Servicio de Salud Metropolitano Sur Oriente
Región Metropolitana
Ministerio de Salud

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

4778 *10.12.2018

APRUEBA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

DE LA DIRECCIÓN DEL SERVICIO DE SALUD METROPOLITANO SUR ORIENTE

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, actualiza y formaliza la Política General de la Seguridad de la Información en esta institución, dictando lo siguiente:

RESOLUCIÓN

ARTICULO N°1- APRUEBASE la Política General de Seguridad de la Información para 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 N° 2. DESEJE SIN EFECTO, Resolución Exenta N° 1498 de fecha 26.04.2017: Aprueba Política de Seguridad de la Información del Servicio de Salud Metropolitano Sur Oriente.

ARTICULO N°3 La presente Resolución surtirá sus efectos a contar de esta fecha

ANOTESE, COMUNIQUESE Y ARCHIVESE

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
- Asesoría Jurídica S.S.M.S.O
- Departamento de Auditoría Interna S.S.M.S.O
- Oficina de Partes S.S.M.S.O

TRANSCRITA FIELMENTE

MINISTRO DE FE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DE LA DIRECCIÓN DEL SERVICIO DE

SALUD METROPOLITANO SUR ORIENTE

AÑO 2018

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

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 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

3. 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.

4. 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 SSMSO.

  - **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 SSMSO. 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 SSMSO. 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.

5. ROLES Y RESPONSABILIDADES

- **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

- **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.

- **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.

- **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.

6. DE LA POLÍTICA

La Dirección del Servicio de Salud Metropolitano Sur Oriente 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 Servicio, 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 Servicio de Salud Metropolitano Sur Oriente.
- ✓ 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 la dirección del Servicio de Salud Metropolitano Sur Oriente, 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 Servicio de Salud Metropolitano Sur Oriente 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 Servicio de Salud y 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 Servicio de Salud Metropolitano Sur Oriente 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 Servicio de Salud Metropolitano Sur Oriente y sus Establecimientos Hospitalarios de la red:

Los siguientes son lineamientos estratégicos de Seguridad de la Información, obligatorios para la Dirección del Servicio y que deben servir de guía para los Establecimientos Hospitalarios de la red Sur Oriente:

- ✓ 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:

Comité de Seguridad de la Información, a nivel de Dirección y a nivel de Establecimientos Hospitalarios.
Comité Técnico de Seguridad de la Información, a nivel de Dirección del Servicio de Salud Metropolitano Sur Oriente.

A nivel Táctico: Encargado de Seguridad de la Información tanto a nivel de Dirección del Servicio y sus pares locales en los Establecimientos Hospitalarios de la red Sur Oriente, responsables 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 de la Dirección del Servicio de Salud Metropolitano Sur Oriente. 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 continua

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 de la Dirección del Servicio de Salud 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, en su versión N°2, se encontrará vigente 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 lo menos 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. CONTROL DE CAMBIOS

Fecha	Versión	Página	Numeración del contenido	Cambio Efectuado / Nombre del responsable
15.11.2018	V.2	Todas las Páginas		Cambio todo el documento/ Cinthia León Fuentealba, Encargada de Control Interno de la Dirección del Servicio de Salud Metropolitano Sur Oriente

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

MINISTERIO DE SALUD
SERVICIO DE SALUD METROPOLITANO
SUR ORIENTE
ASESORIA JURIDICA
DR.AIB./HPR./JLRD./lpg.

ASESOR JURIDICO
S.S.M.S.O.

RESOLUCION EXENTA N° 26.04.2017 001498

VISTOS: Estos antecedentes; lo solicitado mediante Prov. s/N de Sr. Director del Servicio, que requiere la aprobación del documento denominado Política de Seguridad de la Información, del Servicio de Salud Metropolitano Sur Oriente; teniendo presente lo establecido en el artículo 8°, número II, letra f) del Reglamento Orgánico de los Servicios de Salud, aprobado por Decreto N°140 de 2004, de Salud; Resolución N°1.600 de 2008 de la Contraloría General de la República, Decreto con Fuerza de Ley N°1 de 2005, de Salud, que fija el texto refundido, coordinado y sistematizado del Decreto Ley N°2.763/79 y de las Leyes N°18.933 y N°18.469 y las facultades que me confiere el Decreto Supremo N°12 de 06 de Febrero de 2015, de Salud, dicto la siguiente:

R E S O L U C I O N

1.- **APRUEBASE** el documento denominado **POLITICA DE SEGURIDAD DE LA INFORMACION SERVICIO DE SALUD METROPOLITANO SUR ORIENTE.**

2.- Dicho documento será de uso obligatorio en dicho establecimiento.

