SENAME
Ministerio de Justicia

Gobierno de Chile

JMMB/JOB/GCT/JPMT/IRC

TRAMITADO

SERVICIO NACIONAL DE MENORES
OFICINA DE PARTES

**REF: DEJA SIN EFECTO ORDINARIO N° 3648/2010 Y APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO NACIONAL DE MENORES.**

**RESOLUCIÓN EXENTA N°** 03991

**SANTIAGO,** 30 SEP 2011

**VISTOS:** Lo dispuesto en el artículo 5 Nos 1, 12 y 13 del D.L. 2.465, de 1979; en los D.S. N° 356 de 1981, del Ministerio de Justicia; en los D.S. Nos 81 de 2004; 83 de 2005 y 93 de 2006, todos del Ministerio Secretaría General de la Presidencia; los Instructivo Presidencial No 5 de 2001; en la Ley No. 20.285 de 2008; en el Ordinario N° 3648 de 2010; en la Resolución N° 400 de 01.06.2011; en el artículo 79 y siguientes del D.F.L. N° 29, de 2004, del Ministerio de Hacienda, que fijó el texto refundido, coordinado y sistematizado de la Ley N° 18.834 y en la Resolución N°1.600, de 2008, de la Contraloría General de la República.

**CONSIDERANDO:**

**1°** Que, Según el Decreto Supremo N° 83 del 12 de enero de 2005 del Ministerio Secretaría General de la Presidencia, la Norma Chilena Oficial NCh-ISO 27001.Of2009, como también lo establecido en la Ley N° 20.285, y otras normativas presentes en el SSI del PMG, las exigencias y recomendaciones que se proveen, presentan desafíos en cuanto a la necesidad de garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información, por lo que es necesario que cada uno de los órganos del Estado cumpla con estas normativas a través de la implantación de un Sistema de Seguridad de la Información.

**2°** Que, en conformidad al artículo 11 del Decreto mencionado en el considerando anterior: "Deberá establecerse una política que fije las directrices generales que orienten la materia de seguridad dentro de cada Institución, que refleje claramente el compromiso , apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional".

**3°** Que, por Ordinario N° 3648 de fecha 15 de diciembre de 2010, se aprobó nueva versión de la Política de Seguridad Informática del Servicio Nacional de Menores e instruyó su difusión a todos los funcionarios.

**4°** Que, en el contexto del PMG 2011, Sistema de Seguridad de la Información y las observaciones efectuadas por los analistas de la División de Tecnologías de la Información de la DIPRES y la División Informática de la Subsecretaría del Interior, es necesario dejar sin efecto la Política de Seguridad Informática vigente y elaborar la resolución que aprueba dicha política.

**5°** Que, el Departamento de Planificación y Control de Gestión en su Memorándum N° 231 de fecha 15 de septiembre de 2011, solicita que se realice el control de legalidad de la referida política y se elabore la respectiva resolución de aprobación y difusión de dicho documento.

**6°** Que, esta autoridad accede a dicha solicitud, por lo que se deja sin efecto el Ordinario N° 3648 de 2010.

3733/4
BSA

**RESUELVO:**

**1° DÉJESE SIN EFECTO** Ordinario N° 3648 de fecha 15 de diciembre de 2010, de la Dirección Nacional del SENAME que aprobó nueva versión de la Política de Seguridad Informática del Servicio Nacional de Menores e instruyó su difusión a todos los funcionarios.

**2° APRUÉBASE** la Política General de Seguridad de la Información del Servicio Nacional de Menores, la cual se incorpora como parte integrante de la presente resolución.

La política deberá ser aplicada a todos los funcionarios, incluyendo al personal de planta, contrata y honorarios y en general a cualquier otra persona o empresa que preste servicios o se encuentre contratado por el Servicio.

**3° PUBLÍQUESE** la presente resolución en la página WEB del SENAME, a fin de que sea difundido a los funcionarios, personal a honorarios y terceros.

**4° DÉJASE** establecido que el cumplimiento de la presente Resolución *no irroga* recursos presupuestarios para el Servicio.

