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.

19185

- 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 CONTINUIDAD OPERATIVA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

SGSI.PO.15

Información del Documento

REV 00	Elaborado por:	Revisado por:	Aprobado por:
Nombre	**Hector Burgos Cañete** Encargado Sistema de Gestión de Seguridad de la Información	**Roberto Aguilera González** Jefe (S) Departamento Planificación y Control de Gestión	**Susana Tonda Mitri** Directora Nacional
Fecha	12 DIC. 2019	12 DIC. 2019	
Firma	SERVICIO NACIONAL DE MENORES Jefe Subdepto. de Planificación y Control de Gestión		SERVICIO NACIONAL DE MENORES DIRECTORA NACIONAL

Control de Versiones

Nombre		Fecha	Dpto.
Elaboró	Hector Burgos Cañete	12 DIC. 2019	Encargado Sistema de Gestión de Seguridad de la Información
Revisó	Roberto Aguilera González	12 DIC. 2019	Jefe (S) 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	12 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 continuidad operativa del servicio en caso de interrupciones o fallas en los distintos procesos definidos en el alcance.

2 POLÍTICA

- El Servicio Nacional de Menores se compromete a garantizar que todos los procesos relacionados con el desarrollo de la oferta operen adecuadamente, bajo los principios de universalidad, continuidad, oportunidad, calidad y confiabilidad, para asegurar el normal funcionamiento de sus operaciones de servicio a la institución y comunidad de usuarios, mediante la implementación de un plan de continuidad operativa (en adelante BCP).
- Para la aplicación del Plan de Continuidad operativa se establecen como elementos primordiales los siguientes: la protección de los activos de información de la Institución y la continuidad de las operaciones.
- El Plan de Continuidad operativa debe incluir la identificación de los principales riesgos que pueden afectar la continuidad del proceso de desarrollo de la oferta.
- La elaboración, dentro del Plan de Continuidad operativa, de procedimientos de comunicación apropiados, tanto internos como externos, que posibiliten la correcta ejecución de los mismos, así como el suministro oportuno de información a todas las partes interesadas.
- La elaboración del El Plan de Continuidad operativa del Servicio Nacional de Menores quedará registrada en el Procedimiento de Continuidad operativa (SGSI.PR.29)

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 Servicio, proveedores y trabajadores externos, que pertenezcan al proceso de "Desarrollo de la Oferta", y los sistemas controlados serán los siguientes:

- Active Directory
- SENAINFO

4 OBJETIVO

El objetivo principal de la presente política es que el Servicio Nacional de Menores, cuente con un plan de continuidad operativa para el proceso de Desarrollo de la Oferta, a efecto de contrarrestar o mitigar el impacto de eventos que pueden provocar interrupciones en dicho proceso, adicionalmente aminorar las repercusiones de las posibles catástrofes sobre las actividades operativa, garantizando que se preserven los datos y funciones esenciales o, de no ser posible, que tales datos o funciones se recuperen, oportuna y progresivamente, hasta la vuelta a la normalidad.

5 RESPONSABILIDADES

- **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 implementación 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.
  - Garantizar que se documenten y mantengan actualizados y disponibles los procedimientos para hacer frente a un incidente, desde que éste se presenta, hasta la restauración o vuelta a la normalidad, tanto en lo que se refiere al accionar interno como externo a la Institución.
  - Asegurar que las funciones y responsabilidades detalladas en los planes de continuidad operativa, se asignen al personal idóneo para la atención de los incidentes.
  - Velar porque se cumpla con los planes de capacitación al personal, tanto titular como sucesor en los roles que debe desempeñar en caso de incidentes.

- **JEFE DEPARTAMENTO DE PLANIFICACIÓN Y CONTROL DE GESTIÓN**
  - Validar los procesos críticos institucionales que se deban considerar en el Plan de Continuidad operativa, así como la estimación del tiempo máximo que puede soportar la Organización con la interrupción del servicio, producto del incidente que se presente.
  - Asegurar que se formulen, evalúen, y mantengan actualizados los Planes de Continuidad operativa, por parte de los responsables de los procesos críticos, y que se divulguen a todos los funcionarios, personal externo y proveedores de servicios. Se entiende como plan de continuidad operativa, un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto en la operación.
  - Asegurar que se mantenga actualizado el análisis de vulnerabilidad y amenazas, así como la evaluación periódica de los riesgos y sus probabilidades de materialización con el fin de actualizar los planes de continuidad operativa.
  - Asegurar que, ante cambios significativos en los procesos empresariales, se actualice el plan de continuidad operativa.

- **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 Continuidad operativa en la Institución y así asegurar que el SGSI logre sus resultados esperados.

- **ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN**
  Tendrá la responsabilidad de coordinar las actividades relacionadas a la gestión de la Política de Seguridad de la Información dentro del SENAME, a través de la ejecución de las siguientes funciones:

1. Coordinar las actividades del Comité de Seguridad de la Información.
2. Coordinar la debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales.
3. Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos asociados a seguridad de la información y ciberseguridad.
4. Mantener coordinación con otros departamentos de la Institución para apoyar los objetivos de la seguridad de la información.
5. 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 esté siempre actualizado. Junto con lo anterior, es responsable de gestionar la publicación y dar a conocer nuevas versiones del documento.
6. Revisar y verificar que el Plan de Continuidad operativa cubra en forma razonable los eventos que tienen una alta probabilidad de ocurrencia y que impacten negativamente la continuidad operacional del servicio
6. Velar por la aplicación de la presente política de continuidad operativa, así como formular, y gestionar las modificaciones en la misma.

- **PERSONAL DEL PROCESO DE DESARROLLO DE LA OFERTA DEL SENAME**
  Conocer, respetar y acatar permanentemente la política de continuidad operativa del SENAME.
  Deben informar al encargado de seguridad de la información cuando se materialice algún riesgo que comprometa o afecta la continuidad operacional

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, para 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, variación de los costos de los controles, impacto de los incidentes de seguridad, cambios legislativos, entre otros.

La responsabilidad de la validación y aprobación de la Política de Continuidad operativa al interior del SENAME es del (la) Director(a) Nacional del Servicio.

Junto con lo anterior se incluirán orientaciones generales del sistema, su importancia y acceso a la información y canales de contacto, tanto como en la charla de inducción a nuevos funcionarios y en el contenido del Manual de Inducción Institucional, ambas actividades desarrolladas por el Área de Inducción y Evaluación de Desempeño de la Unidad de Desarrollo Organizacional de SENAME.

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, 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 siguiente Política de Continuidad operativa entra en vigencia una vez sea oficializada por el (la) Director(a) Nacional del Servicio Nacional de Menores. 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 de Continuidad operativa (SGSI.PO.15) 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:

- **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.
- **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.
- **Plan de Continuidad operativa (BCP):** es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado.
- **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.