3.- La presente Resolución surtirá sus efectos a contar de esta fecha.

ANOTESE Y COMUNIQUESE,

SERVICIO SALUD SUR ORIENTE
DIRECTOR

DR. ANTONIO INFANTE BARROS
DIRECTOR
SERVICIO DE SALUD
METROPOLITANO SUR ORIENTE

DISTRIBUCION:
-Dirección S.S.M.S.O.
-Subdirección Administrativa S.S.M.S.O.
-Subdirección de RR.HH. S.S.M.S.O.
-Depto. Informática S.S.M.S.O.
-Encargado de Seguridad de la Información S.S.M.S.O.
-Asesoría Jurídica S.S.M.S.O.
-Oficina de Partes

SERVICIO SALUD METROP. SUR ORIENTE
MINISTRO DE FE

TRANSCRITA FIELMENTE
MINISTRO DE FE

Política de Seguridad de la Información
Servicio de Salud Metropolitano Sur Oriente
SSMSO

Sistema de Seguridad de la Información
Marzo 2016

Control Documental

HISTORIA DEL DOCUMENTO	
Nombre del Documento	Política de la Seguridad de la Información del Servicio de Salud Metropolitano Sur Oriente
Responsable del Documento	Cristian Roitman P. Jefe de Soporte y Redes Encargado de Seguridad de la Información del SSMSO
Creado por	Cristian Roitman P.
Aprobado por	Comité de Seguridad de la Información
Fecha de Creación	Marzo 2016

CONTROL DE VERSIONES			
Versión	Fecha de Vigencia	Aprobación	Comentarios
1.0	Marzo 2016	Comité de Seguridad de la Información	

Política de Seguridad de la Información
Servicio de Salud Metropolitano Sur Oriente

El servicio de Salud Metropolitano Sur Oriente (en adelante SSMSO) reconoce que **la información es un activo esencial** para el desarrollo de los procesos institucionales y establece el compromiso de la protección de la misma, con el fin de asegurar la continuidad del negocio, dar cumplimiento a la normativa aplicable, a las definiciones estratégicas vigentes y minimizar los riesgos mediante un conjunto adecuado de normas, procedimientos y controles.

1. Compromiso Institucional

El SSMSO se compromete a implementar, ejecutar, mantener, mejorar y difundir sistemáticamente un sistema de seguridad de la información.

Gestionar la seguridad de la información como un proceso continuo, tal como recomienda la Política General de Seguridad de la Información MINSAL, 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-Of2009*, con el objetivo de preservar los activos de información.

2. Objetivos de la Política de Seguridad de la Información

Este documento define y establece los principios que conforman las Política de Seguridad de la Información. Los pilares fundamentales de esta política van de la mano con los siguientes objetivos:

- Proteger los activos de información de la institución frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad de la información.

- Identificar y catastrar todos los activos de información relevantes que estén presentes directa o indirectamente en cada proceso institucional.

- Realizar las actividades necesarias de análisis de riesgo, según las normativas técnicas y estándares disponibles y aplicables, para diseñar e implantar medidas y controles que permitan mitigar los riesgos que sean identificados.

- Asegurar la implementación, ejecución, mantención mejora continua y difusión del sistema de seguridad de la información.

- Minimizar la posibilidad de ocurrencia de hechos contingentes que pudieran interrumpir la operación de la institución y reducir el impacto de los daños a la infraestructura, medios de almacenamiento, equipos de procesamiento y comunicaciones.

- Definir normas y procedimientos en concordancia con las mejores prácticas de la normativa vigente.

- Mantener la Política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia.

- Establecer el compromiso de nuestra institución con la seguridad de los sistemas de información, fijando los pilares de marco normativo de seguridad, su estructura organizativa, gestión, continuidad operativa, y finalmente, velar por el cumplimiento de esta.

