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

COMPLEJO HOSPITALARIO SAN JOSE DE MAIPO

ACREDITADO

APRUEBA SISTEMA DE SEGURIDAD DE LA INFORMACION DEL COMPLEJO HOSPITALARIO SAN JOSE DE MAIPO.

RESOLUCION EXENTA N° 000685 /

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 para 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 este Complejo, 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 que esté replicado en los Establecimientos Hospitalarios de la red Sur Oriente, con el objetivo de gestionar la seguridad de la información de forma homogénea.

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

RESOLUCIÓN

ARTICULO N°1-

APRUÉBESE el siguiente Sistema de la Seguridad de la Información para el Complejo Hospitalario San José de Maipo:

1. DECLARACIÓN INSTITUCIONAL:

Las Tecnologías de la información y de las comunicaciones (TIC), al ser incorporadas progresivamente a los procesos institucionales y al quehacer de los funcionarios al ejercer sus labores en el Complejo Hospitalario San José de Maipo, presentan una serie de beneficios, ventajas y oportunidades, pero conllevan, también, ciertos riesgos, que pueden eventualmente afectar a los activos de información institucional.

Por consiguiente, gestionar la Seguridad de la Información es un imperativo 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 la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles 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.

El Complejo Hospitalario San José de Maipo se compromete a gestionar la seguridad de información como un proceso continuo en el tiempo, a través de un programa de implantación del tipo "Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma Chilena Oficial NCh- ISO27001: Of2013, con el objeto de preservar los activos de información institucional con respecto a:

- **Su Integridad:** la información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. Este principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas del negocio, así como evitar fraudes o irregularidades de cualquier índole que haga que la información sea alterada.

- **Su Confidencialidad:** la información sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones. Este principio fundamental de seguridad busca garantizar que toda información de los funcionarios, funcionarios y proveedores, y sus medios de procesamiento o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

- **Su Disponibilidad:** La información debe estar disponible para el personal, usuarios y entidades reguladoras de manera oportuna y acorde a sus niveles de autorización. Este principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando ésta es requerida por el proceso de la institución. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento o equipamiento de procesamiento.

2. OBJETIVOS DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

2.1 Objetivo General

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucionales relevantes, asegurando la continuidad operacional de los procesos.

2.2 Objetivos Específicos

Identificar y catastrar todos los activos de información relevantes que están presentes directa o indirectamente en los procesos de la institución, abarcando tanto los procesos críticos, como los de soporte.

Realizar actividades necesarias de análisis de riesgo, según normativas, técnicas y estándares disponibles y aplicables, para diseñar e implantar medidas y controles que permitan mitigar los riesgos que sean identificados, sin perder de vista el enfoque de la gestión por procesos institucionales.

Proteger la información, sus medios de procesamiento, conservación y transmisión del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarla o ponerla en riesgo.

Mantener y hacer uso de la estructura y el marco de estándares, políticas y procedimientos en materia de seguridad de la información.

Minimizar la posibilidad de ocurrencia de hechos contingentes que pudieran interrumpir las operaciones y reducir el impacto de los daños a las instalaciones, medios de almacenamiento, equipos de procesamiento y de comunicación.

Contar y hacer uso de planes de continuidad operacional ante hechos contingentes que interrumpan la operación del servicio.

Sensibilizar y capacitar a los funcionarios del Complejo, acerca de su responsabilidad para mantener la seguridad de la información como un aspecto relevante en los procesos de esta Institución.

3.- ESTRUCTURA DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

3.1 La estructura documental del Sistema de Seguridad de la Información, estará conformado por una Política General de seguridad de la información, políticas específicas de seguridad de la información, procedimientos de operación instructivos y registros.

Se entenderá 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 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 cómo (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 del SGSI: están asociados a documentos de los otros cinco niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

3.2 Aprobación de una Política y otros documentos

Las políticas de seguridad de la información, los procedimientos de operación y los instructivos serán aprobadas por el director del Complejo Hospitalario San José de Maipo, sin perjuicio de su facultad para delegar la firma de tales documentos.

4. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

4.1 Integrantes del Comité de Seguridad de la Información

Para el logro de los objetivos descrito, existirá un Comité de Seguridad de la información del Servicio de Salud, compuesto por los siguientes funcionarios de esta Institución:

- Director (a) del Complejo Hospitalario San José de Maipo, quien presidirá el presente Comité.
- Subdirector(a) Administrativo del Complejo Hospitalario San José de Maipo.
- Subdirector (a) Médico del Complejo Hospitalario San José de Maipo
- Jefe (a) Departamento de Gestión y Desarrollo de las Personas del Complejo Hospitalario San José de Maipo.

