



PS-NC-011

POLÍTICA PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v03 – Junio 2020

	Responsable	Fecha	Firma
Elaborado	Rodrigo Vidal / Unidad Seguridad TIC	Junio 2020	
Revisado	José Villa / Área Seguridad de la Información (Representante Comité de Seguridad) Lorena Donoso / Abogado División Jurídica	Junio 2020	
Aprobado	Gabriel Reveco / Encargado Ciberseguridad (Presidente Comité de Seguridad de la Información)	Junio 2020	

POLÍTICA PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-011	Versión: 03.00
		Página 2 de 8	

Contenido

1	PROPOSITO	3
2	ALCANCE O AMBITO DE APLICACIÓN	3
3	DEFINICIONES	3
4	MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS	4
5	ROLES Y RESPONSABILIDADES	5
6	MATERIAS QUE ABORDA.....	6
7	DIRECTRICES DE LA POLÍTICA	6
7.1	Directrices Generales.....	6
7.2	Políticas de sistemas de tratamiento de datos	6
7.3	En el ejercicio de sus funciones	7
8	MECANISMO DE DIFUSIÓN.....	7
9	PERÍODO DE REVISIÓN.	8
10	EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA	8
11	HISTORIAL Y CONTROL DE VERSIONES.....	8

POLÍTICA PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-011	Versión: 03.00
			Página 3 de 8

1 PROPOSITO

El propósito de esta política es definir las directrices para la protección y privacidad de la información personal que se recoja, almacene procese y transmita, y en general se haga tratamiento de esta, en el Ministerio de Salud.

2 ALCANCE O AMBITO DE APLICACIÓN

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 la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales.

Sin perjuicio de lo anterior las obligaciones legales respecto a la confidencialidad de datos, de las personas que trabajan en su tratamiento o acceden a ellos de cualquier forma, no cesan por haber terminado sus actividades en el respectivo organismo.

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
Administración de activos	A.08.01.03	Uso aceptable de los activos
Cumplimiento	A.18.01.04	Privacidad y protección de la información de identificación personal

3 DEFINICIONES

Datos Personales: Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, con independencia de su soporte.

Datos Sensibles: Datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Tratamiento de datos: Cualquier operación o complejo de operaciones o procedimientos técnicos de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar,

POLÍTICA PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-011	Versión: 03.00
			Página 4 de 8

interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

4 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- **Marco Normativo**
 - NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
 - 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
- **Documentos Relacionados**
 - Documento del Sistema de Gestión de Seguridad de la Información, disponibles en isalud.minsal.cl.
- **Leyes o Decretos**
 - Ley 19.650, que perfecciona las normas del área de la salud.
 - Ley N° 19.966, que Establece un Régimen de Garantías Explícitas en Salud. La Ley N°19.966 fue promulgada el 25 de agosto de 2004 y publicada el 03 de septiembre de 2004.
 - Ley N° 19.628, de 1999, Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada.
 - Ley N° 20.285, de 2008, Ministerio Secretaría General de la Presidencia, sobre acceso a la información pública.
 - Ley N° 20.584, de 2012, Ministerio de Salud, Subsecretaría de Salud Pública, regula derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud.
 - Ley N° 20.120, de 2006, Ministerio de Salud, Subsecretaría de Salud Pública, sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana.
 - Ley N° 20.724, de 2014, Ministerio de Salud, modifica el código sanitario en materia de regulación de farmacias y medicamentos.
 - D.F.L. N°29, de 2005, Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre estatuto Administrativo.
 - Decreto con Fuerza de Ley N° 1/19653, Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado.

POLÍTICA PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-011	Versión: 03.00
			Página 5 de 8

5 ROLES Y RESPONSABILIDADES

- **Funcionarios, personal a honorarios y terceros**
 - Utilizar la información solamente, dentro del ámbito de sus competencias y para el uso específico o finalidad para la cual se ha recolectado y a no comunicar, diseminar o de alguna otra forma, ceder a terceros no autorizados, salvo autorización previa y escrita del responsable del Activo de que se trate o del titular de los datos cuando corresponda.
 - Las personas que trabajan en el tratamiento de datos personales están obligadas a guardar secreto sobre los mismos, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo o por haber terminado el vínculo con Misal que le habilitó para acceder a dichos datos.
 - Los datos deberán ser tratados con debida diligencia, sujetándose a las instrucciones que le imparta el respectivo Subsecretario, en su calidad de responsable del registro o banco de datos.
 - Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.
 - Los datos personales deberán ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.
- **División Administración y Finanzas**
 - Incluir en los contratos de terceros las cláusulas de confidencialidad y resguardo de la información según lo establecido en el procedimiento acuerdos de confidencialidad en contratos con terceros.
- **Departamento de Recursos Humanos**
 - Incluir en los contratos de honorarios las cláusulas de confidencialidad y resguardo de la información.
- **División Jurídica**
 - Identificar y difundir las normativas que obligan a la protección de los datos y privacidad de la información personal y velar por su estricto cumplimiento.

