Servicio de Salud Metropolitano Sur Oriente
Complejo Hospitalario San José de Maipo
Ministerio de Salud

COMPLEJO HOSPITALARIO SAN JOSE DE MAIPO

ACREDITADO DE SALUD

APRUEBA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL COMPLEJO HOSPITALARIO SAN JOSÉ DE MAIPO. -

RESOLUCION EXENTA Nº 000686 /

SAN JOSE DE MAIPO, 08 MAY 2019

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 lo previsto en la RESOLUCION EXENTA RA N° 346 de fecha 08 de marzo de 2019 del SSMSO; dicto la siguiente:

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 Complejo Hospitalario San José de Maipo, 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 el Complejo Hospitalario San José de Maipo 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 el Complejo Hospitalario San José de Maipo, adopte las medidas que estime pertinente para resguardar la seguridad de la información.

6. Que, el Complejo Hospitalario San José de Maipo 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 Red Sur Oriente.

7. En este contexto, y por todas las consideraciones expuestas, el Complejo Hospitalario San José de Maipo, define, actualiza y formaliza la Política General de la Seguridad de la Información en esta institución, dictando lo siguiente:

Servicio de Salud Metropolitano Sur Oriente
Complejo Hospitalario San José de Maipo
Ministerio de Salud

COMPLEJO HOSPITALARIO SAN JOSE DE MAIPO

ACREDITADO
DE SALUD

RESOLUCIÓN

ARTICULO 1- APRUEBASE la Política General de Seguridad de la Información para el Complejo Hospitalario San José de Maipo, que se encuentra descrita en el documento adjunto, como anexo, y que forma parte integrante de la presente Resolución.

ARTÍCULO 2. Déjese constancia que el tenor del documento aprobado en el artículo anterior es denominado "Política de Seguridad de la Información del Complejo Hospitalario San José de Maipo" que se incorpora y que consta de 15 páginas -

ANOTESE, COMUNIQUESE Y ARCHIVESE

HOSPITAL SANATORIO SAN JOSE DE MAIPO
DIRECCION

SR. JAIME CARVAJAL YAÑEZ
DIRECTOR (S) COMPLEJO HOSPITALARIO
SAN JOSE DE MAIPO

COMPLEJO HOSPITALARIO SAN JOSÉ DE MAIPO
MINISTRO DE FE

Transcrito Fielmente
MINISTRO DE FE

DISTRIBUCIÓN:
- Dirección CHSJM
- Subdirección Administrativa
- Unidad de Control de Gestión
- Auditoria Interna
- Subdirección Medica
- Unidad de Calidad y Seguridad del Paciente
- Unidad de Informatica
- Oficina de Partes

SR. JCY/RUK/mam. -

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DEL COMPLEJO HOSPITALARIO

SAN JOSE DE MAIPO

AÑO 2019

INDICE

1. OBJETIVO

Esta Política General de Gestión de Seguridad de la Información establece los lineamientos de la estructura documental del Sistema de Seguridad de la Información aprobado mediante Resolución Exenta N° 4632 de fecha 30 de noviembre de 2018, de la Dirección del Servicio de Salud Metropolitano Sur Oriente. Esto permite gestionar la mejora continua en la protección de la Seguridad de la Información de esta institución.

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.

Esta Política abarca los siguientes controles definidos en la norma NCh- ISO 27001-2013:

- ✓ Políticas para la Seguridad de la Información
- ✓ Revisión de las Políticas de Seguridad de la Información
- ✓ Propiedad de los Activos
- ✓ Proveedores

La presente política se aplica sobre todo tipo de información, considerando todo medio de soporte y presentación, como son la voz y medios digitales, ya sean magnético, óptico, electrónico o fotográfico.

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 de la Norma NCh-ISO 27.001:2013 Análisis de requisitos e implementación relacionados	
A.05	Dominio: Políticas de Seguridad de la Información
A.05.01.01	Política de Seguridad de la Información
A.05.01.02	Revisiones de las Políticas de Seguridad de la Información

DOCUMENTOS DE REFERENCIA

- 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: https://www.csirt.gob.cl/decretos.html
  - ✓ Leyes relacionadas: https://www.csirt.gob.cl/leyes.html
- Marco normativa para las funciones en el Sector Salud, como:
  - ✓ Ley N° 19.628 sobre la protección de la vida privada, Ministerio Secretaría General de la Presidencia.
  - ✓ Ley N° 20.285 sobre acceso a la información pública, Ministerio Secretaría General de la Presidencia.
  - ✓ D.F.L N° 29 que fija texto refundido, coordinado y sistematizados de la ley N° 18.834, sobre Estatuto Administrativo.
  - ✓ Ley N°19.653 Ministerio o Secretaría 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 clínicas de manera de resguardar el correcto empleo, disponibilidad y confidencialidad de las mismas.

Otros documentos:

- ✓ Resolución Exenta N° 1161, que aprueba Sistema de Seguridad de la Información de las Subsecretarías de Salud Pública y Redes Asistenciales.
- ✓ Resolución Exenta N° 1481 del 24.11.2017, que aprueba Política General de Seguridad de la Información para las Subsecretarías de Salud Pública y Redes Asistenciales.
- ✓ Modelo de madurez de procesos de seguridad de la información propuestos a nivel Sector Salud Pública.
- ✓ Documentos normativos de Seguridad de la Información del Ministerio de Salud: http://web.minsal.cl/seguridaddelainformación/

Normas del Sistema de Gestión de Seguridad de la Información:

- ✓ NCh-ISO 27001:2013 Análisis de requisitos e implementación.
- ✓ NCh-ISO 27002:2013 Código de prácticas para los controles de seguridad de la información.

3. DEFINICIONES

- ✓ **Activo**: Cualquier elemento, objeto u otro, que tenga valor para la institución.
- ✓ **Información:** Es la interpretación que se da a los datos. Toda forma que contenga datos relacionados con la organización.
- ✓ **Activo de Información**: Todos los elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de la información de valor para la institución, independiente de su naturaleza, medio o forma de presentación.
- ✓ **Autenticación**: Asegurar la confirmación de la identidad de un usuario, es decir, garantizar que cada una de las partes es realmente quien dice ser.
- ✓ **Buen Uso**: se entiende al uso adecuado de lo estipulado en las políticas de seguridad del SSMSO, quien se reserva el derecho de tomar medidas disciplinarias para sancionar, en caso de existir evidencias de no cumplimiento de estas disposiciones.
- ✓ **Seguridad de la Información**: Es la preservación de la confidencialidad, la integridad y la disponibilidad de la información de la Dirección del Servicio de Salud Metropolitano Sur Oriente
- ✓ **Sistema de gestión de la seguridad de la información (SGSI)**: parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, monitorear, revisar y mejorar la seguridad de la información.
- ✓ **Evento de Seguridad de la Información**: ocurrencia identificada de un estado de un proceso, sistema y/o servicio que indica una posible violación a la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.
- ✓ **Incidente de Seguridad de la Información**: un evento o serie de eventos de seguridad de la información no deseada o inesperada que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- ✓ **Información Confidencial**: Toda aquella que tenga el potencial de afectar la continuidad operacional de la institución, el prestigio, la imagen del SSMSO.

- ✓ **Información Interna:** Es toda aquella información que al ser divulgada, adulterada o destruida, sin generar un daño grave al SSMSO, produzca un perjuicio operacional que involucre pérdida de tiempo y recursos en su recuperación/reposición.

- ✓ **Información Pública**: Información que por su naturaleza no presenta riesgos para el SSMSO y que puede ser divulgada al público general. •

- ✓ **No Repudio**: Dar garantía de que el usuario no pueda negar la operación realizada.

- ✓ **Propietario de la Información**: usuario responsable de la información y el proceso que este utilice (manuales, electrónicos). • Recuperación: Restauración de las capacidades de proceso de sistemas a las condiciones de operación normales.

- ✓ **Terceros**: Personal externo a la institución que pertenece a una de las siguientes categorías:

  - **Proveedor**: Empresas prestadoras de servicios, empresas contratistas, subcontratistas y cualquiera, que por cuenta propia o de terceros, desarrolle trabajos para o por cuenta del CHSJM.

  - **Visitante**: Toda persona externa de la institución, que, sin ser proveedor o cliente, se le autoriza de manera restringida el acceso a las instalaciones/recursos del CHSJM. En esta categoría están los familiares, amigos de los empleados, clientes potenciales, auditores y vendedores.

  - **Usuario**: Toda persona natural a la cual se le concede autorización para acceder a lugares físicos, información y sistemas del CHSJM. Incluyendo al propio personal (interno o externo) de la organización, y a terceros. Adicionalmente, serán aplicables las definiciones que se establezcan en la normativa vigente asociada a la Seguridad de la Información.

4. ROLES Y RESPONSABILIDADES

- **Encargado de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.**

  - ✓ Actuar como asesor en materias relativas a seguridad de la información para la Dirección del Complejo Hospitalario San José de Maipo.

  - ✓ 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

- **Comité de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.**

  - Supervisar la implementación de la estructura documental del Sistema de Seguridad de la información, aplicable en el Complejo Hospitalario San Jose de Maipo.

  - 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 del Complejo Hospitalario San José de Maipo.

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

- **Comité Técnico de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.**

✓ Elaborar Políticas de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.

✓ Elaborar Procedimientos de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.

✓ Elaborar, implementar y realizar seguimiento al Plan de Comunicación y Consulta del Sistema de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.

✓ Implementar el Sistema de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.

✓ 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.

- **Usuarios Finales**

Se debe entender como usuarios finales a todos quienes tienes la responsabilidad de acatar las políticas y normativas definidas, independiente que además tengan otro rol nominado en este ámbito. Debe considerar:

- Todos los funcionarios (planta, contrata, reemplazos y suplencia)
- Personal a Honorarios
- Terceros (proveedores, compra de servicios, servicios externalizados, etc.)

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

5. DE LA POLÍTICA

La Dirección del Complejo Hospitalario San Jose de Maipo se compromete a gestionar la seguridad de la Información como un proceso continuo en el tiempo, que se debe cumplir en el marco de la normativa gubernamental existente, por medio de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que el Servicio determine. Para estos efectos, esta Dirección del Complejo, se basará 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 adecuados de integridad, confidencialidad y disponibilidad, de todos sus activos de información relevantes para la institución, como un principio clave en la gestión de sus procesos.

6.1 LINEAMIENTOS ESTRATÉGICOS

6.1.1 Decálogo de principios de Seguridad de la Información

- ✓ Promover la información como un activo vital de quehacer de la Dirección del Complejo Hospitalario San Jose de Maipo.
- ✓ Proteger la privacidad y confidencialidad de toda información sensible o de carácter personal, independiente de su formato, medio de soporte y almacenamiento.

- ✓ Preservar la integridad de los datos, ya que de su exactitud, actualización y veracidad pueden llegar a depender de una vida.

- ✓ Asegurar que la información crítica estará disponible a tiempo y forma sólo para quienes estén debidamente autorizados para tener acceso a ella.

- ✓ Establecer un modelo de gestión de riesgos para la seguridad de la Información; que permita determinar el tipo y naturaleza de controles necesarios para la mitigación de los riesgos identificados como relevantes.

- ✓ Cumplir con el marco normativo establecido para la seguridad de la información del Sector Salud e institucional, mediante la gestión de los controles definidos.

- ✓ Mantener un adecuado respaldo y resguardo de la información gestionada en el Complejo Hospitalario San Jose de Maipo, que permitan prevenir eventuales pérdidas o daño de ella.

- ✓ Habilitar equipos y Sistemas de identificación, análisis, notificación, respuesta resguardo de registros y aprendizaje frente a debilidades e incidentes de seguridad de la información, permitiendo su mitigación y evitando su recurrencia.

- ✓ Desarrollar programas de formación para todo el Personal de la Dirección del Servicio de Salud Metropolitano Sur Oriente.

6.1.2 Identificación de requisitos para la Seguridad de la Información

La Dirección del Complejo Hospitalario San Jose de Maipo deberá periódicamente identificar y analizar las fuentes que generan requisitos de seguridad de la información, en donde se destaca:

- ✓ Un modelo y una metodología formal de gestión de riesgos, consistente con los cambios de la Dirección de este complejo asistencia y de los lineamientos del Sector Salud.

- ✓ Los requisitos legales, normativos y contractuales que aplica al Sector de Salud, sobre todo los que generan nuevos requerimientos de protección de confidencialidad, integridad, disponibilidad, trazabilidad y gestión en general de la protección de información sensible.

- ✓ Los eventos adversos propios o provenientes de amenazas externas que hayan ocurrido recientemente, dejando en evidencia debilidades en sus actuales sistemas de protección o modelos de control en seguridad de la información.

- ✓ Las amenazas del ciberespacio, que deben ser monitoreadas y analizadas para determinar su potencial riesgo.

- ✓ Los propios lineamientos de la Dirección del Complejo Hospitalario San Jose de Maipo y procesos de innovación, por su relación con apertura de nuevos frentes o factores de riesgo.

6.1.3 Lineamientos estratégicos de Seguridad de la Información para la Dirección del Complejo Hospitalario San Jose de Maipo:

Los siguientes son lineamientos estratégicos de Seguridad de la Información, obligatorios para el complejo Hospitalario son:

- ✓ La información, en todas sus formas y presentaciones, es un activo vital para todo el Sector Salud, también lo son los activos necesarios para sus procesos, como tecnologías, instalaciones físicas y personas involucradas.

- ✓ La Seguridad de la Información es un atributo necesario en los servicios ofrecidos, entendiendo que la protección de la disponibilidad, integridad y confidencialidad de dicha información es una condición básica e indispensable del Sector Salud.

- ✓ Para brindar gobernabilidad se define una estructura organizacional compuesta a nivel estratégico por:

A nivel Táctico: Encargado de Seguridad de la Información del Complejo Hospitalario, es responsable de coordinar las implementaciones asociadas a la seguridad de la información y a nivel operacional por los usuarios finales responsables de cumplir el marco normativo.

- ✓ Todo colaborador es responsable de la información que manipula; así como del correcto uso de los recursos tecnológicos que le hayan sido asignados para apoyar tareas relacionadas con la Seguridad de la Información y con sus obligaciones laborales.

- ✓ De esta política general y de una evaluación permanente de riesgos en la seguridad de la información se desprenden un conjunto de políticas, procedimientos, estándares, instructivos y otros elementos que conforman el marco normativo, así como otros tipos de controles necesarios para la Gestión de Seguridad de la Información.

- ✓ Para mejorar la cultura organizacional, se considera primordial la difusión, capacitación y concientización de estos lineamientos y todo el marco normativo de Seguridad de la Información para los trabajadores y terceros que brinden servicio en la institución.

- ✓ En todo proyecto o actividad se debe maximizar el esfuerzo en cumplir tempranamente con el marco normativo de Seguridad de la Información; así como todo regulación y legislación vigente aplicable. Del mismo modo permitir una gestión de mejora continua, debiese considerarse un modelo que integre etapas de planificación, implementación, monitoreo y mejora, según corresponda.

- ✓ Todos los usuarios que tomen conocimiento de una amenaza interna o externa, deliberada o accidental, sea una actividad o situación que afecte actual o potencialmente la seguridad de los activos de información, deben informarlo de inmediato a su instancia organizacional superior.

- ✓ Ésta política debe ser conocida y respetada, al igual que las restantes normas de Seguridad de la Información, como parte de los deberes de cada funcionario, personal honorarios o terceros. Su no cumplimiento será considerado una falta grave contra la protección de los intereses y los activos de la institución. El incumplimiento de las obligaciones emanadas de esta Política, de las políticas específicas, procedimientos u otros documentos que se deriven de éstos, serán sancionados en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del Complejo Hospitalario. Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, se procederá al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

6.1.4 Lineamientos estratégicos de Gestión de mejora continúa

Se debe estructurar y mantener un modelo de Gestión de mejora continua para el Sistema de Seguridad de la Información; que permita desarrollar cada uno de los procesos necesarios para mantener en el tiempo los controles de Seguridad, con el objetivo de avanzar en los Niveles de madurez de procesos propuestos a nivel del sector salud.

Este lineamiento sectorial, se orienta al cómo mantener la gestión en el tiempo y para ello, se recomienda, el uso de Modelo Deming, conocido como PDCA, por sus siglas de Plan Do, Check, act. Puede ser otro modelo equivalente, que propicie una mejora continua.

6.1.5 Lineamientos estratégicos de Modelo de Gestión de Riesgo

Se debe estructurar y mantener, a su vez, un modelo de Gestión de mejora continua para los riesgos o potenciales problemas en Seguridad de la Información; que permita analizar las situaciones que ponen en peligro el cumplimiento institucional y sectorial de protección de la confidencialidad, integridad y disponibilidad de la información, identificando el tipo y naturaleza, además de priorizando y asignando los controles de mitigación necesarios para los riesgos determinados como relevantes para la institución.

Este lineamiento sectorial, se oriente al por qué mantener una gestión sobre las potenciales amenazas, vulnerabilidades e impactos a la seguridad de la información, de modo que permita justificar en el tiempo los controles aplicables a su mitigación.

6.1.6 Estructura documental en gestión de Seguridad de la Información

La estructura documental se encuentra definida en el Sistema de Seguridad de la Información y se encuentra conformado por una Política de Seguridad de la Información, que se aprueba por este acto. Políticas específicas de seguridad de la información, procedimientos de operación, instructivos y registros.

Tales documentos se encuentran definidos en la Resolución que aprueba dicho sistema entendiéndose por:

- ✓ **Política de Seguridad:** intenciones globales y orientación de la organización, relativas a la seguridad de la información, tal como se expresan formalmente por la dirección.

- ✓ **Política General de la Seguridad de la Información:** política que establece el enfoque de la organización para administrar sus objetivos de Seguridad de la Información.

- ✓ **Políticas específicas de Seguridad de la Información:** políticas 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.

- ✓ **Procedimientos:** documento operativo que establece la forma específica para llevar la planificación, operación y control de las actividades o procesos de seguridad de la información.

- ✓ **Instructivos:** documentos que describen como (instrucciones, formularios, checklist) se realizan las tareas y las actividades específicas relacionadas con la Seguridad de la Información.

- ✓ **Registros:** Evidencia objetiva del cumplimiento de los requisitos SGSI; están asociados a documentos de los otros cinco niveles como output que demuestra que se ha cumplido con lo indicado en los mismos.

6.1.7 Lineamientos estratégicos para la gestión de la Madurez de los procesos del Sistema de Seguridad de la Información

Para homogenizar una mirada de avance y desarrollo de los principales procesos necesarios del Sistema de Seguridad de la Información de esta Dirección, se definirá una base de medición estandarizada para los niveles de madurez de dichos procesos, la que se fundamenta en los niveles de madurez de marcos de referencia internacionales como CMM, CobiT, ISO/IEC 15504. Esto permitirá contrastar la realidad de la institución con cierto nivel deseable como línea base para dicha temática, lo que permite extraer brechas o GAPs y sobre ellas facilitar la planificación de controles de mitigación. Asimismo, se propone analizar los controles de Seguridad de la información bajo dicho modelo de niveles de Madurez de Procesos.

A lo menos una vez al año se debe contrastar la aplicación de cada lineamiento como un proceso de control de seguridad de la información, evaluando su nivel de madurez, por auditoría interna del Complejo Hospitalario o por una parte no involucrada directamente en dicho control.

Se debe priorizar los esfuerzos para alcanzar una línea base de nivel de madurez que será al menos en los procesos de control que se debe priorizar. Por ejemplo, alcanzar un nivel de madurez 3 o formalizado, esto consideraría, entre otros, contar con una política y un procedimiento y/o instructivo, que permita formalizar el quehacer en dicho tema (ver estándar propuesto del Modelo de niveles de madurez de procesos MINSAL).

El GAP o brecha entre la situación actual y el nivel de línea de base, determinarán las acciones de mitigación necesarias, que se obtienen de los requerimientos solicitados en el nivel inmediatamente superior del modelo de madurez. Se debe mantener un Sistema de mejora continua en cada uno de tales procesos de control, utilizando para ello el modelo Deming señalado.

Por lo anterior, para su implementación se requiere que para cada control 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, mediante la implementación de las condiciones solicitadas. Para los controles en curso se debe mantener la gestión y procurar alcanzar niveles superiores de madurez del proceso. La mejora continua se logra precisamente avanzando al siguiente nivel de madurez propuesto del modelo.

El modelo propuesto considera niveles de madurez del proceso, evaluados de 5 a 0 como:

5- Resiliente: El proceso se adecúa y reacciona a los cambios del entorno.
4- Gestionado: Se tiende a la mejora continua de la forma de hacer las cosas.
3- Formalizado: Se documentan y formalizaran las acciones a seguir.
2-Repetible: Existen acuerdos prácticos de repetición de la forma de hacer las cosas.
1-Básico: Se realiza el proceso caso a caso en forma independiente por cada individuo.
0-Inexistente: Carencia completa de cualquier proceso reconocible.

Este modelo propuesto a nivel Sectorial por el Ministerio de Salud, debe ser adecuado y formalizado como estándar propio de la Dirección de este Servicio de Salud, para facilitar la evolución de sus procesos de gestión.

Para mayor detalle, revisar los siguientes documentos:

- Documento sectorial de modelo de niveles de madurez de procesos en el ámbito de Gestión de Seguridad de la Información Sector Salud, disponible en sitio de este Ministerio.

- Documento de modelo de madurez y avances respectivos de la Dirección del Servicio de Salud.

7. Mecanismos de difusión y distribución

Esta Política General, se encontrará vigente página web del Complejo Hospitalario en un banner, cuyo nombre será: Sistema de Gestión de Seguridad de la Información

El Encargado de Seguridad de la Información del Complejo Hospitalario, velará por maximizar la cobertura de su difusión, a lo menos a través de:

- Publicación en la página web del Complejo Hospitalario
- Correo informativo
- Entrega de documentos directamente a cada funcionario del Complejo de ser Necesario.
- Utilización de Diferentes medios de comunicación a los funcionarios para dar a conocer la Política de Seguridad del Complejo 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. –

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DEL COMPLEJO HOSPITALARIO

SAN JOSE DE MAIPO

AÑO 2019

INDICE

1. OBJETIVO

Esta Política General de Gestión de Seguridad de la Información establece los lineamientos de la estructura documental del Sistema de Seguridad de la Información aprobado mediante Resolución Exenta N° 4632 de fecha 30 de noviembre de 2018, de la Dirección del Servicio de Salud Metropolitano Sur Oriente. Esto permite gestionar la mejora continua en la protección de la Seguridad de la Información de esta institución.

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.

Esta Política abarca los siguientes controles definidos en la norma NCh- ISO 27001-2013:

- ✓ Políticas para la Seguridad de la Información
- ✓ Revisión de las Políticas de Seguridad de la Información
- ✓ Propiedad de los Activos
- ✓ Proveedores

La presente política se aplica sobre todo tipo de información, considerando todo medio de soporte y presentación, como son la voz y medios digitales, ya sean magnético, óptico, electrónico o fotográfico.

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 de la Norma NCh-ISO 27.001:2013 Análisis de requisitos e implementación relacionados	
A.05	Dominio: Políticas de Seguridad de la Información
A.05.01.01	Política de Seguridad de la Información
A.05.01.02	Revisiones de las Políticas de Seguridad de la Información

DOCUMENTOS DE REFERENCIA

- 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: https://www.csirt.gob.cl/decretos.html
  - ✓ Leyes relacionadas: https://www.csirt.gob.cl/leyes.html
- Marco normativa para las funciones en el Sector Salud, como:
  - ✓ Ley N° 19.628 sobre la protección de la vida privada, Ministerio Secretaría General de la Presidencia.
  - ✓ Ley N° 20.285 sobre acceso a la información pública, Ministerio Secretaría General de la Presidencia.
  - ✓ D.F.L N° 29 que fija texto refundido, coordinado y sistematizados de la ley N° 18.834, sobre Estatuto Administrativo.
  - ✓ Ley N°19.653 Ministerio o Secretaría 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 clínicas de manera de resguardar el correcto empleo, disponibilidad y confidencialidad de las mismas.

Otros documentos:

- ✓ Resolución Exenta N° 1161, que aprueba Sistema de Seguridad de la Información de las Subsecretarías de Salud Pública y Redes Asistenciales.
- ✓ Resolución Exenta N° 1481 del 24.11.2017, que aprueba Política General de Seguridad de la Información para las Subsecretarías de Salud Pública y Redes Asistenciales.
- ✓ Modelo de madurez de procesos de seguridad de la información propuestos a nivel Sector Salud Pública.
- ✓ Documentos normativos de Seguridad de la Información del Ministerio de Salud: http://web.minsal.cl/seguridaddelainformación/

Normas del Sistema de Gestión de Seguridad de la Información:

- ✓ NCh-ISO 27001:2013 Análisis de requisitos e implementación.
- ✓ NCh-ISO 27002:2013 Código de prácticas para los controles de seguridad de la información.

3. DEFINICIONES

- ✓ **Activo**: Cualquier elemento, objeto u otro, que tenga valor para la institución.
- ✓ **Información:** Es la interpretación que se da a los datos. Toda forma que contenga datos relacionados con la organización.
- ✓ **Activo de Información**: Todos los elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de la información de valor para la institución, independiente de su naturaleza, medio o forma de presentación.
- ✓ **Autenticación**: Asegurar la confirmación de la identidad de un usuario, es decir, garantizar que cada una de las partes es realmente quien dice ser.
- ✓ **Buen Uso**: se entiende al uso adecuado de lo estipulado en las políticas de seguridad del SSMSO, quien se reserva el derecho de tomar medidas disciplinarias para sancionar, en caso de existir evidencias de no cumplimiento de estas disposiciones.
- ✓ **Seguridad de la Información**: Es la preservación de la confidencialidad, la integridad y la disponibilidad de la información de la Dirección del Servicio de Salud Metropolitano Sur Oriente
- ✓ **Sistema de gestión de la seguridad de la información (SGSI)**: parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, monitorear, revisar y mejorar la seguridad de la información.
- ✓ **Evento de Seguridad de la Información**: ocurrencia identificada de un estado de un proceso, sistema y/o servicio que indica una posible violación a la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.
- ✓ **Incidente de Seguridad de la Información**: un evento o serie de eventos de seguridad de la información no deseada o inesperada que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- ✓ **Información Confidencial**: Toda aquella que tenga el potencial de afectar la continuidad operacional de la institución, el prestigio, la imagen del SSMSO.

- ✓ **Información Interna:** Es toda aquella información que al ser divulgada, adulterada o destruida, sin generar un daño grave al SSMSO, produzca un perjuicio operacional que involucre pérdida de tiempo y recursos en su recuperación/reposición.

- ✓ **Información Pública**: Información que por su naturaleza no presenta riesgos para el SSMSO y que puede ser divulgada al público general. •

- ✓ **No Repudio**: Dar garantía de que el usuario no pueda negar la operación realizada.

- ✓ **Propietario de la Información**: usuario responsable de la información y el proceso que este utilice (manuales, electrónicos). • Recuperación: Restauración de las capacidades de proceso de sistemas a las condiciones de operación normales.

- ✓ **Terceros**: Personal externo a la institución que pertenece a una de las siguientes categorías:

  - **Proveedor**: Empresas prestadoras de servicios, empresas contratistas, subcontratistas y cualquiera, que por cuenta propia o de terceros, desarrolle trabajos para o por cuenta del CHSJM.

  - **Visitante**: Toda persona externa de la institución, que, sin ser proveedor o cliente, se le autoriza de manera restringida el acceso a las instalaciones/recursos del CHSJM. En esta categoría están los familiares, amigos de los empleados, clientes potenciales, auditores y vendedores.

  - **Usuario**: Toda persona natural a la cual se le concede autorización para acceder a lugares físicos, información y sistemas del CHSJM. Incluyendo al propio personal (interno o externo) de la organización, y a terceros. Adicionalmente, serán aplicables las definiciones que se establezcan en la normativa vigente asociada a la Seguridad de la Información.

4. ROLES Y RESPONSABILIDADES

- **Encargado de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.**

  - ✓ Actuar como asesor en materias relativas a seguridad de la información para la Dirección del Complejo Hospitalario San José de Maipo.

  - ✓ 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

- **Comité de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.**

  - Supervisar la implementación de la estructura documental del Sistema de Seguridad de la información, aplicable en el Complejo Hospitalario San Jose de Maipo.

  - 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 del Complejo Hospitalario San José de Maipo.

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

- **Comité Técnico de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.**

✓ Elaborar Políticas de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.

✓ Elaborar Procedimientos de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.

✓ Elaborar, implementar y realizar seguimiento al Plan de Comunicación y Consulta del Sistema de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.

✓ Implementar el Sistema de Seguridad de la Información del Complejo Hospitalario San Jose de Maipo.

✓ 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.

- **Usuarios Finales**

Se debe entender como usuarios finales a todos quienes tienes la responsabilidad de acatar las políticas y normativas definidas, independiente que además tengan otro rol nominado en este ámbito. Debe considerar:

- Todos los funcionarios (planta, contrata, reemplazos y suplencia)
- Personal a Honorarios
- Terceros (proveedores, compra de servicios, servicios externalizados, etc.)

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

5. DE LA POLÍTICA

La Dirección del Complejo Hospitalario San Jose de Maipo se compromete a gestionar la seguridad de la Información como un proceso continuo en el tiempo, que se debe cumplir en el marco de la normativa gubernamental existente, por medio de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que el Servicio determine. Para estos efectos, esta Dirección del Complejo, se basará 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 adecuados de integridad, confidencialidad y disponibilidad, de todos sus activos de información relevantes para la institución, como un principio clave en la gestión de sus procesos.

6.1 LINEAMIENTOS ESTRATÉGICOS

6.1.1 Decálogo de principios de Seguridad de la Información

- ✓ Promover la información como un activo vital de quehacer de la Dirección del Complejo Hospitalario San Jose de Maipo.
- ✓ Proteger la privacidad y confidencialidad de toda información sensible o de carácter personal, independiente de su formato, medio de soporte y almacenamiento.

- ✓ Preservar la integridad de los datos, ya que de su exactitud, actualización y veracidad pueden llegar a depender de una vida.

- ✓ Asegurar que la información crítica estará disponible a tiempo y forma sólo para quienes estén debidamente autorizados para tener acceso a ella.

- ✓ Establecer un modelo de gestión de riesgos para la seguridad de la Información; que permita determinar el tipo y naturaleza de controles necesarios para la mitigación de los riesgos identificados como relevantes.

- ✓ Cumplir con el marco normativo establecido para la seguridad de la información del Sector Salud e institucional, mediante la gestión de los controles definidos.

- ✓ Mantener un adecuado respaldo y resguardo de la información gestionada en el Complejo Hospitalario San Jose de Maipo, que permitan prevenir eventuales pérdidas o daño de ella.

- ✓ Habilitar equipos y Sistemas de identificación, análisis, notificación, respuesta resguardo de registros y aprendizaje frente a debilidades e incidentes de seguridad de la información, permitiendo su mitigación y evitando su recurrencia.

- ✓ Desarrollar programas de formación para todo el Personal de la Dirección del Servicio de Salud Metropolitano Sur Oriente.

6.1.2 Identificación de requisitos para la Seguridad de la Información

La Dirección del Complejo Hospitalario San Jose de Maipo deberá periódicamente identificar y analizar las fuentes que generan requisitos de seguridad de la información, en donde se destaca:

- ✓ Un modelo y una metodología formal de gestión de riesgos, consistente con los cambios de la Dirección de este complejo asistencia y de los lineamientos del Sector Salud.

- ✓ Los requisitos legales, normativos y contractuales que aplica al Sector de Salud, sobre todo los que generan nuevos requerimientos de protección de confidencialidad, integridad, disponibilidad, trazabilidad y gestión en general de la protección de información sensible.

- ✓ Los eventos adversos propios o provenientes de amenazas externas que hayan ocurrido recientemente, dejando en evidencia debilidades en sus actuales sistemas de protección o modelos de control en seguridad de la información.

- ✓ Las amenazas del ciberespacio, que deben ser monitoreadas y analizadas para determinar su potencial riesgo.

- ✓ Los propios lineamientos de la Dirección del Complejo Hospitalario San Jose de Maipo y procesos de innovación, por su relación con apertura de nuevos frentes o factores de riesgo.

6.1.3 Lineamientos estratégicos de Seguridad de la Información para la Dirección del Complejo Hospitalario San Jose de Maipo:

Los siguientes son lineamientos estratégicos de Seguridad de la Información, obligatorios para el complejo Hospitalario son:

- ✓ La información, en todas sus formas y presentaciones, es un activo vital para todo el Sector Salud, también lo son los activos necesarios para sus procesos, como tecnologías, instalaciones físicas y personas involucradas.

- ✓ La Seguridad de la Información es un atributo necesario en los servicios ofrecidos, entendiendo que la protección de la disponibilidad, integridad y confidencialidad de dicha información es una condición básica e indispensable del Sector Salud.

- ✓ Para brindar gobernabilidad se define una estructura organizacional compuesta a nivel estratégico por:

A nivel Táctico: Encargado de Seguridad de la Información del Complejo Hospitalario, es responsable de coordinar las implementaciones asociadas a la seguridad de la información y a nivel operacional por los usuarios finales responsables de cumplir el marco normativo.

- ✓ Todo colaborador es responsable de la información que manipula; así como del correcto uso de los recursos tecnológicos que le hayan sido asignados para apoyar tareas relacionadas con la Seguridad de la Información y con sus obligaciones laborales.

- ✓ De esta política general y de una evaluación permanente de riesgos en la seguridad de la información se desprenden un conjunto de políticas, procedimientos, estándares, instructivos y otros elementos que conforman el marco normativo, así como otros tipos de controles necesarios para la Gestión de Seguridad de la Información.

- ✓ Para mejorar la cultura organizacional, se considera primordial la difusión, capacitación y concientización de estos lineamientos y todo el marco normativo de Seguridad de la Información para los trabajadores y terceros que brinden servicio en la institución.

- ✓ En todo proyecto o actividad se debe maximizar el esfuerzo en cumplir tempranamente con el marco normativo de Seguridad de la Información; así como todo regulación y legislación vigente aplicable. Del mismo modo permitir una gestión de mejora continua, debiese considerarse un modelo que integre etapas de planificación, implementación, monitoreo y mejora, según corresponda.

- ✓ Todos los usuarios que tomen conocimiento de una amenaza interna o externa, deliberada o accidental, sea una actividad o situación que afecte actual o potencialmente la seguridad de los activos de información, deben informarlo de inmediato a su instancia organizacional superior.

- ✓ Ésta política debe ser conocida y respetada, al igual que las restantes normas de Seguridad de la Información, como parte de los deberes de cada funcionario, personal honorarios o terceros. Su no cumplimiento será considerado una falta grave contra la protección de los intereses y los activos de la institución. El incumplimiento de las obligaciones emanadas de esta Política, de las políticas específicas, procedimientos u otros documentos que se deriven de éstos, serán sancionados en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del Complejo Hospitalario. Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, se procederá al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

6.1.4 Lineamientos estratégicos de Gestión de mejora continúa

Se debe estructurar y mantener un modelo de Gestión de mejora continua para el Sistema de Seguridad de la Información; que permita desarrollar cada uno de los procesos necesarios para mantener en el tiempo los controles de Seguridad, con el objetivo de avanzar en los Niveles de madurez de procesos propuestos a nivel del sector salud.

Este lineamiento sectorial, se orienta al cómo mantener la gestión en el tiempo y para ello, se recomienda, el uso de Modelo Deming, conocido como PDCA, por sus siglas de Plan Do, Check, act. Puede ser otro modelo equivalente, que propicie una mejora continua.

6.1.5 Lineamientos estratégicos de Modelo de Gestión de Riesgo

Se debe estructurar y mantener, a su vez, un modelo de Gestión de mejora continua para los riesgos o potenciales problemas en Seguridad de la Información; que permita analizar las situaciones que ponen en peligro el cumplimiento institucional y sectorial de protección de la confidencialidad, integridad y disponibilidad de la información, identificando el tipo y naturaleza, además de priorizando y asignando los controles de mitigación necesarios para los riesgos determinados como relevantes para la institución.

Este lineamiento sectorial, se oriente al por qué mantener una gestión sobre las potenciales amenazas, vulnerabilidades e impactos a la seguridad de la información, de modo que permita justificar en el tiempo los controles aplicables a su mitigación.

6.1.6 Estructura documental en gestión de Seguridad de la Información

La estructura documental se encuentra definida en el Sistema de Seguridad de la Información y se encuentra conformado por una Política de Seguridad de la Información, que se aprueba por este acto. Políticas específicas de seguridad de la información, procedimientos de operación, instructivos y registros.

Tales documentos se encuentran definidos en la Resolución que aprueba dicho sistema entendiéndose por:

- ✓ **Política de Seguridad:** intenciones globales y orientación de la organización, relativas a la seguridad de la información, tal como se expresan formalmente por la dirección.

- ✓ **Política General de la Seguridad de la Información:** política que establece el enfoque de la organización para administrar sus objetivos de Seguridad de la Información.

- ✓ **Políticas específicas de Seguridad de la Información:** políticas 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.

- ✓ **Procedimientos:** documento operativo que establece la forma específica para llevar la planificación, operación y control de las actividades o procesos de seguridad de la información.

- ✓ **Instructivos:** documentos que describen como (instrucciones, formularios, checklist) se realizan las tareas y las actividades específicas relacionadas con la Seguridad de la Información.

- ✓ **Registros:** Evidencia objetiva del cumplimiento de los requisitos SGSI; están asociados a documentos de los otros cinco niveles como output que demuestra que se ha cumplido con lo indicado en los mismos.

6.1.7 Lineamientos estratégicos para la gestión de la Madurez de los procesos del Sistema de Seguridad de la Información

Para homogenizar una mirada de avance y desarrollo de los principales procesos necesarios del Sistema de Seguridad de la Información de esta Dirección, se definirá una base de medición estandarizada para los niveles de madurez de dichos procesos, la que se fundamenta en los niveles de madurez de marcos de referencia internacionales como CMM, CobiT, ISO/IEC 15504. Esto permitirá contrastar la realidad de la institución con cierto nivel deseable como línea base para dicha temática, lo que permite extraer brechas o GAPs y sobre ellas facilitar la planificación de controles de mitigación. Asimismo, se propone analizar los controles de Seguridad de la información bajo dicho modelo de niveles de Madurez de Procesos.

A lo menos una vez al año se debe contrastar la aplicación de cada lineamiento como un proceso de control de seguridad de la información, evaluando su nivel de madurez, por auditoría interna del Complejo Hospitalario o por una parte no involucrada directamente en dicho control.

Se debe priorizar los esfuerzos para alcanzar una línea base de nivel de madurez que será al menos en los procesos de control que se debe priorizar. Por ejemplo, alcanzar un nivel de madurez 3 o formalizado, esto consideraría, entre otros, contar con una política y un procedimiento y/o instructivo, que permita formalizar el quehacer en dicho tema (ver estándar propuesto del Modelo de niveles de madurez de procesos MINSAL).

El GAP o brecha entre la situación actual y el nivel de línea de base, determinarán las acciones de mitigación necesarias, que se obtienen de los requerimientos solicitados en el nivel inmediatamente superior del modelo de madurez. Se debe mantener un Sistema de mejora continua en cada uno de tales procesos de control, utilizando para ello el modelo Deming señalado.

Por lo anterior, para su implementación se requiere que para cada control 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, mediante la implementación de las condiciones solicitadas. Para los controles en curso se debe mantener la gestión y procurar alcanzar niveles superiores de madurez del proceso. La mejora continua se logra precisamente avanzando al siguiente nivel de madurez propuesto del modelo.

El modelo propuesto considera niveles de madurez del proceso, evaluados de 5 a 0 como:

5- Resiliente: El proceso se adecúa y reacciona a los cambios del entorno.
4- Gestionado: Se tiende a la mejora continua de la forma de hacer las cosas.
3- Formalizado: Se documentan y formalizaran las acciones a seguir.
2-Repetible: Existen acuerdos prácticos de repetición de la forma de hacer las cosas.
1-Básico: Se realiza el proceso caso a caso en forma independiente por cada individuo.
0-Inexistente: Carencia completa de cualquier proceso reconocible.

Este modelo propuesto a nivel Sectorial por el Ministerio de Salud, debe ser adecuado y formalizado como estándar propio de la Dirección de este Servicio de Salud, para facilitar la evolución de sus procesos de gestión.

Para mayor detalle, revisar los siguientes documentos:

- Documento sectorial de modelo de niveles de madurez de procesos en el ámbito de Gestión de Seguridad de la Información Sector Salud, disponible en sitio de este Ministerio.

- Documento de modelo de madurez y avances respectivos de la Dirección del Servicio de Salud.

7. Mecanismos de difusión y distribución

Esta Política General, se encontrará vigente página web del Complejo Hospitalario en un banner, cuyo nombre será: Sistema de Gestión de Seguridad de la Información

El Encargado de Seguridad de la Información del Complejo Hospitalario, velará por maximizar la cobertura de su difusión, a lo menos a través de:

- Publicación en la página web del Complejo Hospitalario
- Correo informativo
- Entrega de documentos directamente a cada funcionario del Complejo de ser Necesario.
- Utilización de Diferentes medios de comunicación a los funcionarios para dar a conocer la Política de Seguridad del Complejo 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. –