- Jefe (a) Departamento de Finanzas del Complejo Hospitalario San José de Maipo
- Asesor (a) Jurídico de la Complejo Hospitalario San José de Maipo
- Encargado (a) de Informática de la Complejo Hospitalario San José de Maipo
- Encargado (a) de Seguridad de la Información Institucional
- Todo Profesional y/o funcionario de la Complejo Hospitalario San José de Maipo (su asistencia se efectuará según solicitud del Comité).

En caso de ausencia de los miembros titulares del Comité de Seguridad de la Información, deberán asistir a las reuniones los subrogantes formalizados por el solo ministerio de la ley, o bien, a quien la respectiva autoridad haya designado esta facultad.

4.2 Funciones del Comité

- Supervisar la implementación de la estructura documental del Sistema de Seguridad de la información, aplicable en el Complejo Hospitalario San José 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 Complejo.
- 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 (SGSI) al interior de la institución.

A lo menos una vez al año, el comité de Seguridad de la Información del Complejo Hospitalario San José de Maipo, debe evaluar el cumplimiento de la Política General de Seguridad de la Información, considerando cambios que surjan en el transcurso de este periodo que podrían afectar el enfoque de la organización a la gestión de seguridad de la información, incluyendo cambios al ambiente de la organización, circunstancias de los servicios sanitarios, disponibilidad de recursos, condiciones contractuales, reguladoras, y legales, o cambios al ambiente técnico. Para ello debe considerar los siguientes aspectos:

- ✓ Retroalimentación de las partes interesadas.
- ✓ Resultados de las revisiones efectuadas por terceras partes.
- ✓ Estado de acciones preventivas y correctivas.
- ✓ Cambios en los procesos institucionales, nueva legislación, tecnología, etc.
- ✓ Alertas antes amenazas y vulnerabilidades.
- ✓ Información relacionada a incidentes de seguridad.
- ✓ Recomendaciones provistas por autoridades relevantes.
- ✓ Medición de los indicadores del Sistema.

4.3 Funcionamiento del Comité

El Comité designará entre sus integrantes un secretario, quien llevará un registro de actas de las reuniones periódicas del Comité, con su respectivo control de asistencia. El Encargado de Seguridad de la Información, velará por la mantención actualizada de estos registros.

En los casos que el secretario designado no asistiese a una reunión del Comité se designará a un reemplazante, quien efectuará el registro del acta correspondiente con su respectivo control de asistencia de la reunión y posteriormente entregará estos antecedentes al secretario titular.

Para aquellos casos que se encuentre impedido de participar en alguna reunión del Comité, el integrante del Comité podrá designar un suplente, que lo reemplazará en sus funciones con derecho a voz y voto.

El quórum mínimo de funcionamiento del Comité será de cuatro de sus integrantes. Sus acuerdos se adaptarán por mayoría de votos. En caso de empate dirimirá el presidente del Comité.

En todos lo demás, el Comité acordará su forma de funcionamiento y normas que estime necesarias.

5. Comité Técnico Seguridad de la Información.

5.1 Integrantes del Comité de Seguridad de la Información

- Encargado (a) de Informática del Complejo Hospitalario San José de Maipo, quien presidirá el presente Comité.
- Encargado/a de Seguridad de la Información Institucional
- Coordinador/a General de redes y Comunicaciones del Complejo Hospitalario San José de Maipo.
- Jefe/a de Soporte y Mesa de Ayuda del Complejo Hospitalario San José de Maipo.
- Todo Profesional y/o funcionario del Complejo Hospitalario San José de Maipo (su asistencia se efectuará según solicitud del presidente del presente Comité Técnico).

5.2 Funciones del Comité

- Elaborar Políticas de Seguridad de la Información del Complejo Hospitalario San José de Maipo.
- Elaborar Procedimientos de Seguridad de la Información del Complejo Hospitalario San José de Maipo.
- Elaborar, implementar y realizar seguimiento al Plan de Comunicación y Consulta del Sistema de Seguridad de la Información del Complejo Hospitalario San José de Maipo.
- Implementar el Sistema de Seguridad de la Información del Complejo Hospitalario San José 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.

5.3 Funcionamiento del Comité

El Comité Técnico de Seguridad de la Información del Complejo Hospitalario San José de Maipo., sesionará al menos dos veces al año.

El Comité designará entre sus integrantes un secretario, quien llevará un registro de actas de las reuniones periódicas del Comité, con su respectivo control de asistencia. El Encargado de Seguridad de la Información, velará por la mantención actualizada de estos registros.

