REF: APRUEBA DOCUMENTO DENOMINADO "POLÍTICA DE CIBERSEGURIDAD", DEL SERVICIO NACIONAL DE MENORES.

RES. EXENTA N° 1748

Santiago, a 29 SEP 2023

SERVICIO NACIONAL DE MENORES OFICINA DE PARTES

TRAMITADO

VISTOS:

Lo dispuesto en el Decreto Ley N° 2.465, de 1979, Ley Orgánica del Servicio Nacional de Menores, en el Decreto Supremo N° 356 de 1980, y en el Decreto Exento N° 2276, de 2022, ambos del Ministerio de Justicia y Derechos Humanos; en el Decreto con Fuerza de Ley N° 29 de 2004, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; la Norma NCh-ISO27001; el Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia; en la Resolución Exenta N° RA 263/818/2022, de 2022, del Servicio Nacional de Menores, y en la Resolución N° 07, de 2019, de la Contraloría General de la Republica.

CONSIDERANDO:

1º Que, el Servicio Nacional de Menores es el organismo del Estado que tiene por misión favorecer la reinserción social de adolescentes y jóvenes sujetos a medidas y sanciones en el marco de la ley de Responsabilidad Penal Adolescente de acuerdo a su etapa de desarrollo vital.

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, se entiende por Ciberseguridad todas aquellas acciones para la protección de los activos de información presente en el ciberespacio y en los diversos medios digitales, así como de la infraestructura que los soporta; que tiene por objeto evitar, mitigar, controlar o transferir los efectos adversos de sus riesgos, amenazas y vulnerabilidades que puedan exponer al Servicio Nacional de Menores (SENAME).

5º. Que, en el sentido anterior, SENAME debe acondicionar, adecuar su infraestructura crítica, adaptándola a la nueva política de Ciberseguridad, identificando sus activos críticos, infraestructura e información que circula por el ciberespacio para mantener su confidencialidad, integridad y disponibilidad. Además de establecer un marco general para el control y gestión de riesgos de ciberseguridad a lo que está expuesto el SENAME.

6º. Que, a fin de lograr lo anterior, el Servicio Nacional de Menores ha elaborado una Política de Ciberseguridad, la que se aprueba a través del presente acto administrativo.

902/23

RESUELVO:

1º APRUÉBASE el documento denominado **POLÍTICA DE CIBERSEGURIDAD,** del Servicio Nacional de menores, cuyo texto es el siguiente:

POLÍTICA DE CIBERSEGURIDAD
DPC.PO01

1. INTRODUCCIÓN

El Servicio Nacional de Menores (SENAME) es un organismo gubernamental centralizado y dependiente del Ministerio de Justicia y Derechos Humanos. 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:

- Contribuir al abandono de conductas delictivas de las personas jóvenes imputadas y de aquellas que cumplen sanciones, a través de una intervención especializada, oportuna y de calidad, de acuerdo con sus necesidades individuales garantizando el respeto irrestricto de sus derechos fundamentales.
- Mejorar el régimen de sanciones e internación de las personas adolescentes o jóvenes imputados por delitos y aquellas que cumplen sanciones de acuerdo a la Ley de Responsabilidad Penal Adolescente (LRPA), mediante el desarrollo de intervenciones con criterios de intersectorialidad e incorporación del enfoque de género.

SENAME acondicionará, adecuará su infraestructura crítica y adaptará a la nueva política de Ciberseguridad, identificando sus activos críticos, infraestructura e información que circula por el ciberespacio para mantener su confidencialidad, integridad y disponibilidad. Además de establecer un marco general para el control y gestión de riesgos de ciberseguridad a lo que está expuesto el SENAME.

Se entiende por Ciberseguridad todas aquellas acciones para la protección de los activos de información presente en el ciberespacio y en los diversos medios digitales, así como de la infraestructura que los soporta; que tiene por objeto evitar, mitigar, controlar o transferir los efectos adversos de sus riesgos, amenazas y vulnerabilidades que puedan exponer al Servicio Nacional de Menores (SENAME).

