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 GESTIÓN DE

REDES

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

SGSI.PO.03

Información del Documento

REV 00	Elaborado por:	Revisado por:	Aprobado por:
Nombre	**Jose Luis Toledo** Encargado Sistema de Gestión de la Seguridad de la información	**Cristian Castillo Silva** Jefe Departamento Planificación y Control de Gestión	**Solange Huerta Reyes** Directora Nacional
Fecha	07/11/2016	07/11/2016	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	07/11/2016	Encargado de Seguridad de la Información
Revisó	Cristian Castillo Silva	07/11/2016	Jefe Departamento Planificación y Control de Gestión

Registro de Modificaciones (*)				
Revisión		**Nombre/Dpto. Emisor**	**Descripción de la modificación**	**Aprobó**
Nº	**Fecha**			
00	07/11/2016	DEPLAE	Emisión	DIRECCIÓN NACIONAL

(*) 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 CONTENIDO

1. INTRODUCCIÓN

La presente política se establece en el marco del Sistema de Gestión de Seguridad de la Información, con la finalidad de administrar y controlar el acceso a las redes del Servicio, garantizando la seguridad de la información en red y la protección de los usuarios conectados.

2. POLÍTICA

2.1 ACCESO A LA RED

Para el acceso a la red interna del Servicio Nacional de Menores, así como a la red de servidores productivos, la nube *azure*, o entornos de laboratorio por parte de personal definido en el punto 3. Definición, la jefatura directa o encargado de proyecto por parte de SENAME debe solicitar a la Unidad de informática la autorización de acceso indicando el tipo de permiso y la duración de este.

El acceso no autorizado a la red de SENAME debe ser informado por el funcionario encargado del área TI o por el funcionario que tenga conocimiento de ello en forma inmediata al comité de seguridad de la información.

Según el lineamiento, el profesional encargado de redes y comunicaciones, es responsable de definir las pautas a seguir con el fin de garantizar la seguridad de los servicios de red con los que cuenta el servicio nacional de menores.

Para el cumplimiento de lo señalado se procederá de acuerdo a lo siguiente:

- Mantener instalados y habilitados en la red solo aquellos servicios y/o aplicaciones que sean utilizados, según lo indicado en el procedimiento Gestión de Redes SGSI.PR.19.
- Controlar el acceso lógico a los dispositivos de comunicaciones, tanto como a la consola de administración, como lo establece el procedimiento de Gestión de redes SGSI.PR.19.
- Controlar el acceso físico a los dispositivos de comunicaciones, manteniendo con llave el acceso a estos dispositivos.

2.2 DIAGRAMA DE RED

El Servicio Nacional de Menores deberá contar con un sistema jerárquico de dispositivos de red organizados según las buenas prácticas, los cuales se mencionan a continuación:

- Núcleo
- Distribución
- Acceso

El encargado de red será el responsable de mantener los diagramas de red actualizados y almacenados en un lugar de acceso controlado, y una vez al año se generará un registro para el sistema de seguridad de la información, con el diagrama de red en aquel momento, como lo establece el procedimiento de Gestión de redes SGSI.PR.19.

2.3 MECANISMOS DE SEGURIDAD

Para mantener la confidencialidad, integridad y disponibilidad de la información se dispondrá de diferentes tipos de mecanismos de protección:

- FIREWALL

  El firewall de la Dirección Nacional contará con zonas definidas donde se restringe el acceso desde el exterior (internet) a la red interna. En la red interna se encuentran los servicios web con autenticación y que pueden ser solicitados desde la red lan y wan. El Firewall deberá gestionarse según lo descrito en el procedimiento de administración de Firewall en el documento SGSI.PR.13.

- SEGURIDAD DE INTERFACE

  Los dispositivos de comunicaciones de la capa de acceso serán controlados mediante bloqueo de dirección Mac y todas las interfaces no operativas estarán apagadas. Dicho control se realizará según lo descrito en el Procedimiento de Gestión de Redes SGSI.PR.19

- SEGMENTACIÓN DE LA RED

  La red del Servicio Nacional de Menores deberá contar con segmentación de redes para todos sus recursos de red, servidores, administración, acceso. Dicha segmentación, se encontrará definida en el Anexo 4 del Procedimiento de acceso a redes SGSI.PR.19

2.4 UTILIZACIÓN DE LA RED WIFI

La red wifi del Servicio Nacional de Menores estará restringida y controlada por un dispositivo especializado, el cual define 2 formas de acceso las cuales son:

2.4.1 WIFI INSTITUCIONAL

- Todos los directivos, Jefes de departamento, sub-departamento y unidad tendrán acceso a la red wifi institucional.
- Solo personal autorizado por su Jefatura directa podrá tener acceso a la red wifi institucional siempre que su utilización sea estrictamente para fines institucionales.
- El acceso a esta red, deberá gestionarse según el procedimiento de mesa de ayuda TI, descrito en el procedimiento SGSI.PR.19

2.4.2 WIFI VISITA

- Todos los visitantes y Funcionario de la Dirección Nacional del Servicio Nacional de Menores podrán tener acceso a la red wifi de visita, previa evaluación por parte de la unidad de informática.
- El acceso a esta red, deberá gestionarse según el procedimiento de mesa de ayuda TI, descrito en el procedimiento SGSI.PR.19.

3. DEFINICIÓN

Esta política se aplica a todos los funcionarios (planta, contrato, honorarios) de la Dirección Nacional del Servicio y trabajadores externos, que sean usuarios de las distintas redes institucionales, y que intervengan en el proceso de Desarrollo de la Oferta.

