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 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

SGSI.PO.13

Información del Documento

REV 01	Elaborado por:	Revisado por:	Aprobado por:
Nombre	**Hector Burgos Cañete** Encargado Sistema de Gestión de la Seguridad de la	**Cristian Castillo Silva** Jefe Departamento Planificación y Control de Gestión	**Susana Tonda Mitri** Directora Nacional
Fecha	06/12/2019	06/12/2019	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		Nombre/Dpto. Emisor	Descripción de la modificación / (Página o sección afectada)	Aprobó
N°	Fecha			
00	C 1 OCT. 2018	DEPLAE	Emisión	DIRECCIÓN NACIONAL
01	C 6 DIC. 2019	DEPLAE	• Actualización de política (Secciones 2.4, 2.7 y 2.10. Se incluye a responsable de seguridad de la información en responsabilidades de aprobación y autorización)	DIRECCIÓN NACIONAL

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El Servicio Nacional de Menores asegurará que el software adquirido y desarrollado tanto por funcionarios de la institución, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de sistemas de información y el Departamento de Planificación y Control de Gestión incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

2 POLÍTICA

El Servicio Nacional de Menores se compromete a gestionar el desarrollo de software que permita asegurar el eficiente cumplimiento de los objetivos de la institución en materia de Sistemas de Información, bajo los siguientes lineamientos generales:

2.1. PROCESO DE CONSTRUCCIÓN/MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

- El proceso de construcción y/o mantenimiento de sistemas de información, debe contar con normas de programación, versionamiento, documentación y pruebas para cada etapa del ciclo de vida: especificación de requerimientos, diseño lógico y físico, pruebas, explotación.
- El ciclo de vida de la construcción y/o mantenimiento de sistemas de información debe incluir procedimientos de pruebas funcionales y no funcionales. Las pruebas no funcionales deben incluir las pruebas de seguridad.
- El proceso de construcción y/o mantenimiento de sistemas, así como los procesos de pruebas, deben efectuarse en ambientes dispuestos para ello.
- Los sistemas que inter operen o intercambien datos, con otros sistemas o base de datos, pertenecientes al SENAME, deben contar con controles de seguridad en ambos extremos de la comunicación.
- La responsabilidad del proceso de construcción y/o mantenimiento de sistemas, en particular la programación (codificación), debe tener siempre dos o más responsables de forma que no se detenga el proceso en periodos de vacaciones, licencias médicas o permisos laborales. Es decir, no debe depender una sola persona.
- El proceso de construcción y/o mantenimiento de sistemas de información tercerizados deben cumplir con esta política y con las normas que dicte el Comité de Seguridad de la Información a este respecto.

2.2. DOCUMENTACIÓN DE SISTEMAS DE INFORMACIÓN

- El acceso a la documentación de sistemas de información, bibliotecas de códigos fuentes y programas ejecutables, debe estar restringida sólo a funcionarios autorizados. La excepción a esta política, son los manuales de usuario, manuales de capacitación, u otros documentos destinados a los usuarios del o los sistemas de información.
- Toda la documentación asociada al ciclo de construcción y/o mantención de sistemas de información debe tener procedimientos de control de versionamiento.

2.3. ESPECIFICACIONES DE AMBIENTES DE DESARROLLO

Para cumplir con esta Política se debe realizar una separación de funciones entre los distintos ambientes involucrados. Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. A continuación, se presenta un modelo ideal formado por tres ambientes que debe ser adaptado a las características propias de la Institución, teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

2.3.1 AMBIENTE DE DESARROLLO

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir alguna fuente para modificar, quedando registrado en el sistema de control de versiones que gestiona el "administrador de programas fuentes" (Debe existir un rol para el sistema informático Senainfo y otro para el resto de las aplicaciones). El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

2.3.2. AMBIENTE DE PRUEBAS

El implementador de este ambiente recibe las librerías y/o ejecutables respectivos y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible. El testeador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctos de acuerdo a las especificaciones y considera que la documentación presentada es completa, remite las librerías y/o ejecutables al implementador de producción. En caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

2.3.3. AMBIENTE DE PRODUCCIÓN

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Las librerías y/o ejecutables se guardan almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

Deberían aplicarse procedimientos de la misma naturaleza y alcance para las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo:
modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos) deberían cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores. Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deberían tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos

realizados y monitorearlos en todo momento.

2.4. ESPECIFICACIONES DE REQUERIMIENTOS DE SEGURIDAD

- Para la construcción de nuevos sistemas de información o mejoras a los existentes, se debe especificar los controles de seguridad desde la etapa de levantamiento de requerimientos, tales como encriptación de claves, de mensajes, de configuración; auditoria de trazabilidad; entre otros.
- En la identificación de controles de seguridad deben participar las áreas de negocio que serán usuarios del sistema de información en construcción o proceso de mantención.
- El diseño e implementación de controles de seguridad, deben ser preferentemente de tipo automático, evitando procesos o intervención manuales. Las excepciones deben ser aprobadas por el Jefe del Subdepartamento de Informática y por el Encargado de Seguridad de la Información.
- En la etapa de diseño, debe considerarse los procedimientos necesarios para realizar revisiones periódicas de contenidos de campos, registros, tablas (de datos), o archivos considerados sensibles, frecuencia de los respaldos y tiempos de retención de estos, y procesos de depuración (limpieza de datos, indexaciones, u otros procesos relacionados con optimización y rendimiento).
- El acceso a las bases de datos de construcción, prueba y producción, deben contar con controles de acceso (autenticación y autorización). Debe definirse quiénes (roles) tienen acceso a las bases de datos en sus diferentes ambientes y qué tipo de acceso (consulta, actualización, eliminación). Jamás en la etapa de construcción y/o prueba se debe dar acceso a los datos de producción.

2.5 VALIDACIÓN DE DATOS DE ENTRADA Y SALIDA

- En términos generales, todo sistema que considere transformación de datos de entrada debe ser diseñada y construida considerando controles de integridad de éstos.
- Los sistemas que se construyan por los profesionales de Desarrollo del Servicio Nacional de Menores o por proveedores, y aquellos sistemas "paquetizados" que se adquieran, deben contemplar funcionalidades que permita acceder tanto a los registros de auditoría como a los registros de trazabilidad.
- Cuando un sistema tenga previsto el envío de datos (interoperabilidad) que contengan información clasificada como reservada, se debe implementar mecanismos de cifrado de los datos.

2.6. ENCRIPTACIÓN

- El dueño o propietario de la Información, en conjunto con el Encargado de Seguridad de la Información, evaluarán la necesidad de usar y aplicar tecnologías de encriptación para proteger información, las cuales están detalladas en la Política de Controles Criptográficos (SGSI.PO.14)

2.7. ADMINISTRACIÓN DE CLAVES

- La administración de cuentas y contraseñas de acceso a los sistemas de información, debe ser centralizada. Excepciones a esta política deben ser justificadas y autorizadas por el Jefe

del Subdepartamento de Informática y por el Encargado de Seguridad de la Información.

- El mecanismo o procedimiento de creación de grupos de usuarios, perfiles o privilegios, entre otros aspectos, deben preferentemente ser administrado en cada sistema de información. Excepciones a esta política deben ser autorizadas por el Jefe del Subdepartamento de Informática y por el Encargado de Seguridad de la Información.
- La solicitud de códigos de cuentas de acceso a los sistemas de información debe efectuarse según se establece en la Política de Control de Acceso y Perímetro de Seguridad Física (SGSI.PO.09).

2.8. CONTROL DE VERSIONES

- Toda la documentación, archivos ejecutables, códigos fuente y librerías de software de los sistemas construidos, script de bases de datos, así como la documentación de paquetes de software adquiridos, debe estar bajo procedimientos de control de cambios y de versionamiento.

2.9. CAMBIOS DE PLATAFORMA OPERATIVA

- Previo a cualquier cambio, actualización, o reconfiguración, planificada, en los servidores de aplicaciones, de bases de datos, u otros equipos asociados a la operación de sistemas de información, los profesionales del Departamento de Planificación y Control de Gestión deben efectuar un análisis y emitir un informe técnico que evalúe los impactos y riesgos que puedan generar estos cambios.

2.10 ADQUISICIÓN DE PAQUETES DE SOFTWARE

- En el proceso de análisis y adquisición de paquetes de software a terceros, deben considerarse aspectos y atributos de seguridad de la información, y el impacto en la seguridad frente eventuales cambios o modificaciones para su implantación en el Servicio Nacional de Menores.
- Las modificaciones a los paquetes de software o sistemas adquiridos a terceros, que surjan producto de su explotación y tengan relación con la seguridad de la información, deben ser aprobados por el Jefe del Subdepartamento de Informática y por el Encargado de Seguridad de la Información.
- Se prohíbe el uso y/o copia de cualquier paquete de software, por parte de los funcionarios del SENAME, del cual no se disponga de su respectiva licencia que lo autorice.

- La instalación de paquetes de software que son denominados "OPEN" deben ser autorizados por el Jefe del Subdepartamento de Informática con el objeto de validar si están dentro de los lineamentos de herramientas de software utilizados por el Servicio Nacional de Menores.

2.11 CAPACITACIÓN

- La puesta en producción de los Sistemas de Información, sean éstos construidos internamente o adquiridos a terceros, deben siempre considerar la realización de actividades de

capacitación dirigida a Usuarios Finales.

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) del Servicio a nivel nacional proveedores y trabajadores externos, que intervengan en el proceso de "Desarrollo de la Oferta y los sistemas controlados serán los siguientes:

- Active Directory
- SENAINFO

4 OBJETIVO

Definir las medidas y controles para la inclusión de inspecciones de seguridad en el proceso de construcción, mantenimiento, adquisición y explotación de sistemas de información.

5 RESPONSABILIDADES

5.1. DIRECTOR(A) NACIONAL DE SENAME

En su calidad de tal, tiene la responsabilidad de revisar y aprobar esta Política dentro de su área de competencia. 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 de Desarrollo Adquisición, Desarrollo y Mantenimiento de Sistemas en toda la Institución y así asegurar que el SGSI logre sus resultados esperados.

5.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

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

- Definir y dictar las políticas, estándares en tecnologías, seguridad de la información (integridad y confidencialidad) y su soporte tecnológico, velando por el cumplimiento de la normativa legal.
- Fijar el nivel de criticidad del sistema de información, y de identificar los controles de seguridad a aplicar para resguardarlos.
- Revisar, aprobar (o rechazar) procesos y controles tendientes a mitigar, eliminar, o transferir los riesgos relacionados con la construcción, mantención y adquisición de sistemas de información, y según corresponda, definir procedimientos para ello.
- Verificar el cumplimiento de los procedimientos y controles de seguridad establecidos para la construcción, mantención, y adquisición de sistemas de información.

5.3. 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:

- Tiene la responsabilidad de definir las normas, procedimientos y controles que permitan asegurar que los procesos de construcción y mantención de sistemas de información se apliquen los controles necesarios para la seguridad de la información de los mismos, tales como:
  - Metodología de análisis
  - Construcción de pruebas unitarias y de integración
  - Administración de sistemas
  - Administración de bases de datos
  - Documentación
  - Sistema de gestión de código

- Promover y verificar el cumplimiento de las políticas de seguridad que se señalan en este documento.
- Implementar, mantener, difundir y disponer los mecanismos de seguridad nativos, propios de las plataformas e infraestructura, con el fin de que estos sean utilizados por las aplicaciones que serán desarrolladas para operar sobre estas plataformas.
- Verificar y validar los requerimientos de seguridad que deben cumplir los paquetes de software ofertados en el mercado, independiente de cómo se realiza la adquisición por parte del Servicio Nacional de Menores.

5.4. PROFESIONALES DEL DEPARTAMENTO DE PLANIFICACIÓN Y CONTROL DE GESTIÓN

Tendrán la responsabilidad de cumplir con lo formalizado en este documento, asegurando que el entorno y proceso de desarrollo de software sean seguros y ejecutando las siguientes funciones:

- Diseñar, construir, documentar y dar mantenimiento a aplicaciones de sistemas de información utilizando herramientas de bases de datos y software de desarrollo de sistemas.
- Capacitar a usuarios en el uso de los sistemas de información institucional y otras herramientas.
- Instalar, dar mantenimiento y actualizar del Software Motor de Administración de Bases de Datos de la Institución y los diferentes servidores de base de datos

6 REVISIÓN, VALIDACIÓN Y DIFUSIÓN

El comité de Seguridad de la Información del Servicio revisará una vez al año la presente política, a efectos de mantenerla actualizada. Asimismo, efectuara 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 y/o normativos, entre otros.

La responsabilidad de la validación y difusión de la Política de Adquisición, Desarrollo y Mantenimiento de Sistemas 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, personal externo y proveedores de servicios, tendrán acceso a esta Política en su última versión vía Intranet y Pagina Web del servicio, en formato digital.

7 CUMPLIMIENTOS

La siguiente Política de Adquisición, Desarrollo y Mantenimiento de Sistemas entra en vigencia una vez sea oficializada por el (la) Director(a) Nacional del Servicio Nacional de Menores. 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 posterior a la fecha de publicación, sean estos directos o de empresas que prestan servicio, se deberá comunicar acerca de la existencia de dicha política, para el conocimiento y adherencia 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 Adquisición, Desarrollo y Mantenimiento de Sistemas (SGSI.PO.13) 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, dichas sanciones están contempladas en la Ley N°18.834 sobre estatutos Administrativos.

9 TÉRMINOS Y DEFINICIONES

- **Activo de Información:** Personas, Sistemas de información, aplicaciones o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información considerada relevante para los procesos de negocio del Ministerio de Obras Públicas o sus Servicios dependientes.
- **Base de datos**: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
- **Desarrollo de Software:** Crear una pieza de código que pueda ser procesado por una máquina para el cumplimiento de un objetivo específico trazado.
- **Paquete de Software:** Conjunto de aplicaciones informáticas diferentes pero relacionadas entre

sí que se distribuyen de forma conjunta.

- **Política**: Documento de alto nivel que declara los principios de la organización respecto a los requisitos, leyes, normativas y otros pertinentes para la Seguridad de la Información.
- **Procedimiento**: Documento que describe la realización de actividades respondiendo el qué, cómo, cuándo, dónde y por quién son realizadas estas actividades. Generalmente, su ejecución involucra a más de un área del Sistema de Gestión de Seguridad de la Información.