Esta política de ciberseguridad se enmarca en la SGSI.PO.01 política general del sistema de gestión de seguridad de la información, además 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), Ley Nº 21.459, de 20 de junio de 2022, Ministerio de Justicia y Derechos Humanos, Que establece normas sobre delitos informáticos, deroga la Ley Nº19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, sobre delitos informáticos, la actual Política Nacional de Ciberseguridad, las buenas prácticas definidas en la Norma Chilena NCh-ISO 27001, el Marco de Ciberseguridad NIST, Controles de Ciberseguridad CIS, y las directrices para la ciberprotección de la Norma Chilena NCh-ISO 27032, la que adicionalmente constituirá el marco rector de todas las iniciativas de ciberseguridad adoptadas por SENAME.

2. POLÍTICA DE CIBERSEGURIDAD

El equipo directivo de SENAME, a través del Departamento de Planificación y Control de Gestión, se compromete a establecer, implementar, mantener y mejorar de manera continua las directrices para la ciberprotección y velar por el cumplimiento del Sistema de Gestión de Ciberseguridad basado en la norma NCh-ISO 27032, Marco de

Ciberseguridad NIST, controles de Ciberseguridad CIS y en la política nacional de ciberseguridad.

Principios básicos

Para ello se establecen los siguientes principios básicos:

- Garantiza que los sistemas de información y telecomunicaciones que dispone SENAME posean el adecuado nivel de ciberresilencia.
- Sensibiliza a todos los funcionarios y colaboradores externos acerca de los riesgos de ciberseguridad y garantiza que disponen de los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para sustentar los objetivos de ciberseguridad de la Institución.
- Potencia las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las nuevas amenazas.
- Impulsa la existencia de mecanismos de ciberresilencia adecuados para los sistemas y operaciones gestionados por terceros que presten servicios a la Institución.
- Se dota de procedimientos y herramientas que permiten adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas.
- Colabora con los organismos y agencias gubernamentales relevantes para la mejora de la ciberseguridad de la Institución, el cumplimiento de la legislación vigente.

3. ALCANCE CIBERSEGURIDAD

El alcance de la presente política será aplicable a los activos críticos de información, activos humanos e infraestructura critica que los soporta y todo aquel que interactúe con estos.

Se aplica a todos los funcionarios (planta, contrata), trabajador a honorarios del SENAME, proveedores y colaboradores externos

4. OBJETIVOS CIBERSEGURIDAD

Los objetivos de la presente política están orientados a salvaguardar los activos críticos de información en el entorno físico, de red local y los que se encuentran interconectados a través de internet.

- Asegurar la Confidencialidad, Integridad y Disponibilidad de los activos de información a través de la ejecución de políticas, gestión de riesgo y aseguramiento informático de plataformas de tecnología de información.

- Definir e implementar controles del actual SGSI (sistema de gestión de seguridad de información) para mitigar ataques cibernéticos conocidos, a los que se encuentran expuestas las aplicaciones y plataformas IT de la organización.

- Planear y ejecutar un programa de auditoría para verificar la adecuada implementación de los controles de seguridad y ciberseguridad en las plataformas IT.
- Gestionar la vulnerabilidad técnica y tratar el riesgo asociado a través de los análisis de vulnerabilidades sobre las plataformas IT.

- Establecer contactos de la industria de la ciberseguridad para hacer frente a ataques de día cero.

- Comunicar, sensibilizar e informar sobre los lineamientos de ciberseguridad a los(as) funcionarios(as) del SENAME.

5. RESPONSABILIDADES CIBERSEGURIDAD

- **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. El equipo directivo 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 Ciberseguridad en toda la Institución y así asegurar que logre sus resultados esperados.