**ANÓTESE Y COMUNÍQUESE.**

GOBIERNO DE CHILE
SERVICIO NACIONAL DE MENORES
DIRECTORA NACIONAL

**ANGÉLICA MARÍN DÍAZ**
**DIRECTORA NACIONAL (S)**
**SERVICIO NACIONAL DE MENORES**

**Distribución:**
- Dirección Nacional.
- DEPLAE
- Unidad de Informática
- Depto.Jdco.
- Oficina de Partes.

SERVICIO NACIONAL DE MENORES

# POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

## DEPARTAMENTO DE PLANIFICACIÓN Y CONTROL DE GESTIÓN

## UNIDAD DE INFORMÁTICA

## AÑO 2011

Versión: 1.0
Julio 2011

# Revisión

**Registro de Cambios**

| Fecha | Autor | Versión | Referencias del Cambio |
|---|---|---|---|
| 11-07-2011 | Juan Pablo Mattmann Torres | 1.0 | Versión Inicial |
| 14-09-2011 | Juan Pablo Mattmann Torres | 1.0 | Todas las páginas |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Revisores**

| Nombre | Versión Aprobada | Posición | Fecha |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**Distribución**

| Nombre | Posición |
|---|---|
| | |
| | |
| | |
| | |

**Propiedades del Documento**

| Item | Detalles |
|---|---|
| Título del Documento | Política General de Seguridad de la Información |
| Autor | Unidad Informática – DEPLAE |
| Fecha Creación | 11-07-2011 |
| Última Actualización | 13-9-2011 |

# I N D I C E

# 1.- INTRODUCCIÓN

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 estos equipos, datos y los sistemas que los soportan, sean seguros.

La Política de Seguridad de la Información protege 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.

Es importante que los principios de la Política de Seguridad de la Información sean parte de la cultura organizacional. Por lo tanto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la Institución para la difusión, consolidación y cumplimiento de la presente Política.

# 2.- TÉRMINOS Y DEFINICIONES

A los efectos de este documento se aplican las siguientes definiciones:

**2.1.- Seguridad de la Información:** Con el fin de proteger sus activos de información críticos, el Servicio Nacional de Menores debe tener una Política de Seguridad de la Información y una estrategia de implementación basada en:

- **Confidencialidad**: Proteger la información sensible de la divulgación no autorizada.
- **Integridad**: Salvaguardar la exactitud y la calidad de la información y del software.
- **Disponibilidad**: Que este siempre disponible para aquellas personas autorizadas para su uso.

Adicionalmente, deberán considerarse los conceptos de:

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

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

- **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Para una correcta interpretación de la presente Política, se realizan las siguientes 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.

- **Activos de Información:** Corresponde a todos aquellos elementos relevantes involucrados en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de valor para la Institución.

  De esta forma, es posible distinguir 3 niveles básicos de activos de información:

  - La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc).
  - Los Equipos/Sistemas/Infraestructura que soportan esta información.
  - Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales

- **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.

**2.2.- Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la 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.

**2.3.- Gestión de Riesgos:** Se entiende por gestión de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

**2.4.- Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un 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.

**2.5.- Encargado de Seguridad de la Información:** Es la 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.

**2.6.- 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.

# 3.- POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

## 3.1.- Objetivo

Proteger los Activos de Información de la Institución y los medios utilizados para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política General de Seguridad de la Institución actualizada, con el propósito de asegurar su vigencia y nivel de eficacia.

La Política General de Seguridad de la Información será complementada mediante el desarrollo de una serie de Políticas sobre aspectos específicos de la Seguridad de la Información, tomando como ejes centrales el Decreto Supremo N° 83 sobre Seguridad y Confidencialidad del Documento Electrónico para los Órganos de la Administración del Estado y los Controles de la Norma ISO 27001:2005, e incluye las siguientes materias:

## 3.2.- Alcance

Esta Política se podrá aplicar en todo ámbito de la Institución, a sus recursos y procesos críticos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

El cumplimiento de esta Política es obligatorio para todo el personal que utiliza los activos de información del Servicio Nacional de Menores en todas sus dependencias ubicadas a lo largo del país, así como también para los contratistas y proveedores de servicios.

Los proveedores de servicios y los contratistas deben tomar conocimiento de la Política y llevar a cabo las acciones correspondientes si sus empleados la transgreden mientras trabajan a nombre del Servicio Nacional de Menores.

