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.

19865

- 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 GENERAL

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

SGSI.PO.01

Información del Documento

REV 03	Elaborado por:	Revisado por:	Aprobado por:
Nombre	**Hector Burgos Cañete** Encargado Sistema de Gestión de la Seguridad de la información	**Cristian Castillo Silva** Jefe Departamento Planificación y Control de Gestión	**Susana Tonda Mitri** Directora Nacional
Fecha	06/12/2019 C 6 DIC. 2019	06/12/2019 C 6 DIC. 2019	C 6 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	C 6 DIC. 2019	Encargado Sistema de Gestión de la Seguridad de la Información
Revisó	Cristian Castillo Silva	C 6 DIC. 2019	Jefe Departamento Planificación y Control de Gestión

Registro de Modificaciones (*)				
Revisión N°	Revisión Fecha	Nombre/Dpto. Emisor	Descripción de la modificación / (Página o sección afectada)	Aprobó
00	31 MAR. 2016	DEPLAE	Emisión	DEPLAE
01	C 1 SEP. 2017	DEPLAE	• Mejoras en el formato / (Todo el documento) • Cambio Directora Nacional / (Información del documento) • Aumento de controles de anexo, debido al informe de brechas comprometido en 2015 y al compromiso de cumplimiento del 2017 / (ANEXO N°1) • Modificación del Alcance / (Sección 3.1) • Inclusión Documentos Relacionados / (Sección 2.1) • Inclusión en política de ámbitos de aplicación de política / (Sección 2) • Especificación de decreto 83 en documentos relacionados, se incluye norma técnica NCh-ISO 27002 en	DIRECCIÓN NACIONAL

			documentación relacionada, se eliminan documentos asociados a la elaboración de documentación y control de registros. / (Sección 2.1) • Se elimina al encargado de calidad de los integrantes del comité. / (Sección 5) • Mejoras en el formato / (Todo el documento) • Se complementan responsabilidades de la dirección para cumplir control A.07.02.01 / (Sección 5) • Se incluyen aspectos de difusión para cumplimiento control A.7.2.2(Sección 6)	
02	C 7 JUN. 2018	DEPLAE	• Se incluye rol y validación de Jefaturas para cumplimiento de control 18.2.2 / (Secciones 5 y 6). • Actualización por resolución N° 0778 del Manual del DEPLAE de la Unidad de Informática a "Subdepartamento de Informática" / (Todo el documento). • Inclusión de Anexo 2 Controles comprometidos 2018. / Sección Anexos • Modificación de Alcance para incluir los controles comprometidos en el año 2018. / (Sección 3)	DIRECCIÓN NACIONAL
03	C 6 DIC. 2019	DEPLAE	• Inclusión de Anexo 3 Controles comprometidos 2019. / Sección Anexos • Modificación de Sección 9 definición de activos humanos • Eliminación del Comité de Calidad dentro de las responsabilidades. • Se elimina sección 2.1 • Modificación de cargos en las responsabilidades del Comité de Seguridad de la Información • Modificación de medidas requeridas por medidas de sensibilización (Último párrafo página 6) • Modificación del cuarto objetivo específico para alinearlo con alcance de la Política. • Modificación de garantizar la implementación por revisar, aprobar y controlar la implementación efectiva (Responsabilidades de Directora Nacional)	DIRECCIÓN NACIONAL

	C 6 DIC. 2019		• Se elimina último párrafo que habla de un canal de denuncias anónimas el cual no existe. • Se complementa la responsabilidad 3 del encargado del SGSI: riesgos asociados a seguridad de la información y ciberseguridad • Se modifica otras dependencias por otros departamentos en responsabilidad 3 del encargado del SGSI • Se modifica gestionar por revisar y aprobar en las responsabilidades del comité de SGSI • Se modifica implantación por implementación en responsabilidad 2 del comité SGSI • Se modifica el punto 4 de las responsabilidades del Comité SGSI, sustituyendo Mantener alineamiento por abordar. • Se modifica el punto 5 de las responsabilidades del Comité SGSI, sustituyendo relevantes por de alto impacto. Su solución por mitigación • Se actualiza el listado de integrantes del Comité, según última Resolución Exenta • Se modifica la palabra publicar por gestionar publicación (Sección Responsable del documento) • Se añade Unidad de comunicaciones en sección de apoyo de difusión de Políticas, ya que la administración de la página web Sename está a cargo de un profesional de esta unidad. • Se modifica el título Jefaturas por Jefaturas de Departamentos Pertenecientes al Proceso de Desarrollo de la Oferta • Se sustituye la palabra respeto por acato en sexto párrafo sección Revisión, validación y difusión. • Se sustituye "las regulaciones" por leyes y normativas asociadas a seguridad de la información (Primer párrafo sección 8) • Se sustituye "Política de sistema de gestión " por Política General de	

	C 6 DIC. 2019		Seguridad de la Información (Segundo párrafo sección 8) • Se ordenan los términos y definiciones alfabéticamente	

(*) 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 CONTENIDOS

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 gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Institución.

Esta política general, las políticas específicas y procedimientos de seguridad asociados, utilizarán como marco de referencia los requerimientos del D.S. N° 83/2004, del Ministerio Secretaría General de la Presidencia (Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confiabilidad de los documentos electrónicos) y las buenas prácticas definidas en la Norma Chilena NCh-ISO 27001:2013, la que adicionalmente constituirá el marco rector de todas las iniciativas de seguridad adoptadas por SENAME.

2. POLÍTICA DEL SGSI

La alta dirección de SENAME, a través su Departamento de Planificación y Control de Gestión, se compromete a establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma NCh-ISO 27001:2013.

Este Sistema de Gestión de Seguridad de la Información le ofrece al SENAME la capacidad de proteger, preservar y administrar, la confidencialidad, integridad y disponibilidad de la información de la institución, salvaguardando la precisión de la misma a través de:

a) Servicios de redes, contenidos y aplicaciones soportadas en las plataformas apropiadas protegiendo los mecanismos de tratamiento, almacenamiento y comunicación.

b) Personal competente y comprometido con una cultura de seguridad reflejada en la aceptación y aplicación de las directrices establecidas.

c) El cumplimiento de las disposiciones legales y regulatorias emitidas por los diferentes organismos.

Para estos efectos, se llevará a cabo un proceso de análisis de riesgos y, de acuerdo a su |resultado, se implementarán acciones de mitigación, con el fin de tratar aquellos que sean considerados críticos para el servicio de acuerdo al alcance definido del SGSI.

Por lo anterior, SENAME identificará, valorará, tratará y monitoreará los riesgos asociados con la operación de sus tareas, y de sus activos de la información, asegurando el eficiente cumplimiento de las funciones sustantivas de la entidad apoyada en una adecuada gestión de dichos riesgos, mediante la aplicación de los controles consignados en el Anexo A del estándar NCh-ISO 27001:2013.

SENAME además implementará las medidas de sensibilización para la formación y toma de conciencia de sus colaboradores y partes interesadas en todos los aspectos relacionados con la seguridad de la información y del SGSI. A su vez, cuando los funcionarios y/o las terceras partes interesadas incumplan la presente política de seguridad de la información o con las políticas derivadas de ella, la alta dirección se reserva el derecho de aplicar las medidas disciplinarias vigentes en la institución dentro del marco legal aplicable, y dimensionadas al impacto que tengan sobre la institución.

3. ALCANCE DEL SGSI

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 intervengan en el proceso de "Desarrollo de la Oferta", y los sistemas controlados serán los siguientes:

- Active Directory
- SENAINFO

Los controles pertenecientes a la Norma Chilena Nch-ISO 27001:2013, que aborda el Sistema de Gestión de Seguridad de la Información, se enuncian en Anexo gde esta Política.

4. OBJETIVOS DEL SGSI

4.1 OBJETIVO GENERAL

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 SENAME, mediante el resguardo de los activos de la información críticos asociados a los procesos del negocio y su soporte, gestionados a través de un Sistema de Gestión de Seguridad de la Información.

4.2 OBJETIVOS ESPECIFICOS

- Proteger y resguardar la información, de acuerdo a la consideración e identificación de los riesgos que pudieran materializarse sobre los activos de la información y las instalaciones de procesamiento de ésta, a través de una adecuada evaluación de los mismos, de forma de entender las vulnerabilidades y las amenazas a las cuales están expuestos.
- Asignar recursos necesarios para el establecimiento, implementación y mejora continua del sistema de gestión de la seguridad de la información.
- Establecer mecanismos de auditoría y control de los activos de la información y tecnologías de procesamiento.
- Comunicar, sensibilizar e informar sobre los lineamientos de seguridad de la información a los(as) funcionarios(as) del Proceso de Desarrollo de la Oferta del SENAME.

5. RESPONSABILIDADES DEL SGSI

- **DIRECTOR(A) NACIONAL DEL 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 General de Seguridad de la Información en toda la Institución y así asegurar que el SGSI logre sus resultados esperados.

  La alta dirección debe exigir a todos los funcionarios y personal externo que apliquen y cumplan la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.

- **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 y con entidades externas 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:** Tendrá la responsabilidad de revisar y aprobar las Políticas 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 implementación de los controles necesarios para ejecutar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas.
3. Colaborar con la solución de riesgos materializados en materias de seguridad de la información.
4. Coordinarse con el Comité de Riesgos de la Institución, para abordar 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 de alto impacto en esta materia y su mitigación.
   Dicho comité debe estar integrado por los siguientes funcionarios:
   - Jefe(a) Departamento de Gestión y Desarrollo de Personas
   - Jefe(a) Departamento de Planificación y Control de Gestión

- Jefe(a) Departamento de Administración y Finanzas
- Jefe(a) Departamento de Adopción
- Jefe(a) Departamento Técnico Protección y Restitución de Derechos
- Jefe(a) Departamento de Justicia Juvenil
- Jefe(a) Departamento Jurídico
- Jefe(a) Unidad de Comunicaciones
- Encargado 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.

- **JEFATURAS DE DEPARTAMENTOS PERTENECIENTES AL PROCESO DE DESARROLLO DE LA OFERTA:** Tienen la responsabilidad de revisar el cumplimiento de las Políticas y Procedimientos, asociadas a seguridad de la información dentro de su área de responsabilidad.

6. REVISIÓN, VALIDACIÓN Y DIFUSIÓN DEL SGSI

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 General de Seguridad de la Información 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.

Las Jefaturas donde hay responsabilidad sobre políticas y/o procedimientos acordes al "Listado Maestro de Documentos - R01.SGSI.PR.01" revisarán al menos una vez al año la documentación del SGSI y sus verificadores a fin de garantizar su cumplimiento.

Los proveedores de Servicio de Tecnologías de Información que presten Servicios a la Institución, deberán garantizar por escrito su acato y cumplimiento de la presente Política de Seguridad de la Información.

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. CUMPLIMIENTO

La presente Política General de Seguridad de la Información 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 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 General 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

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, tales como: Datos Digitales, Activos Tangibles, Activos Intangibles, Software, Sistemas Operativos.

- **Activos de Servicios TI:** Corresponde a todos los soportes que se requiere el sistema TI, tales como: Servicios de autentificación, Servicios de Red.

- **Activos Físicos:** Corresponde a todos aquellos elementos físicos relevantes, tales como: Infraestructura TI, Hardware de TI, Controles del entorno TI.

- **Activos Humanos:** Corresponde al personal que interviene en los procesos definidos en el alcance, estos son Empleados y Personal Externo.

- **Autenticidad**: Validez de la información en origen, tiempo, forma y distribución.

- **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.

- **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.

- **Criticidad**: Nivel de riesgo que presenta una amenaza para la seguridad de un activo de información.

- **Disponibilidad**: Preservación de un activo de información y acceso de 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.

- **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.

- **Evaluación de Riesgos:** Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la Institución.

- **Gestión de Riesgos:** Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Este proceso es cíclico y debe llevarse a cabo en forma periódica.

- **Incidente de Seguridad:** Un incidente de seguridad es un evento adverso que se produce al interior de la Institución, que compromete la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

- **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.

- **Legalidad**: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la Institución y las personas.

- **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 Gestión de Seguridad en la Información (SGSI):** El SGSI es el diseño, implementación, mantenimiento de un conjunto de procesos y políticas para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información.

- **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.

ANEXO

CONTROLES COMPROMETIDOS 2017

Cláusula	Enumeración de controles	Objetivo / Controles
A.5 Políticas de Seguridad de la Información	A.5.1	**Objetivo : Orientación de la dirección para la Seguridad de la Información**
	5.1.1	Política para la seguridad de la información
	5.1.2	Revisión de las políticas de Seguridad de la Información
A.6 Organización de la Seguridad de la Información	A.6.1	**Objetivo: Organización Interna**
	6.1.1	Roles y responsabilidades de la seguridad de la información
	6.1.2	Segregación de funciones
	6.1.3	Contacto con las autoridades
	A.6.2	**Objetivo: Dispositivos móviles y trabajo remoto**
	6.2.1	Política de dispositivos móviles
A.7 Seguridad ligada a los Recursos Humanos	A.7.1	**Objetivo: Previo al empleo**
	7.1.1	Selección
	A.7.2	**Objetivo: Durante el empleo**
	7.2.1	Responsabilidades de la dirección
	7.2.2	Concientización, educación y formación en seguridad de la información
A.8 Administración de Activos	A.8.1	**Objetivo: Responsabilidad por los activos**
	8.1.1	Inventarios de activos
	8.1.2	Propiedad de los activos
	8.1.3	Uso aceptable de los activos
	8.1.4	Devolución de activos
	A.8.2	**Objetivo: Responsabilidad por los activos**
	8.2.1	Clasificación de la información
	8.2.2	Etiquetado de la información
	8.2.3	Manejo de Activos
	A.8.3	**Objetivo: Manejo de los medios**
	8.3.1	Gestión de los medios removibles
	8.3.2	Eliminación de los medios
	8.3.3	Transferencia física de medios
A.9 Control de acceso	A.9.1	**Objetivo: Requisitos de negocio para el control de acceso**
	9.1.1	Política de control de acceso
	A.9.2	**Objetivo: Gestión de acceso del usuario**
	9.2.1	Registro y cancelación de registro de usuario
	9.2.2	Asignación de acceso de usuario
	9.2.3	Gestión de derechos de acceso privilegiados
	9.2.5	Revisión de los derechos de acceso de usuario

	9.2.6	Eliminación o ajuste de los derechos de acceso
	A.9.3	**Objetivo: Responsabilidades del usuario**
	9.3.1	Uso de información de autenticación secreta
	A.9.4	**Objetivo: Control de acceso al sistema y aplicaciones**
	9.4.1	Restricción de acceso a la información
	9.4.2	Procedimientos de inicio de sesión seguro.
	9.4.3	Sistema de gestión de contraseñas
A.11 Seguridad Física y del Ambiente	A .11.1	**Objetivo: Áreas Seguras**
	11.1.1	Perímetro de seguridad física
	11.1.2	Controles de acceso físico
	A.11.2	**Objetivo: Equipamiento**
	11.2.1	Ubicación y protección del equipamiento
	11.2.4	Mantenimiento del equipamiento
	11.2.7	Seguridad en la reutilización o descarte de equipos.
	11.2.8	Equipo de usuario desatendido
	11.2.9	Política de escritorio y pantalla limpios
A.12 Seguridad de las Operaciones	A.12.1	**Objetivo: Procedimientos operacionales y responsabilidades**
	12.1.1	Procedimientos de operación documentados
	12.1.2	Gestión de cambios
	12.1.3	Gestión de la capacidad
	12.1.4	Separación de los ambientes de desarrollo, prueba y operacionales
	A.12.2	**Objetivo: Protección contra código malicioso**
	12.2.1	Controles contra códigos maliciosos
	A.12.3	**Objetivo: Respaldo**
	12.3.1	Respaldo de información
	A.12.4	**Objetivo: Registro y Monitoreo**
	12.4.4	Sincronización de relojes
	A.12.5	**Objetivo: Control de Software de operación**
	12.5.1	Control del software operacional
A.13 Seguridad de las Comunicaciones	A.13.1	**Objetivo: Gestión de la Seguridad de red**
	13.1.1	Controles de red
	13.1.2	Seguridad de los servicios de red
	13.1.3	Separación en las redes
	A.13.2	**Objetivo: Transferencia de Información**
	13.2.3	Mensajería electrónica
A.15 Relaciones con el Proveedor	A.15.1	**Objetivo: Seguridad de la Información en las relaciones con el Proveedor**
	15.1.1	Política de seguridad de la información para las relaciones con el proveedor

	15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor
A.16 Gestión de incidentes de Seguridad de la Información	A.16.1	**Objetivo: Gestión de incidentes de seguridad de la información y mejoras**
	16.1.1	Responsabilidades y procedimientos
	16.1.2	Informe de eventos en la seguridad de la información
	16.1.3	Informe de las debilidades de seguridad de la información
	16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información
	16.1.5	Respuesta ante incidentes de seguridad de la información
A.18 Cumplimiento	A.18.1	**Objetivo: Cumplimiento con los requisitos legales y contractuales**
	18.1.1	Identificación de la legislación vigente y los requisitos contractuales.
	18.1.3	Protección de los registros.
	18.1.4	Privacidad y Protección de la información de identificación personal.

CONTROLES COMPROMETIDOS 2018

Cláusula	Enumeración de controles	**Objetivo /** Controles
A.6 Organización de la Seguridad de la Información	A.6.1	**Objetivo: Organización Interna**
	6.1.4	Contacto con grupos de especial interés
A.7 Seguridad ligada a los Recursos Humanos	A.7.1	**Objetivo: Previo al empleo**
	7.1.2	Términos y condiciones de la relación laboral
	A.7.2	**Objetivo: Durante el empleo**
	7.2.3	Proceso disciplinario
	A.7.3	**Objetivo: Desvinculación y cambio de empleo**
	7.3.1	Responsabilidad del cese o cambio
A.9 Control de acceso	A.9.1	**Objetivo: Requisitos de negocio para el control de acceso**
	9.1.2	Acceso a las redes y a los servicios de la red
	A.9.2	**Objetivo: Gestión de acceso del usuario**
	9.2.4	Gestión de información secreta de autenticación de usuarios
A.11 Seguridad Física y del Ambiente	A .11.1	**Objetivo: Áreas Seguras**
	11.1.3	Seguridad de oficinas, salas e instalaciones
	11.1.4	Protección contra las amenazas externas y de origen ambiental
	A.11.2	**Objetivo: Equipamiento**
	11.2.5	Retiro de activos
A.13 Seguridad de las Comunicaciones	A.13.2	**Objetivo: Transferencia de Información**
	13.2.1	Políticas y procedimientos de intercambio de información
	13.2.2	Acuerdos de intercambio
	13.2.4	Acuerdos de confidencialidad
A.14 Adquisición, desarrollo y mantenimiento del sistema	A.14.1	**Objetivo: Requisitos de seguridad de los sistemas de información**
	14.1.1	Análisis y especificación de los requisitos de seguridad
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas
	14.1.3	Protección de las transacciones de servicios de aplicación
	A.14.2	**Objetivo: Seguridad en procesos de desarrollo y soporte**
	14.2.1	Política de desarrollo seguro

	14.2.2	Procedimientos de control de cambios
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
	14.2.4	Restricciones a los cambios en los paquetes de software
	14.2.5	Principios de ingeniería de sistema seguro
	14.2.6	Entorno de desarrollo seguro
	14.2.7	Externalización del desarrollo de software
	14.2.8	Prueba de seguridad del sistema
	14.2.9	Prueba de aprobación del sistema
A.16 Gestión de incidentes de Seguridad de la Información	A.16.1	**Objetivo: Gestión de incidentes de seguridad de la información y mejoras**
	16.1.6	Aprendizaje de los incidentes de seguridad de la información
A.18 Cumplimiento	A.18.2	**Objetivo: Revisiones de seguridad de la información**
	18.2.1	Revisión Independiente de la Seguridad de la Información.
	18.2.2	Cumplimiento con las políticas y normas de seguridad.
	18.2.3	Revisión de cumplimiento técnico.

CONTROLES COMPROMETIDOS 2019

Cláusula	Enumeración de controles	Objetivo / Controles
A.6 Organización de la seguridad de la información	A.6.1	**Objetivo: Organización interna**
	A.6.1.5	Seguridad de la información en la gestión de proyecto
	A.6.2	**Objetivo: Dispositivos móviles y trabajo remoto**
	A.6.2.2	Trabajo remoto
A.9 Control de acceso	A.9.4	**Objetivo: Control de acceso al sistema y aplicaciones**
	A.9.4.4	Uso de programas utilitarios privilegiados
	A.9.4.5	Control de acceso al código fuente de los programas
A.10 Criptografía	A.10.1	**Objetivo: Controles Criptográficos**
	A.10.1.1	Política sobre el uso de controles criptográficos
	A.10.1.2	Gestión de claves
A.11 Seguridad física y del ambiente	A.11.1	**Objetivo: Áreas seguras**
	A.11.01.05	Trabajo en áreas seguras
	A.11.01.06	Áreas de entrega y carga
	A.11.2	**Objetivo: Equipamiento**
	A.11.2.2	Elementos de soporte

	A.11.2.3	Seguridad en el cableado
	A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones
A.12 Seguridad de las operaciones	A.12.4	**Objetivo: Registro y monitoreo**
	A.12.4.1	Registro de evento
	A.12.4.2	Protección de la información de registros
	A.12.4.3	Registros del administrador y el operador
	A.12.6	**Objetivo: Gestión de la vulnerabilidad técnica**
	A.12.6.1	Gestión de las vulnerabilidades técnicas
	A.12.6.2	Restricciones sobre la instalación de software
	A.12.7	**Objetivo: Consideraciones de la auditoría de los sistemas de información**
	A.12.7.1	Controles de auditoría de sistemas de información
A.15 Relaciones con el proveedor	A.15.1	**Objetivo: Seguridad de la información en las relaciones con el proveedor**
	A.15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones
	A.15.2	**Objetivo: Gestión de entrega del servicio del proveedor**
	A.15.2.1	Supervisión y revisión de los servicios del proveedor
	A.15.2.2	Gestión de cambios a los servicios del proveedor
A.16 Gestión de incidentes de seguridad de la información	A.16.1	**Objetivo: Gestión de incidentes de seguridad de la información y mejoras**
	A.16.1.7	Recolección de evidencia
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	A.17.1	**Objetivo: Continuidad de la seguridad de la información**
	A.17.1.1	Planificación de la continuidad de la seguridad de la información
	A.17.1.2	Implementación de la continuidad de la seguridad de la información
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
	A.17.2	**Objetivo: Redundancias**
	A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información
A.18 Cumplimiento	A.18.1	**Objetivo: Cumplimiento con los requisitos legales y contractuales**
	A.18.1.2	Derechos de propiedad intelectual
	A.18.1.5	Regulación de los controles criptográficos
	A.18.2	**Objetivo: Revisiones de seguridad de la información**
	A.18.2.1	Revisión independiente de la seguridad de la información
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad
	A.18.2.3	Verificación del cumplimiento técnico