- Hacer uso de los planes de continuidad operacional, ante hechos contingentes, que interrumpan la operación normal de la institución.

- Sensibilizar, capacitar, entrenar y difundir a los funcionarios de la institución, en las materias de Seguridad de la Información, mediante talleres, charlas, publicaciones en Intranet y/o correo electrónico, según corresponda.

3. Alcance y Limitaciones

Esta política es de aplicación obligatoria a toda la institución, incluyendo los procesos, a los funcionarios, sistemas de información, aplicaciones, repositorios, entidades externas y proveedores que se relacionan con ésta, en cuando corresponda, estableciendo los lineamientos, responsabilidades y requerimientos necesarios para el Sistema de Seguridad de la Información.

Cubre toda la información contenida en la institución en el presente o en el futuro. La no inclusión explicita en el presente documento no constituye argumento para no proteger los activos de la información que se encuentren en otras formas.

La política cubre toda información en sus distintos estados. Ya este impresa, escrita en papel, almacenada electrónicamente, transmitida por correo electrónico, mostrada audiovisualmente, contenida en una conversación.

Debe ser divulgada y cumplida por todo el personal del SSMSO. Independientemente del cargo, nivel jerárquico y su grado de responsabilidad dentro de la institución.

No pretende ser una política absoluta, está sujeta a modificaciones y mejoras permanentes, producto del trabajo evolutivo del Comité de Seguridad informatica del SSMSO.

Contempla los ámbitos de control específicos contenidos en la *nCh-ISO 27001.Of2009*.

4. Terminología y Conceptos

Para efectos de la presente política y sus documentos relacionados, se definen los siguientes conceptos:

- ***Activo:*** Cualquier elemento, objeto u otro, que tenga valor para la institución.
- **Activo de Información:** será todo aquello que acceda, contenga, administre, transmita, modifique o realice alguna acción sobre la información que tiene valor para la institución.
- ***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.
- ***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 deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- ***Información:*** Es la interpretación que se da a los datos. Toda forma que contenga datos relacionados con la organización.

- ***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.

- ***Seguridad de la Información:*** preservación de la confidencialidad, la integridad y la disponibilidad de la información.

- ***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.

- ***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 SSMSO.

  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 SSMSO. 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 SSMSO. 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.

5. Legislación y Normativas de referencia

Esta política está construida en base al estudio de las leyes y normativas chilenas, en relación con la protección de datos personales, propiedad intelectual y uso de herramientas informatica, así como, las políticas base referentes a seguridad de la información emitidas por el ***Ministerio de Salud***.

Esta política se encuentra dentro del marco legal jurídico definido por las leyes y decretos siguientes:

- *Ley 18168: General de Comunicaciones*
- *Ley 19799: Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.*
- *Ley 19223: Tipifica figuras penales relativas a la informatica.*
- *Ley 17336: Sobre propiedad intelectual*
- *Ley 19628: Sobre protección de la vida privada o protección de datos de carácter personal.*
- *Ley 19812: Sobre protección de la vida privada.*
- *Ley 19927: Ley contra la Pedofilia*
- *Ley 20584: Derechos y Deberes que tienen las Personas en relación con acciones vinculadas a su atención de Salud.*
- *Ley 19880: Base y Procedimientos Administrativos, se refiere a acceso de la información personal y privacidad.*
- *DS 77/2004: Aprueba Norma Técnica sobre eficiencia de la comunicaciones electrónicas entre Órganos de la Administración del Estado y entre estos y los ciudadanos.*
- *DS 81/2004: Establece las características mínimas obligatorias de interoperabilidad que deben cumplir los Documentos Electrónicos en su generación, envío, recepción, procesamiento y almacenamiento.*
- *DS 83/2004: Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad del Documento Electrónico.*
- *DS 93: Aprueba Norma Técnica para minimizar la recepción de mensajes electrónicos no deseados en las casillas electrónicas de los Órganos de la Administración del Estado y sus funcionarios.*

- *DS 100/2006: Fija características mínimas obligatorias que deben cumplir los sitios Web de los Órganos de la Administración del Estado.*