En los casos que el secretario designado no asistiere a una reunión del Comité se designará a un reemplazante, quien efectuará el registro del acta correspondiente con su respectivo control de asistencia de la reunión y posteriormente entregará estos antecedentes al secretario titular.

Para aquellos casos que se encuentre impedido de participar en alguna reunión del Comité, el integrante del Comité podrá designar un suplente, que lo reemplazará en sus funciones con derecho a voz y voto.

El quórum mínimo de funcionamiento del Comité será de tres de sus integrantes. Sus acuerdos se adaptarán por mayoría de votos. En caso de empate dirimirá el Encargado de Seguridad de la Información.

En todos lo demás, el Comité acordará su forma de funcionamiento y normas que estime necesarias.

6. Encargado de Seguridad de la Información

El Encargado de Seguridad de la Información tendrá las siguientes funciones:

- 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.

7. Gestión de la Seguridad de la Información en Establecimientos Hospitalarios red Sur Oriente

7.1 Cada Establecimiento Hospitalario de la red Sur Oriente, deberán apoyar al Sistema de Seguridad de la Información, para lo cual deberá existir en cada Hospital de la red Sur Oriente un Encargado de Seguridad de la Información y un Comité de Seguridad de la Información, que esté compuesto al menos:

- ✓ Subdirector Administrativo
- ✓ Subdirector de Gestión Asistencial
- ✓ Subdirector de Gestión y Desarrollo de las Personas
- ✓ Jefe Departamento de Informática.
- ✓ Jefe Departamento de Finanzas

Se recomienda que, en caso de existir los siguientes cargos en los Hospitales de la red, las personas que cumplen también integren el Comité de Seguridad:

- ✓ Jefes y/o Encargados de Procesos
- ✓ Jefes y/o Encargados de riesgos
- ✓ Encargado/as de Gestión de Calidad

El Comité deberá contar con un secretario.

7.2 Los Comité de Seguridad de la Información de cada Establecimiento tendrán las siguientes funciones (aspectos referenciales):

- Supervisar la implementación de las Políticas de Seguridad de la Información y de los procedimientos estándares que se desprenden de tales instrumentos.

- Proponer al Jefe de Servicio estrategias y soluciones específicas para la implementación de los controles necesarios para materializar las políticas de seguridad particulares del Servicio e instituciones dependientes y la debida solución de las situaciones de riesgos detectadas.

- Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones sobre ello.

- Coordinarse con Comités de Seguridad de otros Establecimientos Hospitalarios de la red sur oriente y la Dirección del Servicio, para mantener estrategias comunes de gestión y reportar a la alta dirección, respecto a oportunidades de mejora en el SGSI del Servicio, así como de los incidentes relevantes y su gestión.

- Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para materializar las políticas establecidas y la debida solución de las situaciones de riesgos detectadas.

7.3 El Director (a) del Complejo Hospitalario San José de Maipo, deberá designar a un Encargado de Seguridad de la Información a objetivo que cumpla las siguientes funciones (aspectos referenciales):

- Organizar las actividades del Comité de Seguridad de la Información
- 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.
- 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 organización, controlar su implementación y velar por su correcta aplicación.
- Establecer puntos de enlace con Encargados de seguridad de otros Establecimientos Hospitalario y Dirección del Servicio y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

Dos veces en el año, se reunirá el Encargado de Seguridad del Información Complejo Hospitalario San José de Maipo con Encargados de Establecimientos Hospitalarios de la red Sur Oriente, con el fin de revisar implementación de la Seguridad de la Información en cada Institución.

8. DIFUSIÓN

El Complejo Hospitalario San José de Maipo, al igual que los Establecimientos Hospitalarios de la red y la Dirección del Servicio, establecerán canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos generados en el marco del Sistema de Seguridad de la información.

Algunos de los canales accesibles y formales de difusión son: correo electrónico, intranet, comunicación impresa, charlas y/o capacitaciones.

Todas las políticas procedimientos y documentos relacionados se informarán a cada funcionario a través de correos masivos, boletines informativos, intranet, pagina web institucional u otras actividades de difusión que se definan para tal efecto.

9. SANCIONES

El incumplimiento de las obligaciones que impone el presente Sistema de Seguridad de la información, como el que establezcan política del Sistema, los procedimientos u otros documentos que se deriven de éstos, serán sancionadas en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del Complejo Hospitalario San José de Maipo. 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 tales infracciones.

ARTÍCULO 2.

ESTABLEZCASE la obligación del Encargado de Seguridad de la Información de difundir la política fijada en este instrumento y velar por su cumplimiento en el Complejo Hospitalario San José de Maipo.

ANOTESE, COMUNIQUESE Y ARCHIVESE

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. -