La presente Política General de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la Seguridad de la Información en el Servicio Nacional de Menores en los siguientes dominios (ISO 27001:2005):

- Política de Seguridad
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad de los Recursos Humanos
- Seguridad Física y del Ambiente
- Gestión de las Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
- Gestión de Incidentes en la Seguridad de la Información
- Gestión de la Continuidad del Negocio
- Cumplimiento

A continuación se indican los principales objetivos de cada uno de los dominios que deben ser abordados en el marco de la implementación del Sistema de Seguridad de la Información dentro de la Institución.

### 3.2.1 Política de Seguridad

Este dominio consiste en proporcionar a la institución la dirección y soporte para la seguridad de la información en concordancia con los requerimientos institucionales y las leyes y regulaciones pertinentes.

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, a través de la emisión y mantenimiento de **un documento de Política General de Seguridad de la Información** en toda la organización.

### 3.2.2 Organización de la Seguridad de la Información

Su objetivo es establecer un marco referencial a nivel directivo para iniciar y controlar la implementación de la seguridad de la información dentro de la institución.

La dirección debe aprobar la política de seguridad de la información, asignar los roles de seguridad a los comités **y designar al encargado de seguridad mediante una resolución**, el cual debe coordinar y revisar la implementación de la seguridad en toda la institución.

Si fuese necesario, se debe establecer una fuente de consultoría sobre seguridad de la información que esté disponible dentro de la institución.

Se deben desarrollar contactos con los especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias mundiales, monitorear los estándares, evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información. Se debe fomentar un enfoque multidisciplinario para la seguridad de la información.

### 3.2.3 Gestión de Activos

Su objetivo es implementar y mantener una apropiada protección de los activos institucionales. Todos los activos deben ser inventariados y contar con un propietario nombrado.

Los propietarios deben identificar todos los activos y deben asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección de los activos.

Adicionalmente se debe asegurar que la información reciba un nivel de protección **adecuado. La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado en su manejo.**

La información puede ser pública o secreta –también se denomina “reservada”- (Ley 20.285), y contar con diferentes grados de importancia dentro de la institución. Algunos activos pueden requerir un nivel de protección adicional o manejo especial dependiendo de su criticidad y riesgo. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

### 3.2.4 Seguridad de Recursos Humanos

Su objetivo es que antes de la contratación, se debe asegurar que los funcionarios, personal a honorarios y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad deben ser definidas y claramente comunicadas a los candidatos antes de la contratación en descripciones de trabajo adecuadas y en los términos y condiciones del empleo. A su vez, se debe realizar la verificación de los antecedentes de dichos candidatos, de acuerdo con las leyes, regulaciones y normas éticas pertinentes y en proporción a los requisitos del cargo y de la información a la cual tendrá acceso , y los riesgos que se emanen de la clasificación de dicha información.

Los funcionarios, personal a honorarios y terceros usuarios de los medios de procesamiento de la información deben firmar un acuerdo sobre sus roles y responsabilidades con relación a la seguridad.

Durante las labores se debe asegurar que los funcionarios usuarios, contratistas y terceras personas estén al tanto de las amenazas y de la pertinencia de la seguridad de la información, de sus responsabilidades y obligaciones, y estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, para reducir el riesgo de error humano e incidentes de seguridad.

Se debe proporcionar a todos los usuarios, funcionarios, personal a honorarios y terceras personas un nivel adecuado de conocimiento, educación y capacitación en procedimientos de seguridad y uso correcto de los medios de procesamiento, activos y servicios de información para minimizar los posibles riesgos de seguridad. Se debe establecer un proceso disciplinario normal para manejar las fallas en la seguridad.

Además se debe asegurar que los funcionarios, contratistas o terceros que sean desvinculados o cambien su relación laboral, lo hagan de una forma adecuada, implementando medidas para que todo equipamiento sea devuelto y se eliminen todos los derechos de acceso de dicho funcionario desvinculado.

### 3.2.5 Seguridad física y del ambiente

Su objetivo es en prevenir el acceso no autorizado, daño e interferencia a las instalaciones de la institución y a la información.

Los equipos de procesamiento de información crítica o sensible de la institución se deben mantener en áreas seguras, protegidos por un perímetro de seguridad definido, con barreras apropiadas de seguridad y controles de entrada. Éstos deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Es necesaria la protección de los equipos, incluyendo los portátiles usados fuera de las dependencias, para reducir el riesgo de acceso no autorizado a datos y para prevenir la pérdida o daño. Se pueden necesitar controles especiales para protegerlos de riesgos o accesos no autorizados, y salvaguardar las instalaciones de apoyo, tales como el suministro eléctrico y la infraestructura de cables.

### 3.2.6 Gestión de las comunicaciones y Operaciones

Su objetivo es crear procedimientos y responsabilidades operacionales de manera de asegurar la operación correcta y segura de los medios de procesamiento de la información.
Cuando sea pertinente, se debe implementar la segregación de deberes para reducir el riesgo de negligencia o mal uso deliberado del sistema.

Los sistemas operativos, los sistemas de aplicación y los medios de procesamiento de la información son vulnerables a la introducción de códigos de software malicioso, como virus de cómputo, virus de red, códigos troyanos y “bombas lógicas”. Los usuarios deben estar al tanto de los peligros de los códigos maliciosos. Se deben introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles a través de antivirus, de manera de proteger la integridad del software y la integración.

Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de la data y practicar su restauración oportuna.

Se debe asegurar la protección de la información que viaja por correo electrónico y su infraestructura de soporte. La gestión segura del correo electrónico, requiere de la cuidadosa consideración de la información que es transmitida, su confidencialidad, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

### 3.2.7 Control de Acceso

El objetivo es asegurar que el acceso del usuario es debidamente autorizado y evitar el acceso no autorizado a los sistemas de información. Se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos deben abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la dada de baja de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debe prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas, su no divulgación y la seguridad del equipo asignado a él.

Se debe implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles y medios de almacenamiento de la información.

Deben implementarse controles efectivos de manera de evitar el acceso no autorizado a los servicios de la red. Se debe controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes no debe comprometer la seguridad de los servicios de la red asegurando:

a) Que existan las interfaces apropiadas entre la red de la institución y las redes de otras organizaciones, y redes públicas;

b) Que se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;

c) Que el control del acceso del usuario a la información sea obligatorio.

Se deben utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios no autorizados. Los medios deben tener la capacidad para:

a) Autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida;

b) Registrar los intentos exitosos y fallidos de autenticación del sistema;

c) Registrar el uso de los privilegios especiales del sistema;

d) Emitir alarmas cuando se violan las políticas de seguridad del sistema;

e) Proporcionar los medios de autenticación apropiados;

f) Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

De igual forma debe ocurrir con la información contenida en los sistemas de aplicación y al utilizar dispositivos móviles para trabajar de forma remota.

### 3.2.8 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

El objetivo es que al interior de la Institución cuando se desarrolle software internamente o, en su defecto, se encarguen su elaboración a un proveedor calificado, se debe garantizar que la seguridad sea una parte integral de los sistemas de información y se incluya en la etapa de formulación del software.

Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones de negocio, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso de negocio puede ser crucial para la seguridad. Se deben identificar y acordar todos los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información en la fase de requerimientos de un proyecto; y deben ser justificados, acordados y documentados como parte de las formalidades para un sistema de información.

### 3.2.9 Gestión de Incidentes en la Seguridad de la Información

El objetivo es asegurar que las debilidades y eventos de seguridad de la información asociados a sistemas de información sean comunicados y de esta manera, permitir tomar acciones correctivas a tiempo.

Se debe establecer un procedimiento formal para informar los eventos de seguridad de la información, junto con la respuesta al incidente y un procedimiento de escalamiento, precisando la acción que se tomará al momento de recibir un informe de un evento de seguridad de la información. Estos procedimientos deben ser de conocimiento de todos los funcionarios de la Institución.

A su vez, se debe asegurar la aplicación de un enfoque constante y eficaz de gestión de incidentes de seguridad, estableciendo las responsabilidades y procedimientos para manejar los eventos y debilidades de seguridad de la información con eficacia, una vez que han sido informados.

Se debe aplicar un proceso de mejora continua en la gestión general de incidentes de seguridad de la información.

La evidencia requerida, cuando corresponda, debe ser recogida asegurando la conformidad con los requisitos legales.

### 3.2.10 Gestión de la Continuidad del Negocio

El objetivo es considerar los aspectos de la seguridad de la información de la gestión de la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Se debe implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la institución y lograr recuperarse de la pérdidas de activos de información (lo cual puede ser resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación. Este proceso debe identificar los procesos institucