna S.S.M.S.O
- Oficina de Partes S.S.M.S.O

SERVICIO SALUD METROP. SUR ORIENTE
MINISTRO DE FE

TRANSCRITA FIELMENTE

MINISTRO DE FE

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

DE LA DIRECCIÓN DEL SERVICIO DE

SALUD METROPOLITANO SUR ORIENTE

AÑO 2018

INDICE

1. OBJETIVOS 3
2. ALCANCE 3
3. DOCUMENTOS DE REFERENCIA 4
4. ROLES Y RESPONSABILIDADES 6
5. MATERIAS TRATADAS 11
6. LINEAMIENTOS ESTRATEGICOS 11
7. MECANISMOS DE DIFUSIÓN Y DISTRIBUCIÓN 20
8. PERIODO DE REVISIÓN DEL DOCUMENTO 21
9. MEDICIÓN DEL CUMPLIMIENTO 21
10. CONTROL DE CAMBIOS 21

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Establecer lineamientos estratégicos transversales para alinear roles, responsabilidades y actividades necesarias para la detección oportuna, tratamiento adecuado y aprendizaje frente a debilidades, eventos o incidentes que comprometan la seguridad de los activos de información, permitiendo así avanzar en conjunto y entregar respuestas homogéneas y efectivas.

En lo concreto, esta Política determina la necesidad de establecer y mantener una estructura ISIRT (Information Security Incident Response Team) o equipos de respuesta ante incidentes de Seguridad de la Información en esta Dirección.

1.2 OBJETIVOS ESPECÍFICOS

- ✓ Generar instancia de coordinación mediante la estructuración de un equipo de respuesta ante incidentes de seguridad de la información. Diferenciar entre debilidades, eventos e incidentes de seguridad de la información.
- ✓ Unificar criterios para detectar, reportar y analizar los incidentes de seguridad
- ✓ Responder y manejar los incidentes de seguridad
- ✓ Mejorar continuamente la gestión de la seguridad en los incidentes de seguridad de la información y avanzar en forma sincronizada en mejorar los niveles de madurez de los procesos más relevantes de esta materia, a nivel institucional.

2. ALCANCE

Esta Política es aplicable a todos los funcionarios (Planta, contrata, reemplazo y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.) que presten servicios para la Dirección del Servicio de Salud Metropolitano Sur Oriente.

Sin perjuicio de lo anterior, se espera que esta política sirva de guía y recomendación para los Establecimientos Hospitalarios de la red Sur Oriente, esto es:

- Complejo Asistencial Dr. Sótero del Río
- Complejo Hospitalario San José de Maipo
- Hospital Clínico La Florida, Dra. Eloísa Díaz Insunza
- Hospital Padre Hurtado
- CRS Hospital Provincia Cordillera

La presente política considera tanto debilidades, eventos e incidentes de seguridad de la información que tengan el potencial de afectar o hayan afectado la confidencialidad, la integridad o la disponibilidad de los activos de información de la institución.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política considera aspectos de los dominios de seguridad de la información y controles de seguridad respectivos, detallados a continuación:

Dominios y Controles de Seguridad relacionadas	
A.05	Dominio: Políticas de Seguridad de la Información
A.05.01.01	Política de Seguridad de la Información
A.16	Dominio: Gestión de incidentes de Seguridad de la Información
A.16.01.01	Responsabilidades y procedimientos
A.16.01.02	Informe de eventos de seguridad de la información
A.16.01.03	Informe de las debilidades de seguridad de la información
A.16.01.04	Evaluación y decisión sobre los eventos de seguridad de la información
A.16.01.05	Respuesta ante incidentes de seguridad de la información
A.16.01.06	Aprendizaje de los incidentes de seguridad de la información
A.16.01.07	Recolección de evidencia

3. DOCUMENTOS DE REFERENCIA

- ✓ CERT/CC-CMU
  - Los lineamientos internacionales del Computer Emergency Response Team/Coordination Center perteneciente a la Universidad Carnegie Mellon.
- ✓ El marco normativo propuesto por el CSIRT del Ministerio del Interior, como entidad coordinadora de los CSIRTs de las instituciones, en este caso "CSIRT Sector Seguridad Pública".
  - https://wwww.csirt.gob.cl/
- ✓ El marco jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior
  - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
  - Leyes relacionadas https://www.csirt.gob.cl/leyes .html