POLÍTICA PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-011	Versión: 03.00
			Página 6 de 8

6 MATERIAS QUE ABORDA.

- Uso aceptable de los activos
- Privacidad y protección de la información de identificación personal

7 DIRECTRICES DE LA POLÍTICA

7.1 Directrices Generales

Todos los funcionarios, personal a honorarios y terceros deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones, según lo establecido en la presente Política y el Sistema de Gestión de Seguridad de la Información del Minsal, la normativa general de salud, la ley 19.628 y los documentos relacionados.

Sin perjuicio de lo anterior, los funcionarios, personal a honorarios y terceros, que trabajan en el tratamiento de los datos personales o sensibles estarán obligados a guardar secreto sobre el mismo, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como, asimismo, sobre los demás actos y antecedentes relacionados con ley 19.628 artículo 7°, sobre Protección a la Vida Privada.

Por lo tanto, los datos personales o sensibles, indistintamente del medio en que estén contenidos, deberán ser protegidos y resguardados adecuadamente por quienes tienen el deber de manipularlos, garantizando razonablemente su privacidad a través de la implementación de procedimientos y controles para su tratamiento.

7.2 Políticas de sistemas de tratamiento de datos

Todo sistema o aplicación en que se traten datos personales deberá ser diseñado y desarrollado de manera tal que se de cumplimiento a las obligaciones de reserva o secreto, de acuerdo con la naturaleza de la información. De esta manera, los sistemas que tengan por objeto el tratamiento de datos sensibles deberán cumplir las reglas siguientes:

- Privacidad por defecto:** Los sistemas y aplicaciones, por defecto, guardarán la privacidad de los datos, debiendo requerirse una acción consciente y trazable para cambiar el modelo de acceso a los datos. En este ámbito, los sistemas y aplicaciones deberán incluir sistemas de resguardo de la privacidad tales como anonimización, seudonimización o encriptación de datos, de acuerdo con los requerimientos funcionales que se definan.
- Seguridad en el diseño:** Los sistemas y aplicaciones deberán ser desarrollados de forma tal que incluyan sistemas de verificación permanente de brechas de seguridad. Asimismo, los sistemas deberán estar diseñados

POLÍTICA PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-011	Versión: 03.00
			Página 7 de 8

para adoptar las medidas urgentes y necesarias para el resguardo de los datos personales en caso de un incidente de seguridad que pudiere afectarlos.

- c) **Responsabilidad demostrable:** Los sistemas y aplicaciones deberán permitir trazar las operaciones de tratamiento de datos personales que se realicen a través de los mismos de forma tal que sea posible verificar y demostrar aquellas operaciones realizadas.
- d) **Segregación datos y de funciones:** El diseño de los sistemas deberá considerar perfiles diferenciados por competencias, de forma tal que sólo puedan acceder a los datos personales los profesionales que se encuentren legalmente facultados para acceder a ellos.

7.3 En el ejercicio de sus funciones

La toma de conocimiento se realiza por tipo de contrato, según se indica a continuación:

- Funcionario (Planta, contrata, reemplazos y suplencia): según lo establecido en el D.F.L. N° 29, de 2005, Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre estatuto Administrativo, especialmente lo señalado en artículos 61, 84 y 85.
- Honorarios: a través de cláusula de confidencialidad en el contrato de honorarios
- Terceros: Cláusula de confidencialidad en los contratos y según lo establecido en el “Procedimiento acuerdos de confidencialidad en contratos con terceros” y las respectivas bases de las adquisiciones respectivas.

Mediante estos instrumentos los funcionarios, personal a honorarios y terceros se comprometerán a utilizar la información solamente para la finalidad legítima específica en que se basó que pudieran acceder a la información y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, sea natural o jurídica, salvo autorización previa y escrita del Responsable del Activo de que se trate conforme a las normas a que se hace referencia en la presente política.

8 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.
- Entrega de una copia, como anexo en las contrataciones realizadas por el Ministerio.

POLÍTICA PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-011	Versión: 03.00
			Página 8 de 8

9 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.

10 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos de 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.

11 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
01	Octubre 2014	Todas	Creación del documento
02	Octubre 2016	<ul style="list-style-type: none"> ✓ Alcance ✓ Difusión ✓ Revisión y Medición 	Actualización de la referencia normativa de la norma NCh-ISO 27001
03	Junio 2020	<ul style="list-style-type: none"> ✓ Alcance ✓ Roles y responsabilidades ✓ Excepciones al cumplimiento de la política 	Actualización del documento y normtavia