El administrador de redes y comunicaciones será el encargado de gestionar la aplicación de las directrices definidas en esta política.

4. OBJETIVOS

La unidad informática del Servicio Nacional de Menores, en función y bajo el marco de la Política General de Seguridad, establece ciertos controles a nivel de red, con el fin de salva guardar el acceso, la integridad, la disponibilidad y la confiabilidad de la misma, aplicando niveles de seguridad a nivel de red.

El profesional de redes y comunicaciones de la unidad informática, es el responsable de la restricción de los accesos a usuarios individualizados en la definición de esta política.

5. ROLES Y RESPONSABILIDADES

5.1 DIRECTOR(A) NACIONAL

- 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 en toda la Institución y así asegurar que el SGSI logre su(s) resultado(s) esperado(s).

5.2 PROFESIONAL DE REDES Y COMUNICACIONES

- Gestionar proyectos para satisfacer necesidades del negocio dentro de los parámetros acordados, incluyendo costos, duración, calidad y riesgos, generando documentación, informes de gestión y reportes técnicos.
- Gestionar servicios a usuarios para asegurar la calidad acordada, contribuyendo a las especificaciones, el desarrollo la investigación, la aplicación y evaluación de las normas de servicio a usuarios para resolver o derivar problemas.
- Diseñar redes según requerimientos, creando esquemas y especificaciones de sistemas y equipos definiendo arquitecturas, topologías y procedimientos de configuración con sus respectivos procedimientos de implementación.

- Proveer servicios de soporte técnico de red, administrando el proceso y verificando las solicitudes de soporte, además de utilizar software e instrumentos de gestión para investigar y diagnosticar problemas de red y colaborar con los usuarios del servicio nacional de menores en la resolución de problemas y solicitudes técnicas.

5.3 JEFATURA DE DEPARTAMENTO DE PLANIFICACION Y CONTROL DE GESTIÓN (DEPLAE)

- Tendrá la responsabilidad de revisar la política en cada una de sus versiones.

5.4 ENCARGADO DE SEGURIDAD

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. Alinear 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.
4. Mantener coordinación con otras dependencias de la Institución para apoyar los objetivos de la seguridad de la información.

5.5 COMITÉ DE SEGURIDAD

Tendrá la responsabilidad de gestionar la Política de Seguridad de la Información dentro del SENAME, a través de la ejecución de las siguientes funciones:

1. Supervisar la implementación de procedimientos y estándares que se desprenden de la política general de seguridad de la información.
2. Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para implementar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas.
3. Arbitrar conflictos en materias de seguridad de la información y sus riesgos asociados, además de proponer soluciones.

4. Coordinarse con los Comités de Calidad y de Riesgos de la Institución, para mantener alineamiento y estrategias comunes de gestión.
5. Reportar a la alta dirección respecto de oportunidades de mejora en el Sistema de Gestión de Seguridad de la Información (SGSI), así como de los incidentes relevantes en esta materia y su solución.

Dicho comité debe estar integrado por lo menos por los siguientes funcionarios:

- Jefe de Operaciones o TI
- Jefe de Recursos Humanos
- Encargado de Calidad
- Encargado de Riesgos
- Asesor Jurídico
- Jefes de Áreas funcionales o encargados de procesos
- Encargado de Seguridad de la Información

5.6 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.

5.7 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 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, 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 Seguridad de la Información al interior del SENAME es del (la) Director(a) Nacional del Servicio, quien se apoyará para estos propósitos en los Equipos Directivos de las Unidades Operativas a nivel nacional.

Los funcionarios tendrán acceso a esta Política en su última versión vía Intranet en formato digital y será comunicado 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 la presente Política de Seguridad de la Información.

7. CUMPLIMIENTO

La presente Política entra en vigencia una vez oficializada por el (la) Director(a) Nacional del SENAME. Las jefaturas de los distintos departamentos, subdepartamentos y unidades 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 lo dispuesto en esta Política constituye una falta sancionable y podrá resultar en medidas disciplinarias definidas por el comité de seguridad de la información y que serán informadas directamente por la Unidad de Informática.

9. TÉRMINOS Y DEFINICIONES

A los efectos de este documento, se aplican las siguientes definiciones:

- **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.
- **Confidencialidad**: Protección de la información sensible ante divulgación no autorizada.
- **Integridad**: Exactitud, configuración y calidad de un activo de información.
- **Disponibilidad**: Preservación de un activo de información y acceso a personas autorizadas a su uso.
- **Activos de Información:** Corresponde a todos aquellos elementos relevantes involucrados en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de valor para la Institución.
- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información:** Se refiere al hardware y software operados por la Institución o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Institución, sin considerar la tecnología utilizada, ya sea se trate de procesamiento de datos, telecomunicaciones o de cualquier otro tipo.
- **Confiabilidad de la Información**: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **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.
- **Comité de Seguridad de la Información:** Cuerpo integrado por representantes de todas las áreas sustantivas de la Institución, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas en el ámbito de la seguridad de la información.

- **Encargado de Seguridad de la Información:** Persona que cumple la función de implementación, cumplimiento y control de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la Institución que así lo requieran.
- **Documento Electrónico:** Es un documento cuyo soporte material es algún tipo de dispositivo electrónico o magnético, y en el que el contenido está codificado mediante algún tipo de código digital, que puede ser leído, interpretado, o reproducido, mediante el auxilio de detectores de magnetización.
- **Redes:** es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos.