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.

19185

- 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 CONTROL DE ACCESO Y PERÍMETRO DE SEGURIDAD FÍSICA

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SENAME
Ministerio de Justicia y Derechos Humanos
Gobierno de Chile

SGSI.PO.09

Información del Documento

REV 01	ELABORADO POR	REVISADO POR	APROBADO POR
Nombre	**Hector Burgos Cañete** Encargado Sistema de Gestión de Seguridad de la Información	**Roberto Aguilera González** Jefe (S) Departamento de Planificación y Control de Gestión	**Susana Tonda Mitri** Directora Nacional
Fecha	1 DIC. 2019	13 DIC. 2019	
Firma			

Control de Versiones

Nombre		Fecha	Dpto.
Elaboró	Hector Burgos Cañete	13 DIC. 2019	Encargado Sistema de Gestión de Seguridad de la Información
Revisó	Roberto Aguilera González	13 DIC. 2019	Jefe (S) 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	DIRECCION NACIONAL
01	13 OCT. 2017	DEPLAE	• Se cambia en el punto de cumplimiento, la Política de aplicación ya que se encontraba errada. / (Sección 7) • Se fusionan las Políticas de control de acceso y perímetro de seguridad física. / (Sección 2) • Se fusiona la Política Control de Acceso SGSI.PO.04 en la presente política. / (Sección 2) • Se fusiona la Política acuerdo de relación con proveedores SGSI.PO.08 en la presente Política. / (Sección 2) • Se elimina documento de perímetro de seguridad física,	DIRECCION NACIONAL

	13 OCT. 2017		Memorándum 1384 del 29 de Julio del 2016, Resolución Exenta N° 1424 del 28 de julio de 2016, documento de elaboración de documentos, Política general por estar repetida y norma técnica de documentación relacionada. / (Sección 2.4) • Se cambia en la Política la palabra funcionario a cargo por subrogante para las solicitudes de acceso. / (Secciones 2.3.2 y 2.3.3) • Se complementan responsabilidades de jefes de proyecto. / (Sección 5) • Se adiciona ítem de ubicación y perímetro de seguridad física en la Política para fusionar y eliminar la PO.06. / (Sección 2.1) • Se incluyen aspectos de difusión para cumplimiento control A.7.2.2 (Sección 6)	
02	13 DIC. 2019	DEPLAE	• Se adiciona la designación de un administrador de sistema y dos suplentes para la asignación de cuentas de terceros (Sección 2.3.1) • Se añaden secciones 2.3.5 para dar cumplimento al control A.6.2.2 de la norma ISO 27001 • Se elimina la difusión de la Política a través de Memorándum. Actualización de equipos de protección de la sala de procesamiento en Sección 2.1	DIRECCION NACIONAL

(*) La presente versión sustituye completamente a todas las precedentes, de manera que el último des listado será el único documento válido de todos los registrados.

TABLA DE CONTENIDOS

1 INTRODUCCIÓN

La presente política se establece en el marco del Sistema de Gestión de Seguridad de la Información, con la finalidad de garantizar la protección física y lógica de los activos de la organización, mediante la definición del correcto uso de los espacios físicos para proteger las áreas que contienen la información y a las instalaciones de procesamiento de la información sensible o crítica evitando el acceso físico no autorizado, disminuyendo el riesgo de daños e interferencias de información y las instalaciones de procesamiento de información. También esta política regula la gestión de accesos a los sistemas, asignación y revisión de privilegios, y el uso de contraseñas de los diversos activos de información existentes en este Servicio, mediante la segregación de funciones.

2 POLÍTICA

El Servicio Nacional de Menores, implantará las medidas requeridas para el resguardo de la información por parte 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 Política de Seguridad de la Información de SENAME 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, sanciones y/o dimensionadas al impacto que tengan sobre la institución.

Se define como crítico, para resguardar la seguridad de la información del proceso de "Desarrollo de la Oferta", proteger la información contra posibles daños y aplicar controles de acceso en el ingreso al Datacenter y las áreas donde labora el personal de desarrollo de la oferta, para lo cual se debe determinar y definir los perímetros de seguridad, el emplazamiento y la ubicación de las áreas que contienen o manipulan información y también aquellos en donde se procesan.

Toda la información determinada con un nivel de confidencialidad alto acorde a la clasificación de la Planilla de Inventarios de activos de información (R01.SGSI.PR.10-01), deberá contar con copias de respaldo y seguridad en su acceso, de tal manera que se garantice que sólo el personal autorizado podrá tener acceso a la información.

Se debe asegurar que todo contrato, cuando sea pertinente, deba incluir cláusulas de seguridad necesarias para el resguardo de los intereses de la Institución. Junto con lo anterior y una vez establecido el vínculo y previo al inicio de los trabajos, garantizar, que los proveedores deban firmar una declaración, según lo descrito en el procedimiento de Privacidad y Protección de la Información de Identificación Personal (SGSI.PR.18).

Dicha declaración estará bajo la tutela del Encargado de Seguridad de la Información del servicio que debe ser firmada por éste y las partes involucradas.

2.1 UBICACIÓN Y PERIMETRO DE SEGURIDAD FÍSICA

La determinación de la ubicación y perímetros recaerá en los criterios evaluados por las divisiones administrativas competentes quienes resolverán la factibilidad e

idoneidad de dichos emplazamientos y ubicación, para ello podrán basarse en propuestas técnicas.

El perímetro de los edificios o lugares que contengan instalaciones de procesamiento de información, debe tener solidez física (ejemplo: no tendrá zonas que se puedan derribar fácilmente); los muros externos deben ser sólidos y todas las puertas exteriores deben estar protegidas contra accesos no autorizados, mediante mecanismos de control adecuados.

Para los equipos de procesamiento se debe tener en consideración:

- Que las instalaciones de los equipos de procesamiento de información (Estaciones de Trabajo) se deben ubicar cuidadosamente y estratégicamente para reducir el riesgo de que personas no autorizadas o ajenas a los procesos, la vean durante su uso.

Para la sala de procesamiento se debe tener en consideración:

- Mantener el equipamiento aislado de muebles, repisas u objetos que representen amenazas.
- La restricción visual, sobre todo a personas no autorizadas.

Para el presente propósito se determinan algunos aspectos mínimos relacionados al control de acceso con los cuales se debe contar para la protección de una sala de procesamientos, tales como:

- Acceso biométrico
- Instalación marco de acero para puerta de seguridad

2.2 ACCESO FÍSICO

La Sala de Procesamiento de Información del Servicio Nacional de Menores debe contar con controles de acceso que permitan evitar el acceso físico no autorizado.
Sala de Servidores: Dicha sala se debe encontrar aislada del resto de la oficina con paredes de material aislante, pintura ignífuga y puerta de seguridad. El acceso debe ser controlado por un dispositivo biométrico que valida el ingreso sólo del personal autorizado de la Unidad Informática.
Para las Áreas que posean activos de procesamiento de información, deben contar con recepción/secretaría quien registrará el acceso de la visita. En éstas áreas, se debe restringir el acceso de personas ajenas a SENAME. Durante su permanencia debe estar siempre acompañado por personal debidamente autorizado quien se responsabilizará por la supervisión de la visita.
En medida de lo posible, se deberán considerar sistemas que permitan proteger las áreas de procesamiento de la información y junto con ello de la correcta funcionalidad de los sistemas anteriormente descritos para cumplir con el objetivo para los cuales son implementados.

2.3 ACCESO LÓGICO

Para la protección de los accesos lógicos a las redes de SENAME y los activos de información definidos, se deberán cumplir las directrices relacionadas con cuatro

grandes temáticas, relativas a la segregación de usuarios, administración de cuentas, accesos privilegiados y gestión de contraseñas.

2.3.1 SEGREGACIÓN DE USUARIOS

Los usuarios en los sistemas deben ser segregados mediante perfiles de usuarios. Dichos perfiles han de ser definidos en consecuencia a la designación de la jefatura, y contener los mínimos accesos a los sistemas de información para llevar a cabo sus funciones.

Estos perfiles serán gestionados por cada administrador de sistema, utilizando las plataformas o herramientas que estén disponibles para su gestión. Por cada sistema se debe nombrar un administrador y dos suplentes que cumplan con sus funciones en caso de ausencia. En el caso del sistema SENAINFO el administrador de sistemas titular o suplentes son los únicos que pueden realizar la creación de cuentas a terceros. Los administradores de sistemas se encontrarán informados en los anexos del Procedimiento de gestión de accesos (SGSI.PR.23).

Las sesiones de los usuarios deberán ser gestionadas mediante un control apropiado de acceso, es decir, exigiendo nombre del usuario y contraseña, protector de pantalla con una contraseña protegida, bloqueo de pantalla automático en periodos de inactividad y control de acceso a los equipos conectados a la red. Para la implementación de aquellas medidas, será utilizada la plataforma Active Directory.

La segregación de funciones específica para cada sistema, estará definida en el Procedimiento de Gestión de Accesos, documento definido con el código SGSI.PR.23 dentro del Sistema de Gestión de Seguridad de la Información.

2.3.2 ADMINISTRACIÓN Y GESTIÓN DE CUENTAS DE USUARIOS

Las solicitudes de nueva cuenta de usuario o modificación de las mismas, podrán ser realizadas por jefaturas de personal de SENAME, particularmente jefes/as de departamento, sub departamento, unidad, directores/as regionales, directores/as de centro, Jefatura administrativa o técnicos, encargados/as de personal o el asignado como subrogante de dichos cargos.

Dicha solicitud debe ser realizada directamente al administrador del sistema de información correspondiente, según lo descrito en cada procedimiento de los diferentes sistemas.

La información mínima que deberá contener la solicitud debe ser:

- Nombre Completo: Nombres, Apellidos
- RUT: Cedula asignada por el Servicio de Registro Civil e Identificación
- Profesión: Profesión que posee el solicitante
- Teléfono: teléfono de contacto institucional
- Mail: Dirección de correo electrónico asignada
- Rol Designado: Rol que tendrá el usuario en el Sistema de Información

Las cuentas de usuarios serán personales e intransferibles, y las credenciales deberán ser tratadas con rigurosa confidencialidad, cambiándolas periódicamente.

La información sensible a la que puedan tener accesos los funcionarios mediante el uso de sus cuentas y credenciales, ha de ser tratada con el debido resguardo

establecido en la Política General de Seguridad de la Información, y la legislación vigente.

Se deberán usar cuentas de usuarios únicas para permitir a los usuarios vincularse y poder individualizar frente a posibles responsabilidades; solo se deben permitir el uso de cuentas grupales cuando sea necesario por operaciones particulares. Dichas cuentas grupales deben ser previamente aprobadas por la jefatura de la Unidad de Informática, según el Procedimiento de gestión de accesos (SGSI.PR.23). La información de autenticación es secreta, en el caso de las cuentas grupales solo podrá ser manejada por los miembros del grupo.

Los administradores de sistemas descritos en este alcance serán los responsables de mantener un registro formal de todas las personas registradas y los permisos asignados a cada sistema.

Para permitir una correcta gestión de las cuentas, el Departamento de Gestión y Desarrollo de Personas tiene la obligación de informar todas las desvinculaciones de los funcionarios de acuerdo al procedimiento establecido de desvinculación para el cierre de credenciales. El Subdepartamento de Informática administrará una lista de distribución que permita mantener informado de las desvinculaciones a todos los administradores de sistemas para proceder al cierre de las credenciales, como se establece en el Procedimiento de administración de activos (SGSI.PR.10).

2.3.3 GESTIÓN DE ACCESOS PRIVILEGIADOS

Las solicitudes de acceso privilegiado, podrán ser realizadas por jefaturas de SENAME, particularmente jefes/as de departamento, sub departamento, unidad, directores/as regionales, directores/as de centro, Jefatura administrativa o técnicos, encargados/as de personal o el asignado como subrogante de dichos cargos.

Los accesos privilegiados serán administrados por los encargados de cada sistema, y para cualquier usuario del Servicio, o trabajador externo, la creación de una cuenta de este tipo, deberá obedecer al Procedimiento de Gestión de Accesos (SGSI.PR.23), anexado a esta política.

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de estos, podría dar paso a incidentes de seguridad de la información dentro del Servicio.

Para evitar irrupciones no deseadas, los administradores de sistemas deben gestionar los privilegios de acuerdo a lo que se indica a continuación:

- Se identificarán los privilegios de cada sistema del alcance de esta política.
- Se asignarán privilegios a los funcionarios sobre la base de la necesidad de uso y dada una solicitud de la jefatura.
- Se otorgarán privilegios de acceso extraordinarios, previa autorización y justificación de quienes se describen anteriormente.

2.3.4 GESTIÓN DE CONTRASEÑAS

Las contraseñas para el acceso a las cuentas deberán ser creadas de acuerdo a lo establecido en el Procedimiento de Gestión de Contraseñas (SGSI.PR.17), y deberán considerar las directrices indicadas en el mismo documento.

2.3.5 TRABAJO Y ACCESO REMOTO

- En el Servicio Nacional de Menores no aplica la modalidad de Teletrabajo, las conexiones de trabajo remoto están permitidas con autorización de la jefatura.
- Solo podrán utilizar la modalidad de trabajo remoto en los sistemas del Servicio Nacional de Menores, aquellas personas con calidad jurídica planta y contrata que se encuentren prestando servicios a la institución. Adicionalmente podrá tener acceso remoto el personal de los proveedores que presten servicio a SENAME.
- Las conexiones de trabajo remoto realizadas por los funcionarios del SENAME desde otra red deben estar controladas de modo que se asegure la autentificación de los usuarios que accedan, la autorización para realizar dicho acceso, la confidencialidad de la información transmitida, la limitación de los recursos accedidos por el empleado y la supervisión de la misma. El procedimiento para conectarse a través de VPN está contemplado en SGSI.PR.23 - Procedimiento de Gestión de Accesos
- El servicio de acceso remoto debe ser provisto exclusivamente a través de una conexión por VPN segura. Se deben tomar los resguardos para que la conexión exija las credenciales del trabajador.
- El acceso remoto debe ser generado a través de un protocolo específico para el establecimiento de una VPN de manera directa entre el equipo que se conectará desde el exterior y el cortafuego (firewall) y los sistemas internos de la institución, proporcionando acceso a los recursos de la red de datos institucional.
- El notebook entregado al funcionario debe estar protegido frente a accesos no autorizados, contar con antivirus corporativo y antimalware. Adicionalmente, el funcionario debe garantizar la seguridad física de los equipos bajo su responsabilidad y se compromete a usarlos exclusivamente para actividades relacionadas con su trabajo. Dicho equipo debe ser facilitado a través de una ficha de entrega de equipo indicando la fecha de entrega, las especificaciones técnicas del mismo y los datos del funcionario, así como también del software instalado. Una vez concluidas las funciones o actividades del trabajador, el equipo deberá ser devuelto, emitiendo una ficha de devolución y revocando los accesos otorgados Estas fichas están contenidas en el Procedimiento de Administración de Activos de Información (SGSI.PR.10)
- Para evitar el acceso al equipo de personas no autorizadas que se encuentren en el recinto donde se realice el trabajo remoto se deberá entregar una normativa al trabajador, indicando las previsiones que debe tomar con el fin de evitar la amenaza del acceso no autorizado de terceros.
- El entorno de trabajo remoto físico debe considerar la seguridad lógica del equipamiento (dispositivos con antivirus licenciados y actualizados), una conexión a internet segura y la confidencialidad de la información manejada.
- Con el propósito de prevenir pérdida de información relevante para la institución, producto de robo o destrucción accidental del equipo computacional asignado al funcionario, en el transcurso del periodo que se trabaje bajo esta modalidad, toda la información que tenga relación con el trabajo que se está realizando deberá ser almacenada en una carpeta compartida, alojada en los servidores de la institución.
- El SENAME tendrá la responsabilidad de dar el debido mantenimiento y actualización tanto del software como del hardware del equipo, con el fin de prevenir posibles problemas que puedan poner en riesgo la confidencialidad de la

información que se maneje, esto a través de Servicios TI.

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

- Active Directory
- SENAINFO

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Controlar el acceso a los activos de información del Servicio, evitando el acceso físico no autorizado, daños e interferencias a la información de la organización e instalaciones de procesamiento de la información, con el fin de minimizar los riesgos de filtraciones o pérdidas de información bajo una correcta gestión de los espacios, usuarios, asignación y revisión de privilegios y el uso de contraseñas.

4.2 OBJETIVOS ESPECÍFICOS

- Definir las reglas de acceso a la información del Servicio.
- Restringir y controlar accesos privilegiados.
- Garantizar contraseñas seguras y de calidad.
- Acordar requisitos de seguridad de la información para mitigar riesgos asociados a accesos de los proveedores a los activos de la institución con el proveedor
- Establecer la incorporación, cuando sea pertinente, de cláusulas relacionadas a la seguridad de la información institucional, incluyendo las cláusulas de seguridad, confidencialidad, propiedad intelectual e integridad, en los acuerdos y contratos con terceros.

5 RESPONSABILIDADES

- **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, debiendo procurar además que se asignen suficientes recursos humanos, materiales y financieros para implementarla. La alta dirección debe establecer claramente el enfoque de la Política en línea con los objetivos institucionales y demostrar su apoyo y su compromiso con la seguridad de la información, promoviendo la mejora continua a través de la emisión y mantenimiento de esta *Política de Perímetro de Seguridad Física,* en toda la Institución y así asegurar que el, Sistema de Gestión de Seguridad de la Información, ahora en adelante SGSI, logre su(s) resultado(s) esperado(s).

- **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.

- **ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN**
  Alinea 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, además de monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos.
  Tiene que mantener la aplicabilidad de este documento acorde a las prácticas operacionales del SENAME, por lo que es responsable de generar las modificaciones necesarias para que esté siempre actualizado. Además, es responsable de gestionar la publicación y dar a conocer nuevas versiones del documento.

- **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.

- **SUBDEPARTAMENTO DE INFORMÁTICA**
  Deberá responsabilizarse de las siguientes actividades:
  - Mantener las condiciones de seguridad de acceso a los activos de información que estén bajo su responsabilidad, resguardando que los usuarios, tanto internos como proveedores sólo tengan ingreso a la información que requieran, dentro de los plazos establecidos.
  - Gestionar los accesos a los activos de información, privilegios de accesos y la gestión de contraseñas seguras.
  - Controlar y restringir el acceso a la sala de procesamiento de información y del perímetro de espacio físico de la División de Informática.
    Mantener un registro actualizado de los ingresos y salidas de personas externas y proveedores, ajenas a la Unidad de Informática.

- **DUEÑOS DE PROCESO/ADMINISTRADORES DE SISTEMAS/JEFES DE PROYECTO PERTENECIENTES AL DESARROLLO DE LA OFERTA**
  Sus responsabilidades incluyen:
  - Mantener las condiciones de seguridad de acceso a los activos de información que estén bajo su responsabilidad, resguardando que los proveedores sólo tengan ingreso a la información que requieran.
  - Gestionar los accesos a los activos de información, privilegios de accesos y la gestión de contraseñas seguras.

- Monitorear periódicamente los accesos a los activos de información.
- Recopilar los antecedentes y confeccionar la declaración de Aceptación de la Política General de Seguridad de la Información del Servicio Nacional de Menores y Visarla en conjunto con el encargado de Seguridad de la Información y la jefatura de Informática.
- Crear, administrar y eliminar las cuentas de usuarios y sus respectivas credenciales, en los momentos que corresponda, del sistema del cual es responsable (Administrador de Sistemas).
- Informar con anticipación a quien corresponda el vencimiento de plazos de acceso establecidos, con el fin de gestionar las solicitudes de prórrogas en caso de que fuere necesario, al igual que el término anticipado de contrato.

- **JEFATURAS DE DIVISIONES ADMINISTRATIVAS**

Responsable de mantener una adecuada identificación de la información crítica en colaboración con el coordinador y/o encargado de riesgos.
Velar por el correcto acceso físico y lógico, evitar daños e interferencias a la información de la organización y a los activos de procesamiento de información.
Gestionar el correcto control de acceso a las áreas críticas de su dependencia y el cumplimiento de acuerdos de confidencialidad cuando sea el caso.

6 REVISIÓN, VALIDACIÓN Y DIFUSIÓN

El Comité de Seguridad de la Información de la Institución revisará una vez al año la presente Política, a efectos de mantenerla actualizada. Asimismo, efectuará toda modificación que sea necesaria en función de posibles cambios que puedan afectar su definición, como, por ejemplo, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, cambios legislativos, entre otros.
La responsabilidad de la validación de la Política de Control de Acceso y Perímetro de Seguridad Física al interior del SENAME es del (la) Director(a) Nacional del Servicio.
El Subdepartamento de Informática de SENAME, apoyarán la difusión de las políticas y procedimientos utilizando las herramientas y plataformas que estime conveniente para tal efecto.
Los funcionarios y proveedores de servicios tendrán acceso a esta Política en su última versión vía Intranet institucional y página web del servicio.

7 CUMPLIMIENTO

La presente Política de Control de Acceso y Perímetro de Seguridad Física entra en vigencia una vez oficializada por el (la) Director(a) Nacional del SENAME. Las jefaturas de las distintas divisiones administrativas del servicio serán responsables de darlas a conocer a su personal subordinado.
Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá comunicar acerca de la existencia de la política, para conocimiento y acceso a la misma.

8 SANCIONES

Cualquier conflicto con las regulaciones debe ser informado inmediatamente al encargado de seguridad del SGSI.

El incumplimiento de la Política del sistema de Gestión 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

- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Confidencialidad**: Protección de la información sensible ante divulgación no autorizada.
- **Integridad**: Exactitud, configuración y calidad de un activo de información.
- **Disponibilidad**: Preservación de un activo de información y acceso a personas autorizadas a su uso.
- **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.
- **Sala de procesamiento de información:** Espacio físico determinado que contiene la infraestructura de procesamiento de información llamado también Datacenter.
- **Active Directory:** Herramienta de Microsoft utilizada por este Servicio para la administración de cuentas de usuario y casillas de correo electrónico.
- **Senainfo:** Sistema operacional institucional del Servicio Nacional de Menores.
- **Datacenter:** Estructura de servidores que almacenan la información generada por los usuarios del Servicio a través de carpetas compartidas.
- **Cuentas grupales de Active Directory:** se refiere a listas de distribución y carpetas compartidas en los Servidores del Datacenter.
- **VPN (Red Virtual Privada):** es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.