SENAME
Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

SERVICIO NACIONAL DE MENORES
OFICINA DE PARTES

TRAMITADO

REF: APRUÉBANSE NUEVAS POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE SE INDICAN.

RESOLUCIÓN EXENTA Nº 4604

SANTIAGO, 19 DIC 2019

VISTOS:

Lo dispuesto en los artículos 5º Nºs 1, 12, y 13 del D.L. N° 2.465, de 1979; en los D.S. N°s 356, de 1980 y 307, de 2018, ambos del Ministerio de Justicia y Derechos Humanos; en los D.S. N°s 83 de 2005, 93 de 2006 y 14 de 2014 todos, del Ministerio Secretaría General de la Presidencia; en la Norma Chilena NCH-ISO 27001:2013; en la Ley N°20.285; en el D.F.L. N° 29, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley Nº 18.834, sobre Estatuto Administrativo; la Resolución Exenta N° 2269, de 9 de julio de 2019, de la Dirección Nacional del SENAME; el Memorándum N° 457, de 13 de diciembre de 2019, del Departamento de Planificación y Control de Gestión; en la Resoluciones N° 7 y 8, de 2019, de la Contraloría General de la República.

CONSIDERANDO:

1°. Que, el Servicio Nacional de Menores es el organismo del Estado que tiene por misión contribuir a proteger y promover los derechos de los niños, niñas y adolescentes que han sido vulnerados en el ejercicio de los mismos y a la inserción social de adolescentes que han infringido la ley penal.

2°. Que, en cumplimiento de sus funciones propias, el SENAME reconoce que la información es un recurso que, como el resto de los activos, tiene valor para la Institución, debiendo consecuencialmente ser protegida. La pérdida parcial de información podría tener consecuencias graves para la gestión, debiendo implementarse mecanismos para garantizar la seguridad en el funcionamiento de equipos, datos y sistemas de soporte.

3°. Que, el Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, aprobó Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos. Asimismo, la Norma Chilena Oficial NCh-ISO 27001:2013, proporciona un marco de gestión de Seguridad de la Información utilizable en cualquier tipo de organización, pública o privada.

4°. Que, a través de la Resolución Exenta N° 2269, de 9 de julio de 2019, de la Dirección Nacional del SENAME, se designó al Encargado (Titular y Subrogante), de Seguridad de la Información, así como también a los integrantes (Titulares y Subrogantes) del Comité de Seguridad de la Información.

5°. Que, por Resolución Exenta N° 3026, de 7 de diciembre de 2017, de la Dirección Nacional del SENAME, se aprobaron las siguientes Políticas del Sistema de Gestión de Seguridad de la Información:

- SGSI.PO.01 Política General del Sistema de Gestión de Seguridad de la Información
- SGSI.PO.02 Política de Escritorios y Pantallas Limpias
- SGSI.PO.03 Política de Gestión de Redes
- SGSI.PO.05 Política de Respaldo y Recuperación de Información
- SGSI.PO.09 Política de Acceso y Perímetro de Seguridad Física
- SGSI.PO.10 Política de Dispositivos Móviles y Medios Removibles
- SGSI.PO.11 Política Uso de Internet y Correo Electrónico

6°. Que, el acto administrativo singularizado en el considerando precedente fue modificado por la Resolución Exenta N° 3580, de 28 de noviembre de 2018, del SENAME, en el sentido de sustituir la General del Sistema de Gestión de Seguridad de la Información, e incorporar dos 2 nuevas políticas a dicho Sistema:

- SGSI.PO.01 Política General del Sistema de Gestión de Seguridad de la Información
- SGSI. PO.12 Política de Transferencia de Información y Acuerdos de Confidencialidad.

1985

- SGSI.PO.13 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.

7°. Que, el Departamento de Planificación y Control de Gestión, a través de su Memorándum N° 457, de 13 de diciembre de 2019, solicitó proceder a la actualización del texto de las políticas existentes y la incorporación de tres nuevas Políticas al Sistema de Gestión de Seguridad de la Información, como se señala a continuación:

- SGSI.PO.01 Política General (Sustitución)
- SGSI.PO.02 Política de Escritorios y Pantallas Limpias (Sustitución)
- SGSI.PO.03 Política de Gestión de Redes (Sustitución)
- SGSI.PO.05 Política de Respaldo y Recuperación de Información (Sustitución)
- SGSI.PO.09 Política de Control de Acceso y Perímetro de Seguridad Física (Sustitución)
- SGSI.PO.10 Política de Dispositivos Móviles, Medios Removibles (Sustitución)
- SGSI.PO.11 Política de Uso de Internet y Correo Electrónico (Sustitución)
- SGSI.PO.12 Política de Transferencia de Información y Acuerdos de Confidencialidad (Sustitución)
- SGSI.PO.13 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas (Sustitución)
- SGSI.PO.14 Política de Controles Criptográficos (Nueva)
- SGSI.PO.15 Política de Continuidad Operativa (Nueva)
- SGSI.PO 16 Política de Seguridad con Proveedores (Nueva)

RESUELVO:

1° APRUÉBANSE los textos de las Políticas del Sistema de Gestión de Seguridad de la Información, singularizadas en el considerando séptimo del presente acto administrativo, siendo su texto el siguiente:

I.

POLÍTICA GENERAL

SISTEMA DE GESTIÓN DE

SEGURIDAD DE LA INFORMACIÓN

SGSI.PO.01

1. INTRODUCCIÓN

El Servicio Nacional de Menores (SENAME) es un organismo gubernamental centralizado y dependiente del Ministerio de Justicia. Fue creado por el Decreto de Ley N° 2.465 del 10 de enero de 1979, que fija el texto de su Ley Orgánica, y fue publicado en el Diario Oficial el 16 de enero del mismo año.

El SENAME tiene como objetivos estratégicos institucionales:

- Restituir y/o reparar los derechos vulnerados de los niños/as y adolescentes por medio de prestaciones de protección.
- Reinsertar socialmente a adolescentes imputados y/o condenados/as conforme a estándares definidos por la Ley 20.084.
- Promover los derechos y prevenir la vulneración de los mismos para niños/as y adolescentes.
- Supervisar la atención de los niños/as y adolescentes atendidos en la oferta del Servicio como a su vez el uso eficiente de los recursos, a fin de mejorar la calidad de las prestaciones dando cumplimiento a los estándares establecidos por el Servicio en concordancia con mandatos legales aprobados por el Estado de Chile.
- Actualizar continuamente la oferta dedicada a la atención de niños, niñas y adolescentes vulnerados/as en sus derechos y la rehabilitación de adolescentes que han infringido la ley, a fin de adecuarlas a las políticas nacionales e internacionales sobre la materia y mandatos legales aprobados por el Estado de Chile y en conformidad a estándares de calidad.

El SENAME reconoce que la información es un recurso que, como el resto de los activos, tiene valor para la Institución y, por consiguiente, debe ser debidamente protegida. La pérdida parcial de información podría tener consecuencias graves para la gestión y, por ende, se deben implementar las salvaguardas adecuadas para garantizar que los equipos, datos y los sistemas que los soportan, sean seguros.

Por esta razón, se establece esta Política del Sistema de Gestión de Seguridad de la Información, el cual tiene como objetivo proteger los activos de Información de una amplia

POLÍTICA DE SEGURIDAD CON PROVEEDORES

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia
y Derechos Humanos

Gobierno de Chile

SGSI.PO.16

Información del Documento

REV 00	Elaborado por:	Revisado por:	Aprobado por:
Nombre	**Hector Burgos Cañete** Encargado Sistema de Gestión de la Seguridad de la Información	**Cristian Castillo Silva** Jefe Departamento Planificación y Control de Gestión	**Susana Tonda Mitri** Directora Nacional
Fecha	06/12/2019	06/12/2019	06 DIC. 2019
Firma	SERVICIO NACIONAL DE MENORES Jefe Subdepto. de Planificación y Control de Gestión	SERVICIO NACIONAL DE MENORES Jefe Depto. de Planificación y Control de Gestión	SERVICIO NACIONAL DE MENORES DIRECTORA NACIONAL

Control de Versiones

Nombre		Fecha	Dpto.
Elaboró	Hector Burgos Cañete	06 DIC. 2019	Encargado Sistema de Gestión de la Seguridad de la Información
Revisó	Cristian Castillo Silva	06 DIC. 2019	Jefe Departamento Planificación y Control de Gestión

Registro de Modificaciones (*)				
Revisión		Nombre/Dpto. Emisor	Descripción de la modificación / (Página o sección afectada)	Aprobó
N°	Fecha			
00	06 DIC. 2019	DEPLAE	Emisión	DIRECCIÓN NACIONAL

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El presente documento, se enmarca dentro de la Política General de Seguridad de la Información para el Servicio Nacional de Menores, con la finalidad de reglamentar la relación con los proveedores de servicios entregados al SENAME.

2 POLÍTICA

2.1. PRESTACIÓN DE SERVICIOS ASOCIADOS AL TRATAMIENTO DE INFORMACIÓN

En las situaciones en que se requiera contratar servicios de tratamiento o resguardo de activos de información, tales como servicios de hosting e infraestructura, plataforma tecnológica, centros de datos y procesamiento, almacenaje de información física o digital, entre otros, se deberá verificar que el proveedor cuenta con mecanismos y controles de seguridad adecuados.

Por su parte, para el caso en que existan proveedores que desarrollen sistemas de información para la Institución, se deberá considerar la revisión de los productos elaborados a partir de revisiones técnicas por parte del Departamento de Planificación y Control de Gestión, a través del Procedimiento de Desarrollo de sistemas y gestión de datos (SGSI.PR.28).

2.2. CONTRAPARTE TÉCNICA EN MATERIAS DE SEGURIDAD Y TECNOLOGÍA

El Encargado de Seguridad de la Información designado por el acto administrativo respectivo, será la Contraparte técnica en materia de seguridad y tecnología en todas aquellas contrataciones de servicios o productos que tengan relación con activos TI del Servicio Nacional de Menores, tales como almacenamiento de documentos, compra de servidores, adquisición de dispositivos móviles, construcción de sistemas, desarrollo de sitios webs, servicios de infraestructura tecnológica, softwares como servicio, enlaces de comunicación, entre otras.

2.4. ACCESO FÍSICO A LOS ACTIVOS DE INFORMACIÓN Y LOS EQUIPOS TECNOLÓGICOS

El acceso físico y lógico por parte de los proveedores a los activos de información deberá ser controlado y supervisado por personal administrativo o técnico, según sea el caso, perteneciente al servicio (SGSI.PO.09 - Política de Control de Acceso y Perímetro de Seguridad Física). En las áreas protegidas o de alto riesgo, como es el caso de la sala de procesamiento de datos, se deberán establecer procedimientos documentados formales que tengan por objeto gestionar la forma en que se realizarán los trabajos en su interior, el que deberá contar con medidas de registro de proveedores (SGSI.PR.23 - Procedimiento de Gestión de Accesos)

2.5. ACCESO REMOTO A TRAVÉS DE HERRAMIENTAS INFORMÁTICAS

Los proveedores podrán acceder en forma remota a los activos tecnológicos a través de herramientas tales como Red Privada Virtual (VPN), cuando ello fuere necesario para el cumplimiento de las obligaciones que emanan del contrato respectivo, esto está establecido en SGSI.PO.09 - Política de Control de Acceso y Perímetro de Seguridad Física. El acceso será gestionado por el Subdepartamento de Informática y sólo podrá tener por finalidad dar soporte a equipos tecnológicos o sistemas de información, revisar errores de funcionamiento o prestar servicios de seguridad y/o monitoreo. Para garantizar lo anterior, el Servicio Nacional de Menores deberá implementar controles que permitan limitar su acceso y registrar

acciones para seguimiento, esto está estipulado en el SGSI.PR.23 - Procedimiento de Gestión de Accesos.

2.6. CONTRATACIÓN PERMANENTE DE SERVICIOS TECNOLÓGICOS

Cuando se requiera elaborar un contrato particular con proveedores que tenga relación con servicios de tratamiento, manipulación, transmisión, monitoreo o almacenamiento de activos de información y redes, ya sea en formato físico o digital, se deberán incorporar cláusulas de seguridad que permitan garantizar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, tales como acuerdos de niveles de servicios (SLA) los cuales son definidos de forma particular con cada proveedor y dependiendo del nivel de criticidad que este tenga, derechos de auditar los procesos involucrados, los procedimientos aplicados frente a incidentes de seguridad, cláusulas de confidencialidad y no divulgación de información, como también la extensión de dichos deberes a empresas subcontratadas.

2.7. INSPECCIÓN Y AUDITORÍA DE LAS CONDICIONES DEL SERVICIO

Para asegurar que los proveedores que prestan servicios en el tratamiento de información de propiedad de la Institución cuenten con estándares y niveles adecuados en materia de seguridad, el Servicio Nacional de Menores se reserva el derecho de solicitar evidencia de la ejecución de auditorías independientes relacionadas a riesgo tecnológico, control interno, o auditorías de certificación relacionados con dicha materia, los que para cualquier efecto serán facilitados de manera temporal y con el objeto de revisar el alcance del trabajo realizado y el detalle de los resultados obtenidos.

2.8. MANEJO DE INCIDENTES DE SEGURIDAD ASOCIADOS A LOS SERVICIOS

Para los proveedores que tengan relación con almacenamiento, comunicación, infraestructura, plataforma o software que sean entregados a la Institución en modalidad de servicio, también conocidos como servicios en la nube, además de los equipos tecnológicos que sean adquiridos o sistemas de información que sean desarrollados por terceros y sobre los cuales existan garantías del fabricante, se deberán establecer y documentar procedimientos para la gestión de incidentes de seguridad (SGSI.PR.12 - Procedimiento de gestión de eventos, debilidades e incidentes)

2.9. PROPIEDAD INTELECTUAL

Queda estrictamente prohibido el uso de programas informáticos que no cuenten con licencia, como lo indica SGSI.PO.13 - Política de Adquisición, Desarrollo y Mantenimiento de Sistemas. "Queda prohibido el uso, reproducción, cesión transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización del proveedor, quien deberá presentar su registro en el INAPI"

2.10. GESTIÓN DE CAMBIOS EN LA PROVISIÓN DE LOS SERVICIOS

Cuando existan cambios en la provisión de los servicios, estos deben ser administrados por el funcionario o equipo asignado para el monitoreo, y revisión de los servicios del proveedor. Esta administración de cambios se debe realizar considerando la mantención y/o mejora de los requisitos de seguridad de la información definidos en la compra del servicio, los controles específicos, la criticidad de la información, los sistemas y procesos involucrados, junto con la reevaluación de los riesgos. Además de lo mencionado se deben considerar los siguientes aspectos:

a) Cambios a los acuerdos del proveedor
b) Cambios realizados por la organización por implementar:
   - Mejoras de los servicios que se ofrecen actualmente (actualizaciones)
   - Desarrollo de cualquier nueva aplicación (SGSI.PR.28 - Procedimiento de Desarrollo de sistemas y gestión de datos)
   - Controles nuevos o cambiados para resolver incidentes de seguridad de la información y mejorar la seguridad
c) Cambios en los servicios del proveedor a implementarse
   - Cambios y mejoras en las redes
   - Uso de nuevas tecnologías
   - Cambio de proveedores

3 ALCANCE

El alcance de la presente política será aplicable a los activos de información, activos físicos, activos de servicio de TI y activos humanos asociados al proceso de Desarrollo de la Oferta de líneas de acción establecidas en la ley N°20.032, realizados en la Dirección Nacional del Servicio Nacional de Menores, ubicada en Huérfanos 587, Santiago.
Se aplica a los funcionarios (planta, contrato, honorarios) de la Dirección Nacional del Servicio, proveedores y trabajadores externos, que intervengan en el proceso de "Desarrollo de la Oferta"

4 OBJETIVO

El objetivo principal de la presente política es definir las reglas básicas para la relación con proveedores. Este documento se aplica a todos los proveedores que tengan influencia sobre la confidencialidad, integridad y disponibilidad de la información sensible del Servicio Nacional de Menores.

5 RESPONSABILIDADES

- **DIRECTOR(A) NACIONAL DE SENAME**
  En su calidad de tal, tiene la responsabilidad de revisar y aprobar esta Política dentro de su área de competencia, debiendo procurar además que se asignen suficientes recursos humanos, materiales y financieros para implementarla. La alta dirección debe establecer claramente el enfoque de la Política en línea con los objetivos institucionales y demostrar su apoyo y su compromiso con la seguridad de la información, promoviendo la mejora continua a través de la emisión y mantenimiento de esta *Política de Seguridad con Proveedores,* en toda la Institución para que el, Sistema de Gestión de Seguridad de la Información, ahora en adelante SGSI, logre sus resultados esperados.
- **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**
  El Comité de Seguridad de la Información del SENAME, tiene dentro de sus responsabilidades y funciones velar por la implantación del Sistema de Gestión de la Seguridad de la Información e impulsar, promover y revisar periódicamente la implementación de las políticas de seguridad de la información.
- **ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN**
  Alinea la debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio, además de monitorear el avance general de la implementación de las estrategias de control y tratamiento de

riesgos.
Tiene que mantener la aplicabilidad de este documento acorde a las prácticas operacionales del SENAME, por lo que es responsable de generar las modificaciones necesarias para que este siempre actualizado. Es responsable de gestionar la publicación y dar a conocer nuevas versiones del documento.
Adicionalmente es el encargado de revisar y verificar que los contratos suscritos con los proveedores cumplan con los requisitos mínimos de seguridad y velar por el cumplimiento de esta política.
Tiene que mantener la aplicabilidad de este documento acorde a las prácticas operacionales del SENAME, por lo que es responsable de generar las modificaciones necesarias para que este se encuentre siempre actualizado. Además, es responsable de publicar y dar a conocer nuevas versiones del documento.

- **PERSONAL DEL PROCESO DE DESARROLLO DE LA OFERTA DEL SENAME**
  Tendrán la responsabilidad de cumplir con lo formalizado en este documento y así garantizar que los activos de información que se encuentren a su cargo estén protegidos contra el mal uso, robo, falta de disponibilidad o destrucción. Deberán trabajar en conjunto con los Directivos en todos los aspectos de la seguridad de la información, para garantizar que se implementen controles y procedimientos en forma adecuada y completa. Además, tendrán la responsabilidad de notificar incidentes de seguridad y potenciales debilidades que pudieran identificarse.

6 REVISIÓN, VALIDACIÓN Y DIFUSIÓN

El Comité de Seguridad de la Información de la Institución revisará al menos una vez al año la presente Política, a efectos de mantenerla actualizada. Asimismo, efectuará toda modificación que sea necesaria en función de posibles cambios que puedan afectar su definición, como, por ejemplo, cambios tecnológicos, impacto de los incidentes de seguridad, cambios legislativos, entre otros.
La responsabilidad de la validación de la Política de Seguridad con Proveedores al interior del SENAME es del (la) Director(a) Nacional del Servicio.
El Subdepartamento de Informática de SENAME, apoyarán la difusión de las políticas y procedimientos utilizando las herramientas y plataformas que estime conveniente para tal efecto.
Los funcionarios y proveedores de servicios tendrán acceso a esta Política en su última versión vía Intranet institucional y página web del servicio.

7 CUMPLIMIENTOS

La presente Política entra en vigencia una vez oficializada por el (la) Director(a) Nacional del SENAME. Las jefaturas de los distintos departamentos, subdepartamentos y unidades del Servicio serán responsables de darlas a conocer a su personal subordinado.
Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá comunicar acerca de la existencia de la política, para conocimiento y acceso a la misma.

8 SANCIONES

Cualquier conflicto con las regulaciones debe ser informado inmediatamente al encargado de seguridad del SGSI.

El incumplimiento de la Política del sistema de Gestión de Seguridad de la Información podrá tener como resultado la aplicación de diversas sanciones en el ámbito administrativo, civil y/o penal, conforme a la magnitud y característica del aspecto no cumplido o vulnerado.

9 TÉRMINOS Y DEFINICIONES

A los efectos de este documento, se aplican las siguientes definiciones:

- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Confidencialidad**: Protección de la información sensible ante divulgación no autorizada.
- **Integridad**: Exactitud, configuración y calidad de un activo de información.
- **Disponibilidad**: Preservación de un activo de información y acceso de personas autorizadas a su uso.
- **Seguridad de la Información:** Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.
- **VPN (Red Virtual Privada):** es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
- **INAPI:** Es el Instituto Nacional de Propiedad Industrial de Chile.