MINISTERIO DE SALUD
DIVISIÓN JURÍDICA
JAA/ETS/CCHA/JHG/LDA

APRUEBA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARÍA DE SALUD PÚBLICA Y LA SUBSECRETARÍA DE REDES ASISTENCIALES Y DEJA SIN EFECTO RESOLUCIONES QUE INDICA.

EXENTA Nº 889 /

SANTIAGO, 26 NOV 2019

VISTOS: Lo dispuesto en la ley N° 19.880 que establece Bases de los Procedimientos Administrativos; en el decreto con fuerza de ley N°1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del decreto ley N° 2763, de 1979 y las leyes N° 18.933 y N°18.469; en el decreto supremo N° 136, de 2004, del Ministerio de Salud, que aprueba Reglamento Organico del Ministerio de Salud; la ley 20.285 de acceso a la información Pública; en la ley N° 19.799 sobre documentos electronicos, forma electronica y servicios de certificación de dicha firma; en el decreto supremo N° 83, de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en la ley N° 19.233 sobre delitos informaticos; en la Norma Chilena NCh-ISO 27001: 2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos; memorándum A/22 Nº 270, del Departamento de Tecnología de la Información y las Comunicaciones del Ministerio Salud, de fecha 06 de noviembre de 2019, y la resolución Núm. 7.- Santiago, 26 de marzo de 2019, de la Contraloría General de la República sobre exención de la toma de razón;

CONSIDERANDO:

1° Que, las nuevas tecnologías de la información y de las comunicaciones (TIC) se han incorporado de manera masiva en los procesos institucionales y al quehacer personal de los funcionarios que ejercen sus labores en el Ministerio de Salud.

2º Que conforme lo previsto en la ley 19.880 los procedimientos administrativos podrán constar en expedientes físicos o eletcrónicos, lo que llevará a que su tramitación pueda desarrollarse a través de medios computacionales.

3º Que, por Decreto Supremo Nº 83 del Ministerio Secretaría de la Presidencia, de 2005 se estableció la norma técnica sobre seguridad y confidencialidad sw los documentos electrónicos.

4º Que la gestión de la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental vigente, el cual requiere actualizar las políticas de seguridad de acuerdo a las metodologías y estándares técnicos que permitan lograr niveles de integridad, confidencialidad y disponibilidad, con todos sus activos de información relevantes para la institución.

5° Que, existe la necesidad de actualizar la Política de Seguridad de la Información del Nivel Central y la del Comité de Seguridad de la Información Minsal, aprobado por Resolución Exenta N° 783 de 2014, modificada por Res. Exenta Nº 15 de 07 de enero de 2016 ajustándola a las necesidades de la actualización de la normativa Nacional en Seguridad de la Información.

6° Que, en mérito de lo expuesto, dicto la siguiente:

RESOLUCIÓN:

1º APRUÉBASE la Política de Seguridad de la Información del Nivel Central, para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales, cuyo texto es el siguiente:

PS-NC-005

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARÍA DE SALUD PÚBLICA Y LA SUBSECRETARÍA DE REDES ASISTENCIALES

Versión Oficial Actual v03 – Octubre del 2019

	Responsable	Fecha
Elaborado	Rodrigo Vidal – Departamento TIC	Octubre 2019
Revisado	Rodrigo Vidal – Departamento TIC José Villa- Departamento TIC	Octubre 2019
Aprobado	Gabriel Reveco – Presidente Comité de Seguridad de la Información	Octubre 2019

CONTENIDO

1. PROPÓSITO

Esta Política General de Gestión de Seguridad de la Información, tiene como propósito establecer los lineamientos para la gestión de la Seguridad de la Información, en el Nivel Central del Ministerio de Salud.

2. ALCANCE O ÁMBITO DE APLICACIÓN

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

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 corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información (Nch-ISO 27001:2013)		
Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Políticas de seguridad de la información	A.05.01.01	Políticas para la seguridad de la información
	A.05.01.02	Revisión de las políticas de seguridad de la información
Organización de la seguridad de la información	A.06.01.01	Roles y responsabilidades de la seguridad de la información
Cumplimiento	A.18.02.01	Revisión independiente de la seguridad de la información

3. MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Documentos del Sistema de Gestión de Seguridad de la Información (SGSI) de MINSAL, disponibles en isalud.minsal.cl.
- Política Nacional de Ciberseguridad (PNCS)
- El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
  - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad.
  - Leyes relacionadas.

- Políticas de Seguridad de la Información de Minsal, disponibles en isalud.minsal.cl.

4. ROLES Y RESPONSABILIDADES

- **Comité de Seguridad de la Información (CSI) del Nivel Central**
  - Proponer a los Subsecretarios de Salud Pública y de Redes Asistenciales las políticas, procedimientos e instrucciones de seguridad de la información y su actualización.
  - Supervisar la implementación de la estructura documental del Sistema de Seguridad de la Información aplicable en las Subsecretarías de Salud Pública y de Redes Asistenciales.
  - Proponer a los Subsecretarios de Salud Pública y de Redes Asistenciales estrategias o soluciones específicas para implementar o controlar los componentes de la estructura documental del Sistema de Seguridad de la Información.
  - Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones sobre ello.
  - Revisar y monitorear los incidentes de seguridad de la información a fin de establecer acciones preventivas y correctivas.
  - Coordinarse con los Comités de Calidad y de Riesgos de la Institución, para mantener estrategias comunes de gestión.
  - Apoyar a las Subsecretarías de Salud Pública o de Redes Asistenciales, según corresponda, en la implementación de los controles comprometidos con la Dirección de Presupuestos, a través del Programa de Mejoramiento de la Gestión de cada año, de acuerdo al indicador transversal definido para la Seguridad de la Información.
  - Revisar los elementos del Sistema de Seguridad de la Información y proponer mejoras a través del Encargado de Seguridad.
  - Difundir los componentes de la estructura documental del Sistema de Seguridad de la Información a través de la Intranet y los medios de comunicación establecidos dentro del Ministerio de Salud.
  - Monitorear cambios significativos que pudieran variar los riesgos presentes en la Institución.
  - Establecer acciones y proponer iniciativas para mejorar la seguridad de la información en las Subsecretarías de Salud Pública y de Redes Asistenciales.
  - Supervisar la realización de auditorías de Seguridad de la Información, internas o externas.

- **Encargados Seguridad de la Información del Nivel Central (SSP-SRA)**
  - Actuar como Asesor en materias relativas a seguridad de la información para la Subsecretaría de Salud Pública y de la Subsecretaría de Redes Asistenciales.

- Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la organización y el control de su implementación, velando por su 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.
- Gestionar la respuesta y priorización del tratamiento de incidentes identificados y/o reportados, que estén vinculados a los activos de información en la Institución.
- Definir las vías de comunicación que se requieran para apoyar en la resolución del incidente de seguridad al interior de la Institución. Sean estas a través del escalamiento al Comité de Seguridad de la Información, Jefes de División y/o Jefes de Gabinete de ambas Subsecretarías según se requiera.
- Organizar las actividades del Comité de Seguridad de la Información.
- Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos.
- Coordinar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de seguridad.
- Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que el permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
- Resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que se puedan tener acceso a los activos de información del Ministerio de Salud, acerca de las Políticas de Seguridad de la Información vigentes en el Ministerio, y en particular sobre las obligaciones que les correspondan en reación a la gestión de incidentes de seguridad.