✓ El Marco normativo para las funciones en el Sector Salud, como:

- Ley 19.628 sobre la protección de la vida privada, Ministerio Secretaria General de la Presidencia.
- Ley N° 20.285 Sobre acceso a la información pública, Ministerio Secretaría General de la Presidencia.
- D.F.L Número 29 que fija texto refundido, coordinado y sistematizados de la ley N° 18.834, sobre Estatuto Administrativo.
- Ley N° 19.653 Ministerio o Secretaria General de la Presidencia, sobre probidad administrativa aplicable a los órganos de la Administración del Estado.
- Decreto 41/2012 que aprueba reglamento sobre fichas clínicas

  Regular el contenido, almacenamiento, administración, protección y eliminación de fichas clónicas de manera de resguardar el correcto empleo, disponibilidad y confidencialidad de las mismas.

✓ Normas y estándares nacionales e internacionales relacionados con gestión de incidentes

- NCh-ISO 27001. Of 2013 Tecnología de la Información- Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información.
- NCh- ISO 27002. Of 2013 Tecnología de la información- Códigos de prácticas para la gestión de la Seguridad de la Información.
- ISO/IEC 27035:2011 Information technology- Security techniques- information security incident management.

✓ Documentos del SGSI- Sec y de cada Sistema de Seguridad de la información institucional:

- Resolución Exenta N° 1161, que aprueba Sistema de Seguridad de la Información de las Subsecretarías de Salud Pública y Redes Asistenciales
- Resolución Exenta N° 1474, que aprueba política de gestión de incidentes de seguridad de la información de la Subsecretarias de Salud Pública y Redes Asistenciales.
- Documento con estándar sectorial del modelo de niveles de madurez de procesos del Sistema de Seguridad de la Información en MINSAL
- Resolución Exenta N°4636-2018, Aprueba Sistema de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente.

- Resolución Exenta N°4778-2018, Aprueba Política General de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente

4. ROLES Y RESPONSABILIDADES

- **Autoridades de la Dirección del Servicio de Salud Metropolitano Sur Oriente**
  - ✓ Lo ejercen el director del Servicio
  - ✓ Aprueba la estructura documental del Sistema de Seguridad de la Información la que incluye políticas generales o particulares sobre la materia.

- **Encargado de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente**

  - Actuar como asesor en materias relativas a seguridad de la información para la Dirección del Servicio y la red Sur Oriente.
  - Organizar las actividades del Comité de Seguridad de la Información
  - Coordinar la debida respuesta y priorización de incidentes riesgos vinculados a los activos de la información de los procesos institucionales y sus objetivos de negocio.
  - Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos.
  - Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la Dirección del Servicio y el control de su implementación, velando por la correcta aplicación y cumplimiento, así como mantener coordinación con otras unidades del Servicio para apoyar los objetivos de seguridad de la información.
  - Investigar los eventos de seguridad identificados y/o reportados.
  - Definir las vías de comunicación que se requieran para apoyar en la Resolución del incidente de seguridad de la información.
  - Establecer puntos de enlace con encargados de seguridad de los Establecimientos Hospitalarios de la red Sur Oriente y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
  - Coordinar la debida respuesta y priorización de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio. En el ejercicio de este rol, le corresponderá especialmente:

- Coordinar la habilitación de un CSIRT en el Nivel Central, para dar seguimientos a la debilidades, eventos e incidentes de Seguridad de la Información
- Servir de punto de contacto para las coordinaciones frente a un incidente transversal
- Hacer seguimiento de los incidentes que ocurran en el sector, para velar por la Resolución de los mismos.
- Informar periódicamente al Jefe de Departamento de Informática de esta Dirección, de los incidentes de seguridad relevantes, su estado y que pudieran afectar esta institución.

