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 CONTROLES CRIPTOGRÁFICOS SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

SGSI.PO.14

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	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 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 CONTENIDOS

1 INTRODUCCIÓN

La presente política se genera con el fin de garantizar la confidencialidad e integridad de los documentos designados como sensibles. El Servicio Nacional de Menores debe utilizar sistemas y técnicas criptográficas para la protección de la información.

El sistema de información debe implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares, guías aplicables, así como:

- Proporcionar una protección adecuada a los equipos utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
- Proteger las claves secretas y privadas evitando sean copiadas o modificadas sin autorización

2 POLÍTICA

2.1 USO DE CONTROLES CRIPTOGRÁFICOS

- En primera instancia se deberá identificar a la(s) persona(s) responsable(s) de implementar la política, así como de su debida administración y la gestión de claves.
- Se debe realizar una evaluación de riesgos, cuyo resultado permitirá identificar el nivel de cifrado requerido para la información que se maneje, según su clasificación. Esta evaluación estará reflejada en la Matriz de Riesgos.
- Se utilizarán controles criptográficos para la protección de la confidencialidad, el cumplimiento del principio de la no repudiación y el control de la integridad de la información en los siguientes casos: protección de claves de acceso a sistemas, documento electrónico, datos y servicios; transmisión de información clasificada fuera del ámbito del servicio; resguardo de información, cuando así surja de la evaluación de riesgos realizada por el propietario de la información y el encargado de seguridad de la información.
- Se definen los algoritmos de cifrado que podrán utilizarse al interior del SENAME, como aplicación directa o como parte de la configuración de otros productos de seguridad comerciales, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas
- Sólo se utilizan algoritmos de cifrado, definidos por estándares internacionales.
- Se utilizarán técnicas criptográficas para autenticar a los usuarios o entidades externas que requieran hacer uso de los sistemas de información del SENAME.
- Se utilizarán mecanismos criptográficos para el establecimiento de canales seguros para comunicaciones, tales como SSL/TLS (HTTPS) incluyendo el uso y gestión de llaves y certificados digitales.
- Toda información contenida o transportada a través de medios móviles o extraíbles deberá contar con un código de protección, según el nivel de clasificación que tengan los datos incluidos, con el fin de resguardar los antecedentes registrados en dichos medios.
- Los funcionarios deben usar el sistema autorizado por el SENAME para efecto de autenticación.

2.2 GESTIÓN DE CLAVES CRIPTOGRÁFICAS

- El encargado de seguridad de la información deberá precisar el equipo que se utilizará para la generación, almacenamiento y archivo de las claves de encriptación.

- Los responsables de generación de claves criptográficas serán los únicos encargados de generar, difundir y archivar los códigos de acceso para archivos y equipos encriptados. Toda solicitud o requerimiento de encriptación deberá ser realizado al encargado de administración de claves.
- La administración de claves criptográficas es responsabilidad única del Subdepartamento de Informática.
- Cada clave criptográfica deberá tener un ciclo de vida, el cual dependerá del nivel de complejidad de la misma y la clasificación de la información o equipo que se desea proteger, pudiendo tener un período de expiración de horas o días. Se definirán las fechas de activación y desactivación para cada clave generada.
- Todas las claves criptográficas deberán estar protegidas contra modificación, divulgación y destrucción. Dichas acciones podrán ser realizadas únicamente por los administradores de claves.
- El SENAME se encargará de abastecer los recursos necesarios para garantizar la protección y seguridad del equipo utilizado para generar, almacenar y archivar las claves criptográficas, tomando en consideración los respaldos correspondientes y resguardando el acceso a estos.

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

Esta política define el uso de algoritmos de encriptación y servicios de protección de información a utilizar en el Servicio Nacional de Menores

5 RESPONSABILIDADES

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

- **SUBDEPARTAMENTO DE INFORMÁTICA**
  - Autorizar formalmente los métodos de encriptación a utilizar en las aplicaciones y sistemas tecnológicos.

- Asistir y administrar los procedimientos de configuración de los controles criptográficos.
- Administrar las claves criptográficas

- **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 y sus objetivos de negocio.
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 éste siempre actualizado. Junto con lo anterior, es responsable de gestionar la publicación y dar a conocer nuevas versiones del documento.

- **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.

- **PERSONAL DE SENAME Y/O USUARIOS PERTENECIENTES AL PROCESO DE DESARROLLO DE LA OFERTA**

Tendrán la responsabilidad de cumplir con lo formalizado en este documento y cautelar el cumplimiento de las medidas control del uso de controles criptográficos

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 Controles Criptográficos al interior del SENAME es del (la) Director(a) Nacional del Servicio, quien se apoyará para estos propósitos en las Jefaturas.

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 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 de Controles Criptográficos (SGSI.PO.14) 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:

- **Cifrado:** Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave (llave criptográfica) necesaria para descifrarlos.
- **Cifrar:** Es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) que transforma la información, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta
- **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.
- **Llaves criptográficas**: Son códigos (algoritmos) que se generan de forma automática y se guarda en un directorio especial durante la instalación. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

- **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.