PS-NC-014

POLÍTICA SEGURIDAD EN LOS ACUERDOS DE INTERCAMBIO DE INFORMACIÓN

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 PROPOSITO

Definir las directrices para proteger el intercambio de información sensible, entre el Ministerio de Salud del nivel central (en adelante MINSAL) con organizaciones externas, a través de:

- Servicios de red.
- Procedimientos de transferencia de información.
- Acuerdos de transferencia.
- Acuerdos de confidencialidad.

2 ALCANCE O AMBITO DE APLICACIÓN

Esta política se refiere a toda la información física y electrónica contenida en los sistemas de información del MINSAL nivel central, residentes en las Subsecretarias de Salud Pública y Redes Asistenciales, que requiera ser entregada a entidades externas. Bajo las siguientes modalidades:

- Acuerdos de intercambio de información con organizaciones externas, bajo el concepto de interoperabilidad de sistemas.
- Intercambio de Información con organizaciones externas, por traspaso de información vía correo electrónico, por acceso a internet, login a otros sistemas, y/o por cualquier medio magnético o de almacenamiento, papel o medio disponible.

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.

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.13.01.02	Seguridad de los servicios de red.
	A.13.02.01	Políticas y procedimientos de transferencia de información.
	A.13.02.02	Acuerdos de transferencia de información.
	A.13.02.04	Acuerdos de confidencialidad o no divulgación.

3 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 Nº 20.285, de 2008, del Ministerio Secretaría General de la Presidencia, sobre acceso a la información pública.
  - Ley N° 19.628, de 2012, del Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada.
  - Decreto 83, de 2005, del Ministerio Secretaría General de la Presidencia, aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

4 ROLES Y RESPONSABILIDADES

- **Departamento Tecnologías de la Información y Comunicaciones**
  - Debe definir los mecanismos de control para la entrega e intercambio de información electrónica a entidades externas.
  - Debe disponer y aplicar medidas de protección adecuadas para el intercambio de información electrónica.

- **Encargado de Seguridad de la Información**
  - Debe auditar el cumplimiento de esta política, gestionar incidentes de seguridad que se produzcan en el intercambio de información y velar por la correcta aplicación de esta política.

- **Propietario de la información**
  - Debe autorizar o rechazar el intercambio de información de su responsabilidad.
  - Aplicar las medias de protección definidas en la presente política.

- **Usuarios**
  - Deben cumplir con lo establecido en esta política.

5 MATERIAS QUE ABORDA.

- Seguridad de los servicios de red.
- Políticas y procedimientos de transferencia de información.
- Acuerdos de transferencia de información.
- Acuerdos de confidencialidad o no divulgación.

6 DIRECTRICES DE LA POLÍTICA

6.1 Consideraciones generales

El intercambio de información puede originarse en por necesidades del propio Ministerio o por requerimiento del organismo externo o incluso de un particular. En todos los casos deberá analizarse y resolver sobre las competencias del requirente para realizar tratamiento de datos de que se trate.

Todo intercambio de información electrónica perteneciente al MINSAL con terceros, debe ser respaldado con un acuerdo (convenio o contrato) que incluya una cláusula de confidencialidad y/o no divulgación de la información proporcionada, en los términos de la ley 19.628 y la ley 20.584, sin perjuicio de lo señalado por la ley Nº 20.285.

La operatividad del convenio o contrato le corresponde a los departamentos o áreas responsables técnicos del Ministerio.

6.2 Seguridad de los servicios de red

En cualquier acuerdo de servicio de red en el nivel central, la División TIC debe asegurar que se incluyan mecanismos de seguridad1, niveles de servicios, requisitos de administración, acuerdos de confidencialidad y derechos de auditoría. Estos requisitos se deben monitorear de manera regular para asegurar el cumplimiento de estas medidas.

Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas y redes con valor agregado y, soluciones de seguridad de redes administradas como firewalls y sistemas de detección de intrusión. Estos servicios abarcan desde la banda ancha no administrada simple a las ofertas complejas con valor agregado.

---

[1] Las funciones de seguridad de los servicios de red pueden ser:

a) aplicación de tecnología para la seguridad de los servicios de redes, como la autenticación, el cifrado y los controles de conexión de redes.
b) parámetros técnicos necesarios para la conexión segura con los servicios de red de acuerdo con la seguridad y las reglas de conexión de redes.
c) los procedimientos para el uso de servicios de redes para restringir el acceso a los servicios de red o aplicaciones, donde corresponda.

6.3 Políticas y procedimientos de transferencia de información y software

6.3.1 Directrices generales

La transferencia de información puede ocurrir a través del uso de varios tipos distintos de instalaciones de comunicación, incluido el correo electrónico, de voz y video.

Por otro lado, la transferencia de software puede ocurrir a través de varios medios distintos, incluida la descarga de internet y la adquisición de proveedores que venden los productos listos para usar, en la medida que cumplan los estándares de seguridad requerimos para el tratamiento de datos sensibles.

Para el resguardo de la información contra malware (software malicioso), en cualquier intercambio a través de comunicaciones electrónicas, se deben llevar a cabo de acuerdo a lo definido en el “Procedimiento contra código malicioso”.

Cualquier servicio o acuerdo de transferencia de información, debe cumplir con los requisitos legales, definidos para el Sistema de Seguridad de la Información, publicado en el sitio web https://www.minsal.cl/seguridad_de_la_informacion/ y los documentos del Sistema de Gestión de Seguridad de la Información disponibles en http://isalud.minsal.cl/

No se deben mantener conversaciones confidenciales en lugares públicos oficinas abiertas y lugares de encuentro inseguros o a través de canales de comunicación que no garanticen la encriptación de señales y confidencialidad de datos.

6.3.2 Intercambio de Información Manual

El intercambio de información manual sólo debe utilizar los servicios de correos autorizados en el MINSAL, en forma certificada, para controlar su eventual trazabilidad. De ser entregada por mano, debe ser de forma personal al destinatario en un sobre sellado y su entrega debe quedar registrada. Los soportes deberán estar protegidos de accesos indebidos a través de sistemas de encriptación o de claves, las cuales se entregarán a través de medios seguros.

6.3.3 Intercambio vía correo electrónico institucional

Toda información enviada desde el Ministerio a través de correos electrónicos deberá incluir en su pie de página, una advertencia en cuanto a su uso y autorizaciones al respecto, quedando bajo responsabilidad del emisor y receptor el cuidado y resguardo de la información.

Además, la información debe ser encriptada para proteger el contenido en los mensajes de correo electrónico.

Cualquier archivo adjunto que sea enviado mediante correo electrónico, debe ser cifrado y protegido para que sólo el destinatario pueda tener acceso a la información.

Queda prohibido el reenvío automático de correos electrónicos a direcciones de correo externas.

6.3.4 Intercambio vía acceso remoto

Todo intercambio por este medio debe cumplir con la Política de Control de acceso y Seguridad de la Red, establecidos por el MINSAL.

6.3.5 Interoperación entre sistemas

Los acuerdos de interoperabilidad entre sistemas entre MINSAL y organismos externos, también llamados Convenios de Cooperación, deben establecer al menos: el tipo de datos que se intercambiará, las competencias de los órganos, los sistemas que interoperarán, las obligaciones, costos, incumplimientos, responsabilidades y estándares de seguridad. Los convenios tendrán vigencia desde la total tramitación de los Actos Administrativos que los aprueben.

6.3.6 Intercambio vía teléfono o mensajería electrónica

El intercambio de información sensible por este medio no se encuentra permitido.

6.4 Acuerdos de transferencia de información

Cualquier acuerdo de transferencia de información entre MINSAL y partes externas, debe abordar la transferencia segura de la información, para esto los acuerdos deben incorporar lo siguiente:

a) Tipos de datos que se transfieren y finalidad autorizada.
b) Competencias del requirente para requerir la información
c) administración de responsabilidades para controlar y notificar la transmisión, el despacho y la recepción;
d) procedimientos para garantizar la capacidad de seguimiento y no repudiación;
e) normas técnicas mínimas para el empaque y la transmisión;
f) acuerdos de garantía en depósito;
g) responsabilidades en caso de incidentes de seguridad de la información, como la pérdida de datos y obligación de notificación de incidentes de seguridad que afecten al sistema o a los datos;
h) uso de un sistema de etiquetado acordado para la información sensible o crítica, que garantice que el significado de las etiquetas se comprenda inmediatamente y que la información se proteja adecuadamente;
i) normas técnicas para registrar y leer la información y software;
j) cualquier control especial necesario para proteger elementos sensibles, como criptografía;
k) mantener una cadena de custodia para la información durante el tránsito;
l) niveles aceptables de control de acceso.

El contenido de información de seguridad de cualquier acuerdo debe reflejar la sensibilidad de la información involucrada.

6.5 Acuerdos de confidencialidad o no divulgación

Todo acuerdo de interoperabilidad y comunicación de datos debe contener acuerdos de confidencialidad y de no divulgación para proteger la información sensible de la organización, junto con informar a los proveedores sobre su responsabilidad al manipular información sensible.

Cuando los acuerdos de confidencialidad incluyan el acceso de terceros a información sensible o confidencial (por ejemplo, datos de pacientes), se deben considerar además los siguientes requisitos:

a) una definición de la información que se protegerá (es decir, información confidencial);
b) duración esperada de un acuerdo, incluidos los casos donde es posible que sea necesario mantener la confidencialidad de manera indefinida;
c) acciones necesarias al terminar un acuerdo;
d) responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada;
e) propiedad de la información, secretos comerciales y propiedad intelectual y cómo esto se relaciona con la protección de información confidencial;
f) el uso permitido de la información confidencial y los derechos del firmante para utilizar la información;
g) el derecho para auditar y monitorear actividades que involucran información confidencial;
h) el proceso para notificar e informar la divulgación no autorizada o la fuga de información confidencial;
i) términos para la información que se va a regresar o destruir al término del acuerdo;
j) medidas esperadas que se tomarán en caso de un incumplimiento del acuerdo.

En base a los requisitos de seguridad de la información, es posible que se deban incluir otros elementos en un acuerdo de confidencialidad o de no divulgación.

Los acuerdos de confidencialidad y no divulgación deben cumplir con todas las leyes y normativas pertinentes para la jurisdicción a la que corresponden.

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 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.

10 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
00	Agosto 2014	Todas	Creación del documento
01	Octubre 2016	Puntos: 1 al 4 Puntos: 5.1 al 5.5 Se incluyen los puntos 7 y 8	Actualización de la normativa de referencia, se incluyen controles a la política.
02	Julio 2020	Todas	Actualización del documento a la normativa vigente