- **Comité de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente**

  - Supervisar la implementación de la estructura documental del Sistema de Seguridad de la información, aplicable en la Dirección del Servicio de Salud Metropolitano Sur Oriente.
  - Proponer, estrategias o soluciones específicas para implementar o controlar los componentes de la estructura documental del Sistema de Seguridad de la Información.
  - Apoyar en las funciones del Encargado de Seguridad de la Información del Servicio.
  - Definir y Establecer los Roles y Responsabilidades de las personas que forman parte del comité de seguridad de la información.
  - Revisar y Aprobar las Políticas en materia de Seguridad de la Información que sean propuestos por el Comité Técnico de Seguridad de la Información.
  - Revisar y Aprobar los Procedimientos en materia de Seguridad de la Información que sean propuestos por el Comité Técnico de Seguridad de la Información.

  - Conocer los riesgos y su criticidad a los cuales se encuentran expuestos los activos de la información.

  - Definir las Acciones a seguir frente a incidentes de seguridad de la información que afecten la continuidad de los procesos críticos para la institución.

  - Aprobar iniciativas para mejorar la seguridad en los activos de la información, propuestas por el Comité Técnico de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente.

- Verificar el cumplimiento de la difusión relacionados al Sistema de Gestión de seguridad de la información al interior de la institución.

- Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones sobre ello, coordinarse con los Comités de Seguridad de Establecimientos Hospitalarios de la red Sur Oriente, para mantener estrategias comunes de gestión y reportar a la Dirección, respecto a oportunidades de mejora en el SGSI, así como los incidentes relevantes y su gestión. En el ejercicio de este rol y en materia de gestión de incidentes a este comité le corresponde:

  - Supervisar las actividades de gestión de incidentes

  - Analizar los tipos de incidentes, periodicidad, tendencias para generar planes de mitigación, los que serán incluidos dentro de sus objetivos de seguridad de la información.

  - Sensibilizar a la institución sobre la importancia del reporte y gestión de incidentes de seguridad de la información.

  - El Establecer los puntos de coordinación institucionales para la Estructura CSIRT en la red Sur Oriente.

  - Revisar y aprobar reporte de medición anual CSIRT de la institución, a informar al Comité Estrategia Digital de Salud.

- **Comité Técnico de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente**

- Elaborar Políticas de Seguridad de la Información de la Dirección de Servicio de Salud Metropolitano Sur Oriente.

- Elaborar Procedimientos de Seguridad de la Información de la Dirección de Servicio de Salud Metropolitano Sur Oriente.

- Elaborar, implementar y realizar seguimiento al Plan de Comunicación y Consulta del Sistema de Seguridad de la Información de la Dirección de Servicio de Salud Metropolitano Sur Oriente.

- Implementar el Sistema de Seguridad de la Información de la Dirección de Servicio de Salud Metropolitano Sur Oriente.

- Revisar y/ o modificar si corresponde, Matriz de Riesgos Institucional en materia de Seguridad de la Información.

- Elaborar Plan de acción de acción de mitigación de riesgos de Seguridad de la Información.
- Monitorear el avance general de la implementación de las estrategias de tratamiento de riesgos contenidas en el plan de acción.

- **Equipo CSIRT local**

✓ Esta dirección de Salud, establecerá un equipo CSIRT o equipo de respuesta, conformada por profesionales y técnicos con las adecuadas competencias y capacidad de gestionarlos procesos de identificación, respuesta y aprendizaje de los incidentes de seguridad de la información.

✓ Este equipo supervisará que los equipos o áreas resolutoras atiendan el incidente de manera adecuada.

✓ Este equipo deberá contar con apoyo de personal de a lo menos las siguientes áreas:

- Infraestructura física
- Operaciones TIC
- Recursos Humanos
- Departamento de Asesoría Jurídica
- Servicios generales/División administración

El personal designado deberá contar con un respaldo que lo reemplace en caso de ausencia.

✓ Será responsable de mantener los servicios del CSIRT Institucional:

- Coordinación de la respuesta ante incidentes, mediante la activación de los Equipos de respuesta o áreas resolutoras
- Identificación de causa raíz de incidentes
- Generar reportes de gestión de incidentes
- Efectuar seguimiento de las medidas de mitigación requeridas
- Mantener contacto con otros CSIRTs; o grupos de interés por temas de gestión de incidentes.
- Reportar a la brevedad al ESI todo evento relevante a nivel local o red de salud. No pudiendo exceder de 48 horas de su detección.

- **Equipo de respuesta o áreas resolutoras**

- Corresponden a una designación o nomenclatura para designar a las personas que, según sus competencias operacionales, son los más capacitados para atender la resolución de un determinado tipo de incidente/vulnerabilidad.

