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:

1º. 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.

2º. 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.

3º. 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.

4º. 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.

5º. 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

6º. 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.

19865

- 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 DISPOSITIVOS MÓVILES, MEDIOS REMOVIBLES

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

SGSI.PO.10

Información del Documento

REV 00	Elaborado por:	Revisado por:	Aprobado por:
Nombre	**Hector Burgos Cañete** Encargado Sistema de Gestión de 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	C 6 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	C 6 DIC. 2019	Encargado Sistema de Gestión de Seguridad de la Información
Revisó	Cristian Castillo Silva	C 6 DIC. 2019	Jefe Departamento Planificación y Control de Gestión

Registro de Modificaciones
(*)

Revisión N°	Revisión Fecha	Nombre/Dpto. Emisor	Descripción de la modificación / (Página o sección afectada)	Aprobó
00	13 OCT. 2017	DEPLAE	Emisión	DIRECCIÓN NACIONAL
01	C 6 DIC. 2019	DEPLAE	• Corrección de palabra Smartphone en página 04 • Corrección de encabezado del documento • Se añade restricción de almacenamiento de información sensible (Sección 2.1) • Eliminación de Responsable del Documento en la sección 5	

(*) La presente versión sustituye completamente a todas las precedentes, de manera que el último del listado será el único documento válido de todos los registrados.

TABLA DE CONTENIDOS

1 INTRODUCCIÓN

Los dispositivos móviles y medios removibles ofrecen una gran cantidad de beneficios y facilidades en la operación de herramientas informáticas básicas y necesarias para la labor del Servicio Nacional de Menores, no obstante, el uso de dichos dispositivos también implica algunos riesgos, que deben ser analizados y gestionados.

La presente política se establece en el marco del Sistema de Gestión de Seguridad de la Información, con la finalidad de reglamentar el uso de los dispositivos móviles y medios removibles dentro del Servicio Nacional de Menores, a fin de minimizar los riesgos asociados a estos.

2 POLÍTICA

2.1 DISPOSITIVOS MÓVILES

A través de la siguiente política, inicialmente se establece que sólo podrán ser utilizados para gestionar y almacenar información del Servicio, aquellos dispositivos móviles provistos por el mismo Servicio, y que han sido registrados por la Unidad de Administración Central, junto a su respectivo responsable. Con esto, los dispositivos móviles particulares del personal, no podrán tener acceso a información o redes correspondientes al Servicio. Aquellos casos particulares en que se requiera de manera imperante el uso de un dispositivo móvil particular para efectos de trabajo, deberá ser registrado tanto el aparato, como el responsable en la Unidad de Administración Central, previa solicitud formal del jefe del Departamento Correspondiente, e informado a el Encargado de Seguridad de la Información.

Además de lo anterior, el uso de dispositivos móviles deberá considerar las siguientes directrices:

- Los dispositivos móviles utilizados en el Servicio serán Notebooks, Tablets, y Smartphones.
- Los dispositivos móviles serán activos de procesamiento de información, y por tanto deberán incorporarse al registro de inventario de activos.
- El responsable de cada dispositivo móvil, deberá encargarse de la seguridad física de estos, protegiéndolo contra golpes, humedad, u otro factor que pudiere dañarlo.
- El responsable de cada dispositivo móvil, deberá encargarse de no instalar softwares y aplicaciones que no apunten a las tareas para la cual fue asignado el dispositivo móvil.
- Sólo los dispositivos móviles registrados y autorizados, podrán tener acceso a redes del Servicio.
- Está prohibido el almacenamiento de información sensible de Niños, Niñas y Adolescentes en los dispositivos móviles institucionales.
- Todo dispositivo móvil deberá poseer una contraseña, acorde a lo establecido en el Procedimiento de gestión de contraseñas (SGSI.PR.17). En caso de Smartphone y tablets, deberán contar con algún método que restrinja el acceso sólo al responsable del dispositivo.
- Todo dispositivo móvil deberá contar con un antivirus
- En caso de pérdida o robo de algún dispositivo móvil, se debe dar aviso inmediato al encargado de seguridad de la información, quien tratará el hecho como un incidente de

seguridad de la información.

2.2 MEDIOS REMOVIBLES

En este apartado de la política, se establece que los medios removibles podrán ser utilizados para transportar información del Servicio, sólo cuando este medio haya sido provisto por el mismo Servicio. Cabe destacar que por medios removibles se refiere a cualquier dispositivo electrónico que pueda almacenar información, tales como Discos duros, Pendrives y Discos CD o DVD.

Además, se debe aclarar que los medios removibles sólo podrán ser utilizados para transportar información de manera temporal, y no para respaldar información, dado que dichos respaldos deben quedar almacenados en otros medios, tal como se establece en la Política de Respaldo y Recuperación de información (SGSI.PO.05).

Todo medio removible que presente fallas o deba ser eliminado por algún motivo, se enviará al encargado de seguridad de la información, quien gestionará su formateo o eliminación segura.

Cada unidad o departamento involucrado en el alcance del sistema de seguridad de la información, deberá mantener un stock determinado de pendrives institucionales, a cargo de secretaría, los cuales serán solicitados por los funcionarios para transportar información y luego serán devueltos vacíos a la misma secretaria. La gestión de estos pendrives, será registrada en un documento de acuerdo a lo que establece el procedimiento para la gestión de equipos (SGSI.PR.22)

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 pertenezcan al proceso de "Desarrollo de la Oferta", y los sistemas controlados serán los siguientes:

- Active Directory
- SENAINFO

Esta política no aplica a los dispositivos móviles y medios removibles de uso personal de los trabajadores, en cuanto estos no estén registrados como dispositivos que almacenarán información del Servicio.

Los Notebooks del Servicio que han de solicitarse a Servicios TI para reuniones o eventos especiales, no serán objetos de esta política, toda vez que ellos son utilizados sólo para eventos puntuales, y no almacenarán información sensible del Servicio.

4 OBJETIVOS

Se implementa la presente política con el objetivo de controlar los riesgos de seguridad de la información implícitos en el uso de dispositivos móviles y medios removibles. Específicamente, se pretende restringir el uso de dispositivos móviles y medios removibles a sólo aquellos de propiedad del Servicio, evitando la utilización de dispositivos particulares que pudieren afectar la confidencialidad de la información sensible del Servicio.

5 RESPONSABILIDADES

- **PROFESIONAL DE REDES Y COMUNICACIONES**
  Gestionar los accesos a redes de los dispositivos móviles.

- **DIRECTOR(A) NACIONAL**
  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 actualización de esta Política de Dispositivos Móviles y Medios Removibles en la Institución y así asegurar que el SGSI logre sus resultados esperados.

- **ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN**
  Tendrá la responsabilidad de monitorear la aplicación de la presente política, además de levantar los formularios de eventos de seguridad de la información cada vez que sea informada o detectada alguna falta en contra de esta política.
  También será el responsable de controlar el uso de dispositivos móviles de particulares, cuando sea requerido por alguna jefatura de departamento, y llevar el registro de los dispositivos móviles autorizados y sus responsables.
  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.

- **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**
  Tendrá la responsabilidad de revisar y aprobar la creación y cambios de versiones realizados a la presente política.

- **PERSONAL DE SENAME Y/O USUARIOS DE DISPOSITIVOS MÓVILES QUE INTERVENGAN EN EL PROCESO DE DESARROLLO DE LA OFERTA**
  Tendrán la responsabilidad de cumplir con lo formalizado en este documento y así garantizar que los dispositivos móviles sean utilizados de manera responsable, resguardando la información sensible que estos puedan almacenar.

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 y difusión de la Política de Seguridad de la Información al interior del SENAME es del (la) Director(a) Nacional del Servicio, quien se apoyará para estos propósitos en las Jefaturas.
El Subdepartamento de Informática o la Unidad de Comunicaciones del SENAME, apoyarán en la difusión de las políticas y procedimientos utilizando las herramientas y plataformas que estime conveniente para tal efecto.
Los funcionarios y personal externo tendrán acceso a esta Política en su última versión vía Intranet en formato digital y página web del servicio.
Los funcionarios, personal externo y proveedores de servicios, tendrán acceso a esta Política en su última versión vía Intranet y Pagina Web del servicio, en formato digital.

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 pertenecientes al Desarrollo de la Oferta serán responsables de difundirlas a su personal a cargo.
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 leyes y normativas asociadas a seguridad de la información 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:

- **Activos de Información:** Corresponde a todos aquellos elementos relevantes involucrados en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de valor para la Institución.
- **Confidencialidad**: Protección de la información sensible ante divulgación no autorizada.
- **Disponibilidad**: Preservación de un activo de información y acceso a personas autorizadas a su uso.
- **Dispositivo móvil:** aparatos de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar a cabo otras funciones más generales. En este Servicio han de considerarse dispositivos móviles los Notebooks, Tablets y Smartphones.
- **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.

- **Integridad**: Exactitud, configuración y calidad de un activo de información.
- **Medios removibles:** Se refiere a aparatos digitales capaces de almacenar información, tales como pendrives, discos duros, CDs y DVDs.
- **Redes:** es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos.
- **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.