SENAME
Ministerio de Justicia y Derechos Humanos
Gobierno de Chile

GAB/JLS/RVS/JBT/HGC

TRAMITADO

SERVICIO NACIONAL DE MENORES OFICINA DE PARTES

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

RESOLUCIÓN EXENTA Nº 2339

SANTIAGO, 17 NOV 2016

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 581, de 2016, 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; en la Resolución Exenta N° 2283, de 11 de noviembre de 2016, de la Dirección Nacional del SENAME; en la Resolución Nº 1600, de 2008, 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 del 12 de enero de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos y la Norma Chilena Oficial NCh-ISO 27001:2013 que proporciona un marco de gestión de Seguridad de la Información utilizable en cualquier tipo de organización, pública o privada.

4º. Que, con fecha 11 de noviembre de 2016, se dictó Resolución Exenta N°2283, de la Dirección Nacional del SENAME, que aprobó la Política General del Sistema de Gestión de Seguridad de la Información.

5º. Que, en el marco de la aludido Sistema de Gestión de Seguridad de la Información, se han emitido las siguientes Políticas, las cuales requieren la debida aprobación por parte de la Dirección Nacional:

- SGSI.PO.02 Política de Escritorios y Pantallas Limpias
- SGSI.PO.03 Política de Gestión de Redes
- SGSI.PO.04 Política de Control de Acceso
- SGSI.PO.05 Política de Respaldo y Recuperación de Información
- SGSI.PO.06 Política de Ubicación y Protección del equipamiento
- SGSI.PO.07 Política de Perímetro de Seguridad Física
- SGSI.PO.08 Política Acuerdo de Relación con Proveedores

6º. Que, por la extensión de los documentos singularizados en el considerando precedente, estos constan en documentación anexa a la presente resolución, entendiéndose formar parte integrante de la misma para todos los efectos legales.

2304/16
1213.

RESUELVO:

1° APRUÉBANSE las Políticas integrantes del Sistema de Gestión de Seguridad de la Información del SENAME, las que constan de documentos anexos a la presente resolución, entendiéndose formar parte integrante de la misma para todos los efectos legales, los que se individualizan a continuación:

- SGSI.PO.02 Política de Escritorios y Pantallas Limpias
- SGSI.PO.03 Política de Gestión de Redes
- SGSI.PO.04 Política de Control de Acceso
- SGSI.PO.05 Política de Respaldo y Recuperación de Información
- SGSI.PO.06 Política de Ubicación y Protección del equipamiento
- SGSI.PO.07 Política de Perímetro de Seguridad Física
- SGSI.PO.08 Política Acuerdo de Relación con Proveedores

2° OBSÉRVENSE las Políticas aprobadas a través del presente acto administrativo por todos los funcionarios, incluyendo al personal de planta, contrata y honorarios y en general a cualquier persona o empresa que preste servicios o se encuentre contratado por este Servicio, teniendo en consideración los parámetros establecidos por la Política General del Sistema de Gestión de Seguridad de la Información, aprobada por Resolución Exenta N°2283, de la Dirección Nacional del SENAME, por lo que el alcance de las mismas se encuentra supeditado al alcance de la referida Política General, establecido en el punto 3.1 de su texto, siendo por tanto aplicables a los activos de información, activos físicos, activos de Servicios TI y activos humanos asociados al proceso de desarrollo de la oferta, de líneas de acción de la Ley N° 20.032, realizados en la Dirección Nacional del SENAME.

3° PUBLÍQUESE la presente resolución en el sitio web institucional del SENAME, a fin que sea difundido a los funcionarios y a terceros.

ANÓTESE Y COMUNÍQUESE.

SERVICIO NACIONAL DE MENORES
DIRECTORA NACIONAL

SOLANGE HUERTA REYES
DIRECTORA NACIONAL
SERVICIO NACIONAL DE MENORES

Distribución:
- Dirección Nacional.
- Departamento de Planificación y Control de Gestión
- Departamento Jurídico.
- Oficina de Partes.

POLÍTICA DE RESPALDO Y RECUPERACION 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 00	ELABORADO POR	REVISADO POR	APROBADO POR
Nombre	**Jose Luis Toledo** Encargado Sistema de Gestión de Seguridad de la Información	**Cristian Castillo Silva** Jefe Departamento de Planificación y Control de Gestión	**Solange Huerta Reyes** Directora Nacional
Fecha	7/11/2016	7/11/2016	10 NOV 2016
Firma			

SERVICIO NACIONAL DE MENORES UNIDAD DE INFORMATICA

SERVICIO NACIONAL DE MENORES Jefe Depto. de Planificacion y Control de Gestión

SERVICIO NACIONAL DE MENORES DIRECTORA NACIONAL KSA

Control de Versiones

Nombre		Fecha	Dpto.
Elaboró	José Luis Toledo	7/11/2016	Encargado de Seguridad de la Información
Revisó	Cristian Castillo Silva	7/11/2016	Jefe Departamento Planificación y Control de Gestión

Registro de Modificaciones (*)				
Revisión		**Nombre /Dpto Emisor**	**Descripción de la Modificación**	**Aprobó**
Nº	**Fecha**			
00	7/11/2016	DEPLAE	Emisión	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

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 que sus divisiones o departamentos necesitan 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).

SENAME determinará la mejor plataforma de procesamiento de datos, considerando para aquello los factores que se consideren relevantes para su decisión.

La División de Informática deberá considerar soluciones de respaldo para servidores y aplicaciones (códigos fuentes, 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. La división 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 división 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 del Servicio Nacional de Menores (SGSI.PR.11),

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, en el caso de que existiere, para abarcar el sitio de respaldo, considerando lo establecido en las Políticas de Perímetro de Seguridad Física (SGSI.PO.07) y la de Ubicación y Protección del Equipamiento (SGSI.PO.06).

La periodicidad, tipo y mecanismo de respaldo y recuperación de activos de información será definido por la División Informática de la Dirección Nacional, quienes serán los responsables de desarrollar los procedimientos y estándares adecuados para tal efecto.
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 del Servicio Nacional de Menores (SGSI.PR.11).

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.

La división 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 la División 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 la División 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 del Servicio Nacional de Menores (SGSI.PR.11).

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.

La División 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.11).

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, trasferencia 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 de la División 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 la Unidad 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 la División de Informática del nivel central, en donde se debe llevar a cabo el mecanismo de borrado de información según el Procedimiento para la Eliminación y Recuperación de Equipos (SGSI.PR.04).

2.6 DOCUMENTOS RELACIONADOS

2.6.1 Política General de Seguridad de la Información de SENAME (SGSI.PO.01).
2.6.2 Política de Perímetro de Seguridad Física (SGSI.PO.07).
2.6.3 Política de Ubicación y Protección del Equipamiento (SGSI.PO.06).
2.6.4 D.S. N°83 DEL 12/01/2004. Aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
2.6.5 NCH-ISO27001: Tecnología de la información.
2.6.6 Procedimiento de Seguridad en la Reutilización o Descarte de Equipos (SGSI.PR.21).
2.6.7 Procedimiento de Mantenimiento del Equipamiento (SGSI.PR.16)

3. DEFINICIÓN

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.

4. OBJETIVOS

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. ROLES Y RESPONSABILIDADES

5.1 DIRECTOR(A) NACIONAL DE SENAME

En su calidad de tal, tiene la responsabilidad de garantizar la implementación efectiva de 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 respaldo y Recuperación de Información,* en toda la Institución y así asegurar que el, Sistema de Gestión de Seguridad de la Información, ahora en adelante SGSI, logre su(s) resultado(s) esperado(s).

5.2 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 sus divisiones o departamentos necesitan para mantener operativos sus procesos, durante eventuales procedimientos de restauración.

5.3 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.

5.4 ADMINISTRADORES DE SISTEMAS/JEFES DE PROYECTO

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 (para los desarrollos internos), 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 coordinador y/o encargado de riesgos.

5.5 ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN

Auditar al menos una vez al año los registros de respaldo y su correcto proceder.

5.6 JEFATURAS DE DIVISIONES ADMINISTRATIVAS

Velar por la correcta aplicación de la presente política.

5.7 RESPONSABLE DEL DOCUMENTO

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. Además, es responsable de publicar y dar a conocer nuevas versiones del documento.

5.8 PERSONAL DE 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 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, variación de los costos de los controles, impacto de los incidentes de seguridad, cambios legislativos, entre otros.

La responsabilidad de la validación y difusión de la Política de respaldo y recuperación al interior del SENAME es del (la) Director(a) Nacional del Servicio.

Los funcionarios, proveedores de servicios y la ciudadanía, tendrán acceso a esta Política en su última versión vía Pagina Web del servicio, en formato digital. Además, será comunicada a través de memorándum a todos los departamentos de la Dirección Nacional.

Los proveedores de Servicio de Tecnologías de Información que presten Servicios a la Institución, deberán garantizar por escrito su respeto y cumplimiento de las Políticas de Seguridad de la Información de SENAME.

7. CUMPLIMIENTO

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 las distintas divisiones administrativas 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

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Datacenter: Es un centro de procesamiento de datos, una instalación empleada para albergar un sistema de información de componentes.

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.