- No constituyen una estructura diferente a la de una operación normal, sino más bien una asociación para la resolución de incidentes.

- En la medida que madura la estructura, se puede ser más preciso en su definición, en la medida que se formalice la atención de tipos de incidentes particulares.

- **Usuarios Finales**

Se debe entender como usuarios finales a todos quienes tienes la responsabilidad de reportar a la brevedad de cualquier sospechosa de debilidad, evento o incidentes de seguridad de la información, a su jefatura inmediata y al PUC (punto único de contacto) definido en su institución, para estos casos.

Debe considerar:

- A todos los funcionarios (planta, contrata, reemplazo y suplencia)
- Personal a honorarios
- Terceros (proveedores, compra de servicios, tratamiento por encargo, servicios externalizados, etc.)

Los requerimientos de seguridad y de reporte de incidentes/vulnerabilidades hacia terceros y personal a honorarios, deben estar considerados en los TDR: Términos de referencia del acuerdo base del servicio contratado.

5.MATERIAS TRATADAS

Las materias tratadas en el documento están relacionadas con la seguridad de la información en la gestión de incidentes de seguridad de la información, abordadas en las siguientes temáticas

6.LINEAMIENTOS ESTRATÉGICOS

6.1Requisitos para gestión de incidentes de Seguridad de la Información

- ✓ Se integran los requisitos y lineamientos respecto a la gestión de incidentes, ya señalados en la Política General de Seguridad de la Información de la Dirección de este Servicio.
- ✓ Para lograr mantener un proceso de gestión de mejorar continua sobre la atención de debilidades, eventos o incidentes de seguridad de la información, se usará el modelo DEMING O PDCA (Plan, DO; Check; act), materializando en:

- Lineamientos de Planificación
- Lineamientos de implementación
- Lineamientos de revisión y mejora

6.2 Lineamientos de planificación

6.2.1 Definiciones asociadas a incidentes de seguridad de la información

Las siguientes definiciones son específicas para el ámbito de gestión de incidentes de seguridad de la información:

Vulnerabilidad o debilidad de la seguridad de la información:
Debilidad en el sentido de incompletitud, vulnerabilidad o carencia en la protección de la confidencialidad, integridad o disponibilidad de un activo o un grupo de activos que puede ser explotada por una o más amenazas, lo que podría poner en riesgo la seguridad de la información. Potencial evento o incidente de seguridad.

Evento de Seguridad de la Información:

Presencia identificada de una condición de un proceso, sistema, servicio de red, que indica una posible violación de la política de seguridad de la información establecida o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. Potencial incidente que no tuvo impacto porque actuaron los controles existentes.

- ✓ **Incidente de seguridad de la información:**

  Cualquier evento o situación que comprometa de manera importante la disponibilidad, integridad y/o confidencialidad de la información:

  Confidencialidad: acceso no autorizado a la información
  Integridad: modificación no autorizada, destrucción o pérdida de información
  Disponibilidad: Inaccesibilidad a la información

  En general, es una violación de una política, estándar o procedimiento de seguridad que no permita el correcto funcionamiento de los servicios.

  Se asocia también con un o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de amenazar comprometer las operaciones del negocio y la seguridad de la información, por lo que se ha efectuada una "declaración" como incidente.

- ✓ **CSIRT**: por sus siglas en ingles Information Security Incidente Response Team, Equipo de respuesta ante incidentes de Seguridad de la información.

- ✓ **PUC:** Punto único de contacto, que debe estar definido tanto a nivel local de cada institución como un PUC CSRIT- Salud, tiene el objetivo de concentrar todo reporte de debilidad, evento o sospecha de incidente.

- ✓ **Clasificación y priorización inicial (rol TRIAGE):** Función dentro del PUC que analiza los requerimientos y en primera instancia puede catalogarlo como la gestión de una debilidad, de un evento o decláralo como incidente de seguridad de la información. En la nomenclatura del CERT/CC, se acostumbra llamar TRIAGE.