- *Decreto 26/2004: Reglamento sobre el Secreto o Reserva de los Actos y Documentos de la Administración del Estado.*

- *Norma Chilena de Seguridad NCH-ISO 27001. Of2009.*

- *Resolución Exenta 781/2014 (MINSAL) - Aprueba Política General de Seguridad de la Información.*

- *Resolución Exenta 1124/2014 (MINSAL) - Aprueba Procedimientos del PMG Sistema de Seguridad de la Información.*

6. Principios de la Seguridad de la Información

Para el logro de los objetivos de la Seguridad de la Información, es fundamental garantizar los siguientes principios, como elementos estructurales de la Seguridad de la Información:

- ***Integridad:*** es la propiedad de salvaguardar la exactitud y completitud de los activos.

- ***Confidencialidad:*** Es la propiedad que determina que la información no esté disponible, ni sea relevada a individuos, entidades o procesos no debidamente autorizados.

- ***Disponibilidad:*** Es la propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- ***Mejora Continua:*** Herramienta de incremento de la productividad y/o eficiencia, que favorece un crecimiento estable y consistente en todos los segmentos de un proceso.

Estos principios base serán complementados por los siguientes principios institucionales:

- La información que posee el SSMSO tiene un valor muy importante para nuestra institución, es nuestra prioridad protegerla.

- La información referente a las personas y ciudadanos que trate el SSMSO pertenece a ellos y no a la Administración conforme a la normativa en protección de datos de carácter personal y de la protección de la vida privada.

- La Información debe estar protegida contra accesos no autorizados y alteraciones, manteniéndola confidencial e integra en todo momento.

- La Información debe estar disponible, garantizando su acceso autorizado, siempre que sea necesario.

- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información del SSMSO deben protegerla, por lo que deben estar informadas con respecto a sus privilegios, niveles de acceso y concientizadas que el activo de información es uno de los pilares de nuestra institución.

- La Seguridad de la Información no es algo inalterable, esta debe ser revisada y mejorada constantemente, como un proceso continuo de mejora.

- Se debe garantizar que estén debidamente protegidos y disponibles, todos aquellos activos de la información (infraestructura, sistemas de comunicaciones, sistemas informáticos, soportes, etc.) donde la información del SSMSO se encuentre almacenada, transportada o procesada.

- El tratamiento de los datos de carácter personal debe estar siempre en conformidad con las leyes aplicables en cada momento, considerando especialmente importante la *Ley 19628*.

- Las medidas de seguridad que se implanten deben ser proporcionales a la criticidad de la información que protejan, así como, a los daños o perdidas que se pueden producir en ella. Para estos efectos se seguirán como referencia las medidas de seguridad impuestas por el *DS 83/2004*.

7. Responsabilidad de la Política de Seguridad

La *Resolución Exenta N°3214/2014* (SSMSO) crea el ***Comité de Seguridad de la información*** como responsable de la implementación de la Política de Seguridad del SSMSO, así como de la aplicación de las Políticas y Procedimientos internos, que permitan resguardar la Seguridad de la Información del Servicio.

8. Organización de la Seguridad de la Información

Se debe conformar un equipo de trabajo ejecutivo para gestionar, evaluar y resolver sobre las materias relativas a la Seguridad de la Información.

Este tendrá la denominación de **"Comité de Seguridad de la Información"**.

8.1. Comité de Seguridad de la Información

Para la gestión de la Seguridad de las Información, se crea el *Comité de Seguridad de la Información*, dentro del ámbito de la presente Política, constituido por un equipo multidisciplinario que tiene por objetivo coordinar las actividades y controles de seguridad establecidos en el SSMSO.

Este comité velara por el fiel cumplimiento de las normativas vigentes, ya sean internas y/o externas, concerniente a materias de seguridad.

Este comité podrá estar incorporado en algún otro comité que tenga el mismo nivel de resolución.

Sesionará de acuerdo a las citaciones que realice el Encargado de la Seguridad de la Información Institucional, sin perjuicio de lo anterior, el Comité de seguridad de la información sesionará al menos 2 veces al año.

Sera Presidido por el Director(a) del SSMSO o quien lo subrogue.