- **Encargado de Ciberseguridad del Nivel Central**

- Velar por el cumplimiento del Instructivo Gabinete Presidencial N°8 del 23 de octubre de 2018 del Ministerio del Interior.
- Actuar como contraparte frente al Ministerio del Interior en materias relativas a Ciberseguridad de la información para el nivel central del Ministerio de Salud.
- Alinear los esfuerzos de las distintas áreas de la institución, respecto a la protección de los sistemas tecnológicos y a la información contenida en ellos, según los criterios de Ciberseguridad.
- Gestionar internamente el tratamiento de incidentes que estén vinculados a los activos de información en la Institución, identificados y/o reportados tanto por el Ministerio del Interior como por instancias internas, efectuando la reportabilidad y el seguimiento adecuado a dichos eventos.
- Apoyar el proceso de Sensibilización en Materias de Ciberseguridad al Interior de la Institución.

- Presidir el comité que tendrá a su cargo la actualización de políticas de Ciberseguridad y Seguridad de la Información al interior de la organización.
- Coordinar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de Ciberseguridad.
- Resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los activos de información del Ministerio de Salud, acerca de las Políticas de Ciberseguridad y Seguridad de la Información vigentes en el Ministerio, y en particular sobre las obligaciones que les correspondan en relación a la gestión de incidentes.

- **Usuarios finales.**
  - Se debe entender como usuarios finales a todos quienes tienen la responsabilidad de acatar las políticas y normativas definidas, independiente que además tengan otros rol nominado en este ámbito.
  - Debe considerar
    - A todos los funcionarios (planta, contrata, reemplazos y suplencia),
    - Personal a honorarios,
    - Terceros (proveedores, compra de servicios, tratamiento por encargo, 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. MATERIAS QUE ABORDA

- Políticas para la seguridad de la información.
- Revisión de las políticas de seguridad de la información.
- Roles y responsabilidades de la seguridad de la información.
- Revisión independiente de la seguridad de la información.

6. DIRECTRICES DE LA POLITICA

6.1 Declaración Institucional

El Ministerio de Salud (MINSAL) 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 la propia institución determine. Para estos efectos, el Minsal 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.

Para la gestión de la Seguridad de la Información al Interior del MINSAL se ha decidido contar con un programa de implantación del tipo "Sistema de Gestión de Seguridad de la Información" (SGSI), basado en los requisitos de la Norma NCh-ISO27001:2013, y las prácticas para los controles de seguridad de la Norma NCh-ISO27002:2013, con el objetivo 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 confidencial, privada y sensible 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 la información de los ciudadanos, 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. Este principio deberá aplicarse en concordancia con lo previsto en la ley 20.285 de acceso a la información pública.

- **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 institucional. 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.
  Tratándose de la información sujeta a las normas de transparencia, la disponibilidad impone que se encuentren en el portal de transparencia activa y que permita responder oportunamente los requerimientos efectuados por los ciudadanos en virtud de su derecho de acceso a la información pública.
  Según lo expuesto anteriormente, las Autoridades del Ministerio de Salud se comprometen a:

- Apoyar los objetivos y principios de la seguridad de la información, y a proveer los recursos necesarios para la gestión de actividades en seguridad.

- Promover un plan de acción de mejora continua con el fin de asegurar una adecuada gestión de la seguridad de la información, según lo dispuesto en la NCh-ISO 27001:2013 y otras normativas vigentes que, conforme a lo dispuesto en el número 7 de esta política general, estarán disponibles permanentemente en el sitio intranet de MINSAL[1].

- Implementar las obligaciones que emanan del Derecho de Acceso a la Información pública, con el debido respeto a la protección de los datos sensibles e información confidencial, de acuerdo a la ley.

6.2 Objetivos de la Gestión de Seguridad de la Información en el Ministerio de Salud

6.2.1 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.

6.2.2 Objetivos Específicos

- Identificar y catastrar todos los activos de información relevantes que están presentes directa o indirectamente en cada proceso institucional, abarcando tanto los procesos críticos institucionales, 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 la operación del negocio y reducir el impacto de los daños a las instalaciones, medios de almacenamiento, equipos de procesamiento y de comunicación.

[1] http://isalud.minsal.cl/

- Hacer uso de planes de continuidad operacional ante hechos contingentes que interrumpan la operación del servicio.
- Sensibilizar y capacitar a los funcionarios del MINSAL acerca de su responsabilidad para mantener la seguridad de la información y su adecuado uso, estableciendo una cultura organizacional que incorpore el tema de seguridad de la información como un aspecto relevante en los procesos de negocio del Ministerio.

6.3 Gestión de la Política y otros documentos del sistema de Gestión de Seguridad de la información

La estructura documental de ese sistema está compuesta por una Política General de Seguridad de la Información, políticas específicas de seguridad de la información, procedimientos de operación, instructivos y registros.
La referida estructura documental aplicable a las Subsecretarías de Salud Pública y de Redes Asistenciales deberá ser aprobada por los respectivos Subsecretarios y será revisada (a lo menos cada dos años) por el Encargado de Seguridad del Nivel Central y el Comité de Seguridad del Nivel Central.

La documentación aplicable a las Subsecretarías de Salud Pública y de Redes Asistenciales debe asegurar:

- Integren el modelo de seguridad con las metodologías y políticas existentes para ambas Subsecretarias.
- Que se cumplan las normas legales y reglamentarias referidas a seguridad, tanto para la información, como para los medios que la contienen.
- Que la información cumpla con los niveles de autorización y responsabilidad correspondientes para su utilización, divulgación, administración, seguimiento y custodia.
- Que la información, sus medios de procesamiento, conservación y transmisión estén protegidos del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotajes, espionaje, violación de la privacidad y otras acciones que pudieran perjudicarla.
- Que los medios de procesamiento, conservación y comunicación de la información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.
- Que los derechos de propiedad sobre la información y sistemas estén establecidos.
- Que las comunicaciones internas y externas cuenten con mecanismos que protejan la integridad, disponibilidad y confidencialidad en la transmisión de información.

- Que se delimiten los ámbitos físicos de acción de las políticas de seguridad, dependiendo de los distintos niveles de riesgo que presentan los medios de procesamiento, conservación y comunicación.
- Que el acceso a los servicios de ambas Subsecretarías, ya sea por medios internos o externos, se realice de acuerdo con las atribuciones de las personas o entidades que las utilicen.
- Que las actividades y uso de recursos críticos, relacionados con productos y servicios, sean monitoreados y su información sea conocida en forma oportuna por los niveles correspondientes.

Las versiones vigentes de la normativa del SGSI y los documentos de apoyo, serán publicados en el sitio intranet de MINSAL (http://isalud.minsal.cl), además de otros sitios o lugares de fácil acceso a los funcionarios.

6.4 Identificación de riesgos

A lo menos cada dos años el Comité de Seguridad de la Información Nivel Central, debe gestionar la actualización de los riesgos de seguridad de la información del Nivel Central, que debe ser construido a partir del análisis de las amenazas y vulnerabilidades a los que se encuentran expuestos los activos de la información relevantes. La metodología de análisis y gestión de riesgos debe estar enfocada en los procesos de provisión institucional, sus actividades, actores y activos, siendo referente:

- CAIGG, apartado Líneas de Acción / Gestión de Riesgos, en el sitio web http://www.auditoriainternadegobierno.cl/.
- Norma NCh-ISO 31000:2012 – Principios y directrices para la Gestión de Riesgos.
- Marco COSO ERM – www.coso.org.
- DIPRES, Guía Metodológica Sistema de Seguridad de la Información.

En el caso de los riesgos residuales, deben ser relevados por el Comité de Seguridad de la Información Nivel Central, al Comité de Riesgos de la Institución para su análisis.

6.5 Revisión y medición

A lo menos una vez al año, el Comité de Seguridad de la Información MINSAL debe evaluar el estado del SGSI e informar a los Subsecretarios de Salud Pública y Redes Asistenciales los resultados, considerando cambios que surjan en el transcurso de este período que podrían afectar el enfoque de la organización a la gestión de la seguridad de la información, incluyendo cambios al ambiente de la organización, circunstancias del negocio, 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 ante amenazas y vulnerabilidades.
- Información relacionada a incidentes de seguridad.
- Recomendaciones provistas por autoridades relevantes.
- Medición de los indicadores del Sistema.

