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 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 02 | Elaborado por: | Revisado por: | Aprobado por: |
|---|---|---|---|
| **Nombre** | **Hector Burgos Cañete**<br>Encargado Sistema de Gestión de Seguridad de la Información | **Cristian Castillo Silva**<br>Jefe Departamento Planificación y Control de Gestión | **Susana Tonda Mitri**<br>Directora Nacional |
| **Fecha** | 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 | 07 NOV. 2016 | DEPLAE | Emisión | DIRECCIÓN NACIONAL |
| 01 | 13 OCT. 2017 | DEPLAE | • Cambios en formato, tipo de letra, tamaño, interlineado / (Todo el documento) | DIRECCIÓN NACIONAL |
| 02 | 06 DIC. 2019 | DEPLAE | • Actualización de Sección 2.1 y 4, incluyendo al encargado de seguridad de la información como responsable<br>• Modificación de la sección 5<br>• Actualización del alcance del documento<br>• Renombramiento de Unidad de Informática por Subdepartamento de Informática (Todo el Documento) | 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. La jefatura directa o encargado de proyecto por parte de SENAME debe solicitar al Subdepartamento 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 encargado de seguridad de la información.

Según el lineamiento, el profesional encargado de redes y comunicaciones y el encargado de seguridad de la información, son responsables 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 gestión 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 del Subdepartamento 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 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 del 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 OBJETIVOS

El Subdepartamento de 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 del Subdepartamento de Informática en conjunto con el encargado de la seguridad de la información, son responsables de la restricción de los accesos a usuarios individualizados en la definición de esta política.

## 5 RESPONSABILIDADES

### 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.

### 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 Gestión de Redes en toda 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 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 implantación 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 DEL 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, 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 Gestión de Redes al interior del SENAME es del (la) Director(a) Nacional del Servicio.

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, proveedores de servicios y personal externo, 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 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 Gestión de Redes 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:

- **Activos de Información:** Corresponde a todos aquellos elementos relevantes involucrados en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de valor para la Institución.
- **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.
- **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.
- **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.
- **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.
- **Redes:** es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos.
- **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.
- **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.