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.

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 RESPALDO Y RECUPERACIÓN DE INFORMACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia y Derechos Humanos
Gobierno de Chile

SGSI.PO.05

Información del Documento

REV 02	ELABORADO POR	REVISADO POR	APROBADO POR
Nombre	**Hector Burgos Cañete** Encargado Sistema de Gestión de Seguridad de la Información	**Cristian Castillo Silva** Jefe Departamento de Planificación y Control de Gestión	**Susana Tonda Mitri** Directora Nacional
Fecha	06/12/2019	6/12/2019	C 6 DIC. 2019
Firma			

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		**Nombre /Dpto Emisor**	**Descripción de la modificación / (Página o sección afectada)**	**Aprobó**
N°	**Fecha**			
00	C 7 NOV. 2016	DEPLAE	Emisión	DIRECCIÓN NACIONAL
01	13 OCT. 2017	DEPLAE	• Modificación de formato, fuente, tamaño e interlineado. / (Todo el documento) • Se actualiza política. (Sección 2)	DIRECCIÓN NACIONAL
02	C 6 DIC. 2019	DEPLAE	• Renombramiento de Unidad de Informática por Subdepartamento de Informática (Todo el Documento) • Actualización de alcance de la Política	DIRECCIÓN NACIONAL

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

TABLA DE CONTENIDOS

1 INTRODUCCIÓN

La presente política se establece en el marco del Sistema de Gestión de Seguridad de la Información, con la finalidad de garantizar la protección de los activos de la organización, mediante copias de respaldo de información óptimas que nos permitan obtener niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de la información de SENAME, considerados relevantes dentro del alcance, con el objeto de asegurar continuidad operacional de los procesos y servicios que desarrolla la institución, mediante el correcto resguardo de éstos.

2 POLÍTICA

El Servicio Nacional de Menores considera que toda información contenida de sus sistemas de información críticos en producción debe ser protegida de posibles daños, por lo que será respaldada con una frecuencia establecida para asegurar el proceso de recuperación. El Departamento de Planificación y Control de Gestión será el encargado de identificar y mantener una matriz actualizada de aquella información necesaria para mantener operativos sus procesos, durante eventuales procedimientos de restauración. Lo anteriormente descrito se plantea en el Procedimiento de Administración de activos de la información (SGSI.PR.10).

El Subdepartamento de Informática deberá considerar soluciones de respaldo para servidores y aplicaciones (códigos fuente, bases de datos) que se consideren críticos para la institución, así como también garantizar la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles, en medida de lo posible, incluso después de algún desastre o la falla de un dispositivo. El Subdepartamento de Informática de SENAME, establecerá las configuraciones correspondientes y la periodicidad de las pruebas para asegurar los requisitos del servicio.
Toda información que no sea considerada crítica para el quehacer de la institución y que resida en los servidores y equipos de escritorios de SENAME, NO SERÁ RESPALDADA.
En las situaciones donde la confidencialidad es relevante, se deberán proteger los respaldos mediante cifrado.

El Departamento de Planificación y Control de Gestión de la Dirección Nacional a través de su Subdepartamento de Informática deberá tomar los recaudos para llevar un registro actualizado con cada respaldo que se lleve a cabo, sea éste de manera manual o automático. Dicho registro deberá quedar almacenado en un archivo determinado con acceso controlado, como indica el Procedimiento de Respaldo y Recuperación del Servicio Nacional de Menores (SGSI.PR.20),

Los respaldos deberán cumplir con un nivel apropiado de protección física de los medios, consistente con las prácticas aplicadas en el sitio principal. Los controles asociados a los dispositivos del sitio de producción deberán extenderse, para abarcar el sitio de respaldo, en el caso de que existiere considerando lo establecido en la Política de control de acceso y Perímetro de Seguridad Física (SGSI.PO.09).

La periodicidad, tipo y mecanismo de respaldo y recuperación de activos de información serán definidos por el Subdepartamento de Informática de la Dirección Nacional en conjunto con el Encargado de Seguridad de la Información, quienes serán los responsables de desarrollar los procedimientos y estándares adecuados para tal efecto, así como también de realizar pruebas de forma periódica que garanticen la recuperación de los datos. Cada respaldo realizado deberá verificarse para certificar que la información fue grabada apropiadamente.

Cada procedimiento debe considerar la frecuencia de respaldo, los medios de almacenamiento, tipo de contenido, tiempo de almacenamiento y borrado, entre otros. Lo anteriormente descrito en el mismo procedimiento de Respaldo y Recuperación del Servicio Nacional de Menores (SGSI.PR.20).

2.1 PROTECCIÓN A LOS MEDIOS DE RESPALDO

Cuando las condiciones lo permitan y para prevenir daños y pérdida accidental de activos de información crítica o sensible, estos activos serán respaldados en un dispositivo destinado específicamente para este propósito y para fines propios de la institución.

En concordancia con el párrafo precedente, se establece en la presente política que el uso de los dispositivos queda reducido o determinado a las funciones propias del servicio.

El Subdepartamento de Informática evaluará los factores determinantes sobre la obsolescencia de los medios magnéticos u ópticos de respaldo y determinará el correcto proceder para mantener la disponibilidad de dichos respaldos considerando la seguridad en la reutilización o descarte de equipos.

2.2 PROTECCIÓN DE LA INFORMACIÓN EN MEDIOS DE RESPALDO

En medida de lo posible el Subdepartamento de Informática deberá establecer el lugar de almacenamiento del respaldo, en una ubicación remota, un nivel mínimo de información de respaldo, junto con registros exactos y completos de las copias de respaldos y los procedimientos documentados de restablecimiento. Ésta instalación deberá ser emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. El nivel mínimo de información será definido por el Comité de Seguridad de la Información, en conjunto con el Subdepartamento de Informática. En ámbitos críticos para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo. Lo anteriormente descrito en el mismo procedimiento de Respaldo y Recuperación del Servicio Nacional de Menores (SGSI.PR.20).

El respaldo de datos y software crítico se debe almacenar en un lugar protegido con acceso controlado, o mediante algún producto de Software adecuado al efecto.

Cuando las condiciones lo permitan toda información crítica grabada en respaldos que son almacenados fuera de la institución, deben ser trasladados con elementos de seguridad adecuados, ya sea utilizando métodos de encriptación o utilizando métodos apropiados para prevenir intentos de acceso físico no autorizado, dicha

ubicación estará en un radio no menor de 5 kilómetros de distancia de la Dirección Nacional del Servicio .

El Subdepartamento de Informática, del nivel central debe mantener un inventario actualizado de la información almacenada externamente. Lo anteriormente descrito en el mismo procedimiento de Respaldo del Servicio Nacional de Menores (SGSI.PR.20).

2.3 VIGENCIA Y RETENCIÓN DE LOS RESPALDOS

La retención de los respaldos de información debe ajustarse a lo señalado en la circular N°051, del 09 de febrero del 2009, sobre disposiciones y recomendaciones referentes a conservación, transferencia y eliminación de documentos, de la Dirección de Bibliotecas, Archivos y Museos DIBAM.

2.4 INFORMACIÓN RELEVANTE CONTENIDA EN ESTACIONES DE TRABAJO, COMPUTADORES O LAPTOPS INSTITUCIONALES

Para ser coherente con la presente política, la información determinada como crítica de SENAME, no deberá almacenarse en estaciones de trabajo, computadores o laptop institucionales, menos en equipos personales.

Cualquier necesidad de traslado de información desde equipos locales a servidores o dispositivos de almacenamiento ubicados en el Datacenter del nivel central debe ser solicitada formalmente por el jefe de la División Administrativa respectiva, al Jefe del Subdepartamento de Informática justificando la criticidad de la información que solicitan trasladar.

2.5 MANTENCIÓN DE LA INFORMACIÓN CONTENIDA EN SERVIDORES

La información contenida en los servidores centrales de la institución que no sea relevante debe ser borrada, para lo cual el Subdepartamento de Informática debe levantar periódicamente un catastro con dicha información.

Todo equipo computacional o medio de almacenamiento instalado en la Dirección Nacional que sea dado de baja, debe ser examinado por el Subdepartamento de Informática del nivel central, en donde se debe llevar a cabo el mecanismo de borrado de información según el Procedimiento de 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 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

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de la información institucional considerados relevantes dentro del alcance, con el objeto de asegurar continuidad operacional de los procesos institucionales y servicios que desarrolla el SENAME, mediante el resguardo de los activos de la información considerados críticos asociados a los procesos de provisión de bienes y/o servicios de SENAME.

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 actualización de esta Política de Respaldo y Recuperación en la Institución y así asegurar que el SGSI logre sus resultados esperados.

- **DEPARTAMENTO DE PLANIFICACIÓN Y CONTROL DE GESTIÓN**

  El Departamento de Planificación y Control de Gestión será el encargado de identificar y mantener una matriz actualizada de aquella información que es necesaria para mantener operativos sus procesos, durante eventuales procedimientos de restauración.

- **SUBDEPARTAMENTO DE INFORMÁTICA**

  Gestionar los respaldos y definir el estándar de éste de los servidores y equipos de hardware, que detalle los respaldos de software básico, de las aplicaciones, configuraciones de servicio y de los datos en ambiente de producción, autorizar las solicitudes de respaldo especiales.

  Deberá coordinar, ejecutar y velar por la realización de las pruebas y restauración de las copias de respaldo efectuadas utilizando las herramientas pertinentes para tales efectos.

  Determinar la periodicidad de las pruebas de restauración, Mantener un inventario de los activos de información sobre los que se realiza copia de seguridad y gestionar la mantención y capacidad de Infraestructura que permita mantener la operatividad de los procesos de SENAME.

- **ADMINISTRADORES DE SISTEMAS**

  Solicitar respaldo y/o restauración según la necesidad que se requiera y los recursos disponibles, realizar pruebas y validar que la actividad se realice.

  Velar por el adecuado funcionamiento de las herramientas de Control de Versiones de Software de respaldo, validando la veracidad y confiabilidad de los respaldos que se realizan en materias de desarrollo de aplicaciones.

Mantener una adecuada identificación de la información crítica en colaboración con el encargado de riesgos.

- **ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN**
  Auditar al menos una vez al año los registros de respaldo y su correcto proceder.
  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. Además, es responsable de publicar y dar a conocer nuevas versiones del documento.

- **PERSONAL DE 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 Respaldo y Recuperación de Información al interior del SENAME es del (la) Director(a) Nacional del Servicio.

El Subdepartamento de Informática o la Unidad de Comunicaciones de SENAME, apoyarán la difusión de las políticas y procedimientos utilizando las herramientas y plataformas que estime conveniente para tal efecto.

Los funcionarios, proveedores de servicios y personal externo, tendrán acceso a esta Política en su última versión vía Intranet institucional y página web del servicio, en formato digital.

7 CUMPLIMIENTOS

La presente Política de Respaldo y Recuperación de Información entra en vigencia una vez oficializada por el (la) Director(a) Nacional del SENAME. Las jefaturas de los distintos departamentos pertenecientes al Proceso de 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 Respaldo y Recuperación 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

- **Datacenter**: Es un centro de procesamiento de datos, una instalación empleada para albergar un sistema de información de componentes.
- **Hardware**: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
- **Log de servidor**: Uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste.
- **Sitio de respaldo**: Lugar físico en el cual se implementará el sitio de contingencia.
- **Software**: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.