Revisión independiente de la seguridad de la información: a lo menos cada dos años se deberá revisar la Política General de Seguridad de la Información, y el estado del SGSI en el Nivel Central mediante auditorías internas o externas.

6.6 CUMPLIMIENTO

Todos los usuarios del Ministerio de Salud ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deberán dar complimiento, en lo que les corresponda, a esta Política General de Seguridad de la Información, las políticas específicas y los procedimientos relacionados que se aprueben al efecto.

Para el caso de terceros y por el solo hecho de participar en algún proceso de compras del servicio, el oferente deberá dar cumplimiento a las Políticas y Procedimientos vigentes de seguridad de la información del Ministerio de Salud, publicadas en el link http://web.minsal.cl/seguridad_de_la_informacion, y sus correspondientes modificaciones, las cuales se presumen conocidas por el contratista o adjudicatario, para todos los efectos legales. Será de responsabilidad del Contratista darlas a conocer y resguardar su cumplimiento por sus empleados y colaboradores internos o externos.

6.7 SANCIONES

El incumplimiento de las obligaciones emanadas de esta Política, de las Políticas específicas del Sistema, 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 MINSAL. 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.

7. MECANISMO DE DIFUSIÓN

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

8. PERÍODO DE REVISIÓN

La revisión del contenido de esta Política se efectuará a lo menos cada dos años por el Comité de Seguridad de la Información, o atendiendo necesidades de cambios para garantizar su idoneidad, adecuación y efectividad.

9. EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos especiales, el Comité de Seguridad de la Información evaluará y podrá establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.

10. HISTORIAL Y CONTROL DE VERSIONES

Versión	Página o Sección Modificada	Fecha de Aprobación	Motivo del cambio
1	Creación del documento	Octubre 2011	Creación del documento
2	Todo el documento	Septiembre 2017	Ampliación del alcance de la política para el Sector Salud
3	Todo el documento	Octubre 2019	Modificación alcance de la política, definiéndolo para las Subsecretarías de Salud Pública y de Redes Asistenciales.

2º **ESTABLÉZCASE** la obligación del Departamento de recursos Humanos de la Subsecretaría de Salud Pública, de difundir la política fijada en este instrumento y al Departamento de Tecnologías de la Información y las Comunicaciones, de velar por su estricto cumplimiento.

3º **INSTRÚYASE** al Jefe de Departamento de Tecnologías de la Información y a los Encargados de Seguridad de la

Información, que realicen las acciones tendientes a la implementación de la presente Política dentro del ámbito de sus competencias.

4º DIFÚNDASE La presente Resolución, a todos los funcionarios de la Subsecretaría de Redes Asistenciales y la Subsecretaría de Salud Pública, a lo menos mediante los siguientes canales:

- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

5º DEJESE SIN EFECTO las siguientes resoluciones: Resolución Exenta Nº 781, de 14 de octubre de 2014, Resolución Exenta Nº 783 de 14 de octubre de 2014, Resolución Exenta Nº 15, de 07 de enero de 2016, y Resoluciòn Exenta Nº 1330 de 14 de noviembre de 2016, todas conjuntas de la Subsecretaría de Salud Pública y de la Subsecretaría de Redes Asistenciales,

ANÓTESE Y COMUNÍQUESE

REPUBLICA DE CHILE SUBSECRETARIA DE SALUD PUBLICA MINISTERIO DE SALUD

DRA. PAULA DAZA NARBONA
SUBSECRETARIA DE SALUD PÚBLICA

REPUBLICA DE CHILE SUBSECRETARIO DE REDES ASISTENCIALES MINISTERIO DE SALUD

ARTURO ZÚÑIGA JORY
SUBSECRETARIO DE REDES ASISTENCIALES