El equipo directivo 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 CIBERSEGURIDAD**

Tendrá la responsabilidad de coordinar las actividades relacionadas a Ciberseguridad

1. Gestionar la formulación y ejecución del plan estratégico de Ciberseguridad, en línea con los objetivos de la institución y conforme al marco normativo, legal y regulatorio, en conjunto con la NCh-ISO 27001 y NCh-ISO 27032.
2. Gestionar la adopción del marco normativo de ciberseguridad del SENAME por parte de terceros prestadores de servicios.
3. Asegurar el cumplimiento de la estrategia de Ciberseguridad definida por la organización, así como de las políticas, normas y procedimientos en este ámbito.
4. Desarrollar la cultura de Ciberseguridad y entregar los conocimientos que permitan identificar ciberamenazas que pongan en riesgo la información y los activos del SENAME.
5. Detectar las amenazas y gestionar los incidentes de Ciberseguridad de manera oportuna, con el objetivo de proteger la infraestructura, los servicios y operaciones del SENAME.
6. Maximizar el uso de las tecnologías de protección existentes e incorporar nuevas.
7. Proteger los datos y activos de información del SENAME de las ciberamenazas existentes, bajo los lineamientos del encargado de ciberseguridad y los resultados de los análisis de riesgo.
8. Definir y mantener la Arquitectura de Ciberseguridad del SENAME.
9. Adquirir y analizar información para identificar, rastrear, predecir y contrarrestar intenciones y actividades de ciberatacantes.
10. Apoyo en la gestión y control de fraudes.
11. Administrar y monitorear el correcto funcionamiento de las herramientas tecnológicas de seguridad implantadas en ambientes de tecnológicos.

- **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 Justicia Juvenil
- Jefe(a) Departamento Jurídico
- Encargado(a) de Seguridad de la Información

6. REVISIÓN, VALIDACIÓN, DIFUSIÓN CIBERSEGURIDAD

El Encargado de Ciberseguridad 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 Ciberseguridad 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, en inducción institucional a nuevos funcionarios a través del servicio de Aula Virtual, actividades desarrolladas por la Unidad de Formación Continua del Subdepartamento de Desarrollo Organizacional del SENAME.

El Subdepartamento de Modernización y Tecnología y 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.

7. CUMPLIMIENTO

La presente Política de Ciberseguridad 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 Ciberseguridad debe ser informado inmediatamente al encargado.

El incumplimiento de la Política de Ciberseguridad 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 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.

- **Ciberespacio:** Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ningún tipo de forma física.

- **Ciberseguridad:** Condición de estar protegido en contra de consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el Ciberespacio que se pueda considerar no deseable.

- **Ciberresilencia:** Es un concepto que engloba continuidad de negocio, seguridad de los sistemas de información y resiliencia de la organización. Es decir, se trata de un concepto que describe la capacidad de continuar generando los resultados previstos a pesar de experimentar sucesos cibernéticos complejos, como ciberataques, desastres naturales o recesiones económicas.

- **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.

- **Encargado de Ciberseguridad:** Persona que cumple la función de asegurar que el plan estratégico de ciberseguridad se lleve a cabalidad.

- **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.

- **Infraestructura crítica:** Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en el funcionamiento normal del servicio.

- **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.

- **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.

2° OBSÉRVESE la Política de Ciberseguridad del Servicio Nacional de Menores, aprobada a través del presente acto administrativo por todos los funcionarios y funcionarias, cualquiera sea su calidad jurídica (de planta, a contrata, a honorarios) del Servicio Nacional de Menores, proveedores y colaboradores externos, según los términos señalados en punto 3 de su texto.

4° DÉJASE SIN EFECTO toda otra versión anterior de Política de Ciberseguridad del SENAME, que hubiere sido aprobada con anterioridad.

ANÓTESE Y COMUNÍQUESE

SERVICIO NACIONAL DE MENORES
DIRECTOR NACIONAL

RACHID ALAY BERENGUELA
DIRECTOR NACIONAL(S)
SERVICIO NACIONAL DE MENORES

SSS/GBT/JSPDL/KVG/DDG/HGC
Distribución:
- Dirección Nacional
- Direcciones Regionales
- Departamentos, Subdepartamentos y Unidades de la Dirección Nacional del SENAME.
- Oficina de Partes