6.2.2 Estructura Jerárquica del CSIRT

Esta estructura se compone de los siguientes niveles, los que deben ser analizados, al menos anualmente, para detectar necesidades de mejora:

6.2.2.1 CSIRT en la Dirección de Servicio

Nivel Institucional Táctico:

Equipo CSIRT

- ✓ Encargado de analizar periódicamente las debilidades, eventos e incidentes catalogados en su institución, con el fin de identificar acciones adicionales a las ya tomadas, además de identificar acciones adicionales a las ya tomadas, además de identificar causa raíz de reportes reiterativos.

- ✓ Definen y mantienen tablas de relación entre tipos de incidentes con equipos resolutores.

Encargados de Seguridad de la Información DSS

- ✓ Coordina las actividades del CSIRT respectivas

Nivel Institucional Operacional

- ✓ Equipos/áreas resolutoras por tipo de incidente

  - Encargados de resolver operativamente el incidente

- ✓ Usuario Final

  - Con su rol de informar al PUC cualquier sospechosa de debilidad o incidente

6.2.2.2 CSIRT en los Establecimientos Hospitalarios

Nivel Sectorial (Dirección del Servicio de Salud Metropolitano Sur Oriente)

- Comité de Seguridad de la información sectorial (CSIS)
- Encargado de Seguridad de la Información Sectorial (ESI- Sectorial)

Nivel Institucional Táctico:

Equipo CSIRT Local

- ✓ Encargado de analizar periódicamente las debilidades, eventos e incidentes catalogados en su institución, con el fin de identificar acciones adicionales a las ya tomadas, además de identificar acciones adicionales a las ya tomadas, además de identificar causa raíz de reportes reiterativos.

- ✓ Definen y mantienen tablas de relación entre tipos de incidentes con equipos resolutores.

Encargados de Seguridad de la Información (ESI) de los Establecimientos Hospitalarios

- ✓ Coordina las actividades del CSIRT respectivas

Nivel Institucional Operacional:

- ✓ Equipos/áreas resolutoras por tipo de incidente

  - Encargados de resolver operativamente el incidente

- ✓ Usuario Final

  - Con su rol de informar al PUC cualquier sospechosa de debilidad o incidente

6.2.3 Establecer un punto único de contacto institucional (PUC)

PUC que se debe definir en esta Dirección de Servicio y donde la definición PUC- NC actuará como integrador para eventos transversales y de acceso a soporte especializado central. Normalmente asignado a la Mesa de Ayuda o de Servicio; podría hasta ser un servicio externalizado.

Se deben capacitar en acciones mínimas inmediatas y en el rol TRIAGE de análisis inicial, declaración de incidente, si corresponde y derivación al equipo resolutor relacionado.

6.2.4 Identificar Equipos/Áreas Resolutoras por tipo de Incidentes

Se deben asociar equipos particulares o áreas generales, como resolutores para abordar incidentes según su naturaleza, lo que debe quedar documentado para servir de guía de asignación de los incidentes una vez declarados.

Los eventos/incidentes que no puedan ser atendidos a nivel local, se deben poder escalar a nivel central, para acceder a equipos resolutores más especializados.

6.2.5 Establecer un formato común de reporte y seguimientos de incidentes

Se debe establecer un formulario común de base para el reporte y seguimiento de incidentes, que contenga los campos mínimos que debe contener cualquier registro, reporte o sistema de gestión de incidentes, los campos mínimos son:

Entre los campos mínimos esperables, se consideran:

I. Generales:

- Identificación única del incidente/ Vulnerabilidad
- Estado del incidente /Vulnerabilidad
- Descripción resumida del incidente

II. Antecedentes del Origen

- Fecha reporte
- Hora reporte
- Identificación de quien reporta
- Activos/Sistemas afectados

III. Tipificación

- Debilidad de Seguridad
- Evento de Seguridad
- Incidente de Seguridad de la Información

IV. Tipo de incidente

- Informático
- No informático

V. Nivel de Criticidad

- Alta
- Media
- Baja

VI. Respuesta inicial

- Contacto responsable de la acción inmediata
- Descripción de la acción inmediata

VII. Asignación

- Equipo/área resolutora asignada
- Contacto responsable de la resolución del incidente

VIII. Seguimiento

- Se activa continuidad del negocio (S/N)
- Registros y evidencia

IX. Post incidente

- Análisis de causas
- Acción correctiva/Preventiva
- Costos asociados

X. Respuesta y cierre

- Detalle de la respuesta final
- Fecha cierre

6.2.6 Unificar estados del ciclo de vida de un incidente/ vulnerabilidad

Se debe homogenizar a nivel sector un conjunto mínimo y consistente de estados por los que puede pasar un incidente, hasta cerrarse,
Este conjunto mínimo, debe al menos contener:

- **Inicial:** No se ha analizado lo suficiente como declararlo un incidente o vulnerabilidad.
- **Declarado** (Como incidente o vulnerabilidad): Ha sido declarado incidente, pero aún no se asigna a un resolutor particular.
- **Asignado:** Está asignado y en revisión
- **Resuelto:** Ya se conoce la manera de resolver el incidente
- **Mitigado:** Ya se han implementado las medidas de mitigación descubiertas
- **Cerrado:** Se da por solucionado el incidente a conformidad de los afectados

6.2.7 Formalización de respuestas ante incidentes de seguridad de la información

Para la formalización procedimental de la respuesta ante incidentes, se debe primero contar con un procedimiento general (genérico) de respuesta ante incidentes, luego necesariamente se deberán construir instructivos o procedimientos para incidentes específicos. En las siguientes etapas se debe llegar a contar con todos los procedimientos, instructivos y formularios más relevantes.

6.2.8 Planificar la sensibilización y capacitación

El Encargado de Seguridad de la información de la Dirección de este Servicio de Salud, será responsable de integrar en su programa de sensibilización y capacitación los temas de reporte y gestión de incidentes de seguridad de la información. Se debe considerar las competencias que requiere CSIRT, los equipos resolutores y la información de sensibilización para los usuarios finales.

6.2.9 Gestionar niveles de madurez del modelo sectorial para dichos procesos

Se propone analizar los controles de seguridad en la gestión de incidentes bajo el modelo de Niveles de Madurez de Procesos propuestos a nivel sectorial y detallado como proceso de gestión de la madurez de procesos del Sistema de Seguridad de la Información, en la Política General de Seguridad de la información para el sector salud.

6.3 Lineamientos de implementación

6.3.1 Habilitar el PUC y Priorización de atención

Habilitar un punto único de contacto y su estructura para el análisis, priorización, declaración y asignación de incidentes de seguridad.

Estas funciones requieren que la institución decida, respecto de:

- Acceso PUC mediante número de contacto telefónico, e-mail, página web
- Difundir el mecanismo de reporte al PUC para todos los colaborares
- Establecer tablas de tipificación de incidentes a menos, Informáticos (I); No informáticos (NI) y sus ejemplos o sub-tipificación.
- Establecer criterios para homogenizar la priorización de incidentes
- Punto de comunicación masiva de estos de incidentes

6.3.2 Detección y reporte de eventos de seguridad de la información

- Clarificar a los usuarios finales, la manera de mejorar la detección de eventos de seguridad y su reporte al PUC local.

- Señalar formato base para el reporte de eventos

6.3.3 Análisis, declaración y asignación

- Evaluación y decisión inicial del punto de contacto (PUC): permite catalogar el requerimiento como reporte de una debilidad, como declaración de un incidente.
- Evaluación y confirmación del incidente por el equipo de respuesta de incidentes
- Escalamiento de incidentes a Nivel Central de ser necesario.

6.3.4 Respuesta a incidentes de seguridad

Se deben documentar los servicios de respuesta inicial, respuesta técnica, mitigación y análisis posteriores, como forense, de ser necesarios.

- Respuesta inicial, inmediata o de primera línea
- Respuestas a incidentes de seguridad de la información, incluyendo análisis forense.
- Recuperación o mitigación del incidente de seguridad de la información,
- Durante el proceso de respuesta/mitigación también se puede escalar al nivel central

- Se deben mantenerlos registros o LOGs de las acciones realizadas. De preferencia en alguna plataforma distinta a la que lo generó.

6.3.5 Implementar actividades asociadas a las brechas del nivel de madurez

Para cada requerimiento de control operacional en que se haya identificado una brecha contra el nivel de línea base deseado, se debe priorizar su mitigación, avanzando al siguiente nivel de madurez del proceso, tal como señala la política general de seguridad de la información sectorial.

6.4 Lineamientos de revisión y mejora

6.4.1 Revisión y reporte de casos relevantes

Cada situación considerada relevante, así como también un informe de debilidades e incidentes en el año, debe ser analizado por el CSIRT local y presentado a su CSI. A petición de éste, el ESI lo escala a nivel central.

6.4.2 Mecanismo de medición

- Debe existir una definición de indicadores de gestión y mejora en la seguridad de los sistemas de información.

- El indicador base de medición a nivel sectorial será el nivel de madurez alcanzado en cada proceso de control operacional.

- Se debe activar el mecanismo de medición establecido por el Comité de Seguridad Sectorial y operar según lo señalado en las responsabilidades respectivas. El ESI de los establecimientos lo escala al Encargado de Seguridad de la información a nivel central (DSS).

6.4.3 Actividades post cierre incidente

El CSIRT local debe considerar la necesidad de actividades posteriores al cierre del incidente, entre ellas, por ejemplo:

- Análisis forense adicional, para identificar antecedentes y factores menos obvios involucrados
- Identificación de lecciones aprendidas
- Identificación de causa raíz en particular en casos de aparición de debilidades, eventos o incidentes de seguridad de la información recurrentes.
- Contabilización de recursos y costos involucrados en incidentes
- Identificación de procesos administrativos para atender procesos disciplinarios

6.4.3 Actividades post cierre incidente

- Identificación de mejoras en la seguridad de la información
- Identificación de mejora al proceso de evaluación de riesgos de seguridad de la información
- Identificación de necesidades de ajuste al proceso de gestión, a la gobernabilidad o al cuerpo normativo de tratamiento de incidente existente
- Avanzar al siguiente nivel de madurez del modelo sectorial propuesto al respecto

6.5 Estructura documental para los incidentes de Seguridad de la Información

- Presente política de Gestión incidentes de Seguridad de la Información
- Formulario base de reporte de incidentes
- Procedimiento de respuesta ante incidentes de Seguridad de la Información
- Tipificación de documentos del Marco Normativo en Seguridad de la Información

7. MECANISMOS DE DIFUSIÓN Y DISTRIBUCIÓN

Esta Política especial, se encontrará disponible en página web de la Dirección del Servicio de Salud Metropolitano Sur Oriente en un banner, cuyo nombre será: Sistema de Gestión de Seguridad de la Información, en la Intranet del SSMSO en las mismas condiciones de página de web de esta institución.

El Encargado de Seguridad de la Información de la Dirección del Servicio, velará por maximizar la cobertura de su difusión, a través de:

- Publicación en la intranet del DSS y pagina web de la Dirección del Servicio
- Correo informativo
- Mural de la Dirección de Servicio
- Entrega de documentos directamente a cada funcionario de la Dirección del Servicio.

Los Establecimientos Hospitalarios de la red Sur Oriente, deberán establecer canales accesibles para la comunicación interna permanente de ésta y todas sus políticas, procedimientos y otros documentos generados en el marco del Sistema de Seguridad de la Información de cada Establecimiento Hospitalario.

8. PERIODO DE REVISIÓN DEL DOCUMENTO

La revisión del contenido de esta política se efectuará al menos una vez al año, o atendiendo necesidades de cambios para garantizar su actualización, idoneidad, adecuación y efectividad en su ámbito de control.

9. MEDICION DEL CUMPLIMIENTO

Encargado de Seguridad de la Información, trimestralmente realizará un informe de cumplimiento de esta política, mediante autoevaluación y reporte (medir y reportar), el cual será entregado a Comité de Seguridad de la información para su revisión y aprobación.

Encargado de Seguridad de la información de esta Dirección solicitará lo anterior a Encargados de Seguridad de la Información de la red Sur Oriente, con el fin de obtener indicadores a nivel sector.

10. CONTROL DE CAMBIOS

Elaborador por:	Revisado por:	Aprobado por:
Cinthia León Fuentealba: Encargada de Control Interno de la Dirección del Servicio de Salud Metropolitano Sur Oriente	Comité técnico de Seguridad de la Dirección del Servicio de Salud Metropolitano Sur Oriente Comité de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente	Fernando Betanzo Vallejos; director de la Dirección del Servicio de Salud Metropolitano Sur Oriente