El secretario será el Encargado de Seguridad de la Información Institucional, quien deberá generar un acta de acuerdos y compromisos de cada una de las sesiones de este Comité.

En los casos de empate en votación o de desacuerdo de los participantes respecto de decisiones relacionadas con seguridad de la información, dirimirá el Director(a) del SSMSO o quien los Subrogue.

8.2. Funciones del Comité de Seguridad

Las funciones relativas a este Comité de Seguridad de la Información, incluyen las siguientes acciones:

- Supervisar la programación del trabajo y los plazos para el cumplimiento de los objetivos de seguridad.
- Supervisar que se logran los objetivos con la documentación y evidencia que se requiera.

- Aprobar la Política de Seguridad, establecer los criterios de revision de la misma, revisarla, distribuirla y velar por su cumplimiento.

- Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la política de seguridad en todo el SSMSO.

- Establecer los requisitos de seguridad que se deben cumplir a nivel organizativo, técnicos u de control de los sistemas y servicios, de su disponibilidad y otros que permitan alcanzar los objetivos de seguridad identificados

- Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

- Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información.

- Valorar el grado de conformidad de los procedimientos implantados por el SSMSO con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su total confirmación.

- Aprobar los procedimientos que se definan para dar cumplimiento a las normas y políticas individuales derivadas de la política de seguridad.

- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información

- Verificar que todas las acciones llevadas a cabo en materia de seguridad sean compatibles o se encuentren respaldadas por la política de seguridad.

- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las administraciones en materia de seguridad.

- Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la integridad.

- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades de cada área.

- Respaldar los planes estratégicos en materia de seguridad definidos por el SSMSO.

- Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad del SSMSO, priorizando las actuaciones en materia de seguridad, cuando los recursos sean limitados.

- Aspectos de Seguridad de la Información que el SSMSO determine.

8.3. Composición del Comité de Seguridad

Los miembros que componen el Comité de Seguridad son los funcionarios serán:

COMITÉ DE SEGURIDAD DE LA INFORMACION SSMSO
Director SSMSO
Subdirector Administrativo del SSMSO
Subdirector de RRHH del SSMSO
Asesor Jurídico del SSMSO
Jefe Departamento de Informatica SSMSO
Encargado de Seguridad de la Información SSMSO

8.4. Roles, funciones y responsabilidades en materia de seguridad

8.4.1. Director del Servicio

La seguridad de la información es responsabilidad del Director del Servicio, quien en su calidad de máxima autoridad, delegara en los niveles pertinentes de la institución los roles, funciones y responsabilidades necesarias para la implementación, ejecución mantención, mejora continua y difusión del Sistema de Seguridad de la Información.

Las funciones del Director de Servicio en relación a la Estructura de la seguridad de la información serán:

- Generar lineamientos y criterios generales para la seguridad de la información.
- Aprobar las políticas institucionales relacionadas.
- Aprobar, mantener y promover la organización de seguridad de la información al interior del SSMSO.
- Evaluar el funcionamiento y efectividad del Sistema de Seguridad de la Información.
- Asignar los recursos, según las necesidades para el Sistema de Seguridad de la Información.
- Aprobar el plan de acción de mitigación de riesgos de seguridad de la información.

8.4.2. Encargado de Seguridad de la Información

Este funcionario asume la responsabilidad de mantener con el mayor grado de seguridad, a los servicios y sistemas del SSMSO,
Atendiendo los principios básicos:

- **Integridad**: la información asociada a los servicios del SSMSO no debe ser alterada personas no autorizadas.
- **Confidencialidad**: La información del SSMSO solo debe ser conocida por las personas autorizadas para ello.
- **Disponibilidad**: garantizar que los usuarios autorizados accedan a la información y a los recursos, cada vez que lo requieran.

Sus funciones generales son:

- Elaborar y supervisar el cumplimiento de la presente política, y de sus normas, políticas internas y procedimientos derivados.
- Asesorar en materia de seguridad de la información a los funcionarios del SSMSO que lo requieran.

- Coordinar la interacción con otros organismos especializados y unidades administrativas en caso que se incurra en violaciones de la presente política.

- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.

- Establecer las medidas de seguridad adecuada y eficaz para cumplir los requisitos de seguridad establecidas por el SSMSO y la normativa vigente.

- Promover la formación y concienciación en materia de la información dentro de su ámbito de responsabilidad.

- Preparar los temas a tratar en las reuniones de comité de seguridad, aportando información puntual para la toma de decisiones.

- Diseñar la arquitectura y medidas de seguridad, la implantación de herramientas y técnicas, su grado de cumplimiento y ajuste a la presente Política.

- Asegurar el nombramiento de responsables por cada área involucrada, a través del acto administrativo que corresponda, en los procesos que se detallan:

Proceso	Responsable
Gestión de Activos	1 Responsable por cada área SSMSO 1 Responsable de Ingeniería de Sistemas y Redes 1 Responsable de Desarrollo de Software 1 Responsable de Administración de Bases de datos 1 Responsable de Gestión Administrativa
Seguridad Recursos Humanos	1 Responsable de Gestión de las Personas
Seguridad Física y ambiental	1 Responsable de la Unidad de Higiene y Seguridad
Gestión de las Comunicaciones y Operaciones	1 Responsable de Unidad de Comunicaciones
Control de Accesos	1 Responsable de Ingeniería de Sistemas
Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	1 Responsable de Desarrollo de Software
Gestión de Incidentes de	Encargado(a) de Seguridad de la

Seguridad de la información	Información
Gestión de la Continuidad del Negocio	1 Responsable por cada Área del SSMSO 1 Responsable de Ingeniería de Sistemas y Redes 1 Responsable de Desarrollo de Software 1 Responsable de Administración de Bases de datos 1 Responsable de Gestión Administrativa
Cumplimiento	1 representante de la División Jurídica

Las funciones a desempeñar por este equipo de trabajo y que serán coordinadas por el Encargado de Seguridad son:

- Coordinar el levantamiento, análisis y documentación de los procesos y activos de información con los responsables de área.
- Desarrollar, implementar, ejecutar, mantener y mejorar en forma continua el sistema de seguridad de la información, además proponer la difusión del mismo.
- Establecer los controles que aseguren el cumplimiento de los procedimientos, normas, instructivos u otros que regulen la seguridad de la información, definiendo los responsables de su ejecución en conjunto con los responsables de área.
- Realizar seguimiento y análisis de los incidentes de seguridad su tratamiento, proponiendo las acciones pertinentes para mitigar estos.
- Coordinar el levantamiento, análisis y actualización continua de la matriz de riesgos de seguridad de la información en conjunto con los responsables de área.
- Elaborar y proponer el plan de acción en conjunto con los responsables de área.
- Gestionar la ejecución del plan de acción aprobado en conjunto con los responsables de área.

Para aquellos sistemas de información que por su complejidad, distribucion, separación física de sus elementos o volumen de usuarios, se necesitara de personal adicional para llevar a cabo las funciones de encargado dela seguridad de la información.

El encargado de seguridad podrá designar cuantos encargados de seguridad delegados considere necesarios.

Estos se harán cargo de su ámbito de todas aquellas acciones que delegue el Encargado de seguridad de la información teniendo dependencia funcional directa de él.

8.4.3. Propietario de la Información

Jefatura o encargado de unidad organizacional, responsable de la protección y uso de la información. El propietario de la información es el responsable de su clasificación, así como, de su mantenimiento y actualización.

8.4.4. Usuario de la Información

Conjunto de personas internas y/o externas que, con la debida autorización del propietario de la información, tiene acceso a consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos u otros medios de almacenamiento.

Los usuarios solo deben contar con acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitaran su capacidad en los entornos informáticos de forma que no puedan realizar actividades diferentes a las autorizadas.

Las principales responsabilidades de los usuarios de la información son:

- Utilizar información solo para el propósito para el que se recibió autorización de uso.
- Conocer las políticas y procedimientos de Seguridad de la información que se han institucionalizado.
- Cumplir con los controles establecidos en las políticas y procedimientos establecidos en el SGSI.
- Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.
- Comunicar los incidentes relaticos a la seguridad de la información.

9. Revisión de la política

La presenta política será revisada y actualizada, se der pertinente, en forma anual, a fin de procurar su mantención en el tiempo y mejora continua, en esta