PS-NC-013

POLÍTICA SEGURIDAD EN LA GESTIÓN Y DESARROLLO DE PERSONAS

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v02 – Julio 2020

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

Contenido

1 PROPÓSITO

El propósito de esta política es asegurar que todas las personas de la institución dispongan de un documento formal sobre los derechos, deberes y responsabilidades en relación con la seguridad de la información, entregando énfasis en las eventuales sanciones ante un acto negligente que ponga en riesgo los activos de información de la institución.

2 ALCANCE O ÁMBITO DE APLICACIÓN

Es aplicable a todos los funcionarios y funcionarias (planta, contrata, reemplazos y suplencias), personal a honorarios suma alzada, códigos del trabajo y terceros (proveedores, compra de servicios, etc.), que presten servicios para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales (Nivel Central).

Sin perjuicio de lo anterior, las obligaciones legales respecto a la confidencialidad de datos, de las personas que trabajan 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
Seguridad ligada a los recursos humanos	A.7.1.1	Selección
	A.7.1.2	Términos y condiciones de la relación laboral
	A.7.2.2	Concientización, educación y formación en seguridad de la información
	A.7.2.3	Proceso disciplinario
	A.7.3.1	Responsabilidades en la desvinculación o cambio de empleo

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, 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 http://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 Nº 19.628, de 1999, Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada.
  - Ley Nº 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. Nº29, 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 Nº 1/19653, Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado.

5 ROLES Y RESPONSABILIDADES

- **Funcionarios y funcionarias (planta, contrata, reemplazos y suplencias), personal a honorarios suma alzada, códigos del trabajo y terceros**

  - Las personas que trabajen en la Subsecretaría de Salud Pública o Subsecretaría de Redes Asistenciales (Nivel Central), están obligadas a proporcionar datos personales fidedignos al Departamento de Gestión y Desarrollo de Personas, además deben mantenerlos actualizados durante el periodo que trabajen en la institución.

  - 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 la Subsecretaría de Salud Pública o Subsecretaría de Redes Asistenciales (Nivel Central), 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.

- **Departamento de Administración y Servicios**

  - Incluir en los contratos a terceros las cláusulas de confidencialidad y resguardo de la información según lo establecido en la presente política.
  - Recuperar los activos asignados de aquellas personas que terminan su relación laboral.

- **Departamento de Gestión y Desarrollo de Personas**

- Verificar los antecedentes de los(as) postulantes de acuerdo con las leyes, regulaciones y normas éticas relevantes.
- Incluir en los convenios de honorarios suma alzada y contratos de códigos del trabajo las cláusulas de confidencialidad y resguardo de la información.
- Entrega de material de inducción a todo nuevo ingreso de funcionario/a.
- Incluir dentro del programa anual de capacitación de la Subsecretaría de Salud Pública, curso o actividad sobre la Seguridad de la Información.

- **División Jurídica**

  - Identificar y difundir las normativas que obligan a la protección de los datos, privacidad de la información personal y seguridad de la Información, y velar por su estricto cumplimiento.

- **Encargado o Encargada de Seguridad de la Información**

  - Impulsar actividades de difusión de Seguridad de la Información, en conjunto con el Departamento de Gestión y Desarrollo de Personas y el Departamento de Comunicaciones y Relaciones Públicas.

6 MATERIAS QUE ABORDA.

- Selección
- Términos y condiciones de la relación laboral
- Concientización, educación y formación en seguridad de la información
- Proceso disciplinario
- Responsabilidades en la desvinculación o cambio de empleo

7 DIRECTRICES DE LA POLÍTICA

7.1 Verificación de antecedentes previo a la contratación

Todo ingreso de un nuevo funcionario o funcionaria, ya sea por contratación directa o proceso de reclutamiento y selección, debe ser canalizado sólo a través del Departamento de Gestión y Desarrollo de Personas.

En el Proceso de Reclutamiento y Selección, se verifica que el/la postulante cumpla con los requisitos de admisibilidad (requisitos legales) y requisitos del perfil del cargo requerido. Se revisan los documentos adjuntados por el o la postulante, quien tiene la responsabilidad de enviar documentos fidedignos, los cuales se resguardan junto con sus otros datos e información, entregados sólo a los y las implicadas en la ejecución del proceso.

La entrega de los documentos originales por parte del postulante y la revisión final de ellos, es realizada por la Unidad de Personal del Departamento de Gestión y Desarrollo de Personas durante el proceso de contratación.

Desde la seguridad de la información, se deben verificar los antecedentes de acuerdo con las leyes, regulaciones y normas éticas relevantes, de acuerdo con la información a la que él o la postulante tendrá acceso y los riesgos, donde sea aplicable y deben incluir a lo menos lo siguiente:

- Verificación (de integridad y precisión) del currículum vitae del postulante.
- Confirmación de los grados académicos que se indican.
- Verificación de la identidad.
- Verificación de antecedentes penales.

7.2 Términos y condiciones de la relación laboral

7.2.1 Cláusulas de seguridad

El Departamento de Gestión y Desarrollo de Personas, en conjunto con el Departamento Jurídico y el Encargado de Seguridad de la Información, deben establecer los aspectos de seguridad de la información que serán incluidos en todos los nombramientos de planta, contrata, reemplazos, suplencias, convenio de honorarios suma alzada y contratos código del trabajo.

El Departamento de Administración y Servicios en conjunto con el Departamento Jurídico y el Encargado de Seguridad de la Información, deben establecer los aspectos de seguridad de la información que serán incluidos en todos los contratos a terceros (proveedores, compra de servicios, etc.). Se deben considerar todas las responsabilidades y derechos legales, en lo relacionado con la propiedad intelectual y protección de los datos de carácter personal *(ver Política de Protección de Datos Personales, disponible en http://isalud.minsal.cl).* Estos acuerdos de confidencialidad y no divulgación deben ser firmados antes de dar acceso a la información o instalaciones de procesamiento de la información.

7.2.2 Toma de conocimiento

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

- Funcionarios y funcionarias (planta, contrata, reemplazos y suplencia): según lo establecido en el D.F.L. Nº 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 Suma Alzada: a través de cláusula de confidencialidad establecida en el convenio de honorarios.

- Códigos del Trabajo: a través de cláusula de confidencialidad establecida en el contrato.

- Contratos a terceros (proveedores, compra de servicios, etc.): a través de cláusula de confidencialidad establecida en el contrato.

Mediante estos instrumentos los funcionarios y funcionarias, personal código del trabajo, 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 o la Responsable del Activo de que se trate conforme a las normas a que se hace referencia en la presente política.

7.2.3 Concientización, educación y formación en seguridad de la información

Todas las personas que ingresan por primera vez a la institución o se reincorporan luego de una ausencia prolongada, independiente de su calidad contractual o si son prestadores de servicio, que comiencen a realizar sus funciones en la institución, deberán pasar por una inducción a las Políticas, Procedimientos y Estándares de Seguridad de la Información. Las personas indicadas con anterioridad serán responsables de la revisión de las actividades y contenido, una vez que tomen conocimiento a través del Departamento de Gestión y Desarrollo de Personas, por medio del proceso de inducción institucional de los funcionarios y funcionarios, y la Jefatura Directa.

El Departamento de Gestión y Desarrollo de Personas, debe incluir en su plan anual de capacitación de la Subsecretaría de Salud Pública, actividades y cursos sobre Seguridad de la Información. Será responsabilidad del Encargado o Encargada de Seguridad de la Información, impulsar actividades de difusión en conjunto con el Departamento de Gestión y Desarrollo de Personas y el Departamento de Comunicaciones y Relaciones Públicas.

7.3 No divulgación de Información.

Todo el personal que está sujeto a las cláusulas de confidencialidad definidas en el punto 7.2 de esta política. En el caso del personal externo, que requiera acceder a información sensible o confidencial de la Subsecretaría de Salud Pública o Subsecretaría de Redes Asistenciales (Nivel Central), deberán firmar un acuerdo de no divulgación de la información (NDA).

7.4 Propiedad intelectual.

Todos los productos, creaciones, desarrollos, campañas, trabajos, investigaciones, etc. generados por el personal en el ejercicio de sus funciones, durante la vigencia de su contrato, nombramiento o convenio, será de propiedad de la Institución.

7.5 Normas de Seguridad de la Información.

Es responsabilidad del personal, conocer y cumplir con las Políticas de Seguridad de la Información, además asistir a charlas y capacitaciones que la institución determine para tales efectos en la materia.

Es obligación del personal informar cualquier vulnerabilidad o incidente de seguridad de la información, a su jefatura directa y al Encargado de Seguridad de la Información.

Cualquier intento de violación de la seguridad de la información, explotación o generación de vulnerabilidades, ejecutada por el personal no facultado o autorizados para ello, será considerado como una falta grave a las políticas de seguridad de la información, independiente de la motivación.

7.6 Proceso disciplinario.

El incumplimiento de las Políticas, Procedimientos u otros Documentos de Seguridad de la Información, será sancionado en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios de la Subsecretaría de Salud Pública y Subsecretaría de Redes Asistenciales (Nivel Central).

Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, es decir, el incumplimiento de la cláusula de confidencialidad sea realizado por personal contratado como Código del Trabajo , Honorario Suma Alzada o Terceros, se considerará un *incumplimiento grave de las obligaciones que impone el contrato y por ende ponen término IPSO FACTO al contrato/convenio, sin derecho a indemnización*, pues en estos casos, los procedimientos disciplinarios no proceden. Desde luego, sin perjuicio de las responsabilidades civiles y penales que correspóndanse procederá al término anticipado del contrato, por incumplimiento de obligaciones y considerando las responsabilidades civiles y penales que se deriven de tales infracciones.

7.7 Finalización de la relación laboral.

Todo proceso de desvinculación debe realizarse en conformidad a la normativa vigente y los procedimientos del Departamento de Gestión y Desarrollo de Personas. Para el caso de los contratos a terceros, se debe realizar de acuerdo con lo definido en el respectivo contrato y a los procedimientos del Departamento de Administración y Servicios.

Una vez que una persona deja de desempeñar funciones o prestar servicios para la Subsecretaría de Salud Pública y Subsecretaría de Redes Asistenciales (Nivel Central), su Jefatura es responsable de informar al Departamento de Gestión y Desarrollo de Personas, al Departamento TIC (para inactivación o bloqueo del usuario del correo electrónico, de las claves de acceso a sistemas de consulta o gestión institucional), al Departamento de Administración y Servicios (para la

recuperación de los activos asignados) y las entidades y organizaciones externas con las que el funcionario o funcionaria, mantenía contacto en nombre de la institución.

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.

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 todas las personas de la Subsecretaría de Salud Pública y Subsecretaría de Redes Asistenciales (Nivel Central), a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la intranet de Subsecretaría de Salud Pública y Subsecretaría de Redes Asistenciales (Nivel Central) http://isalud.minsal.cl/
- Correo informativo.
- Entrega de una copia, como anexo en las contrataciones realizadas por el Ministerio.

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 2011	Todas	Creación del documento
02	Julio 2020	Todas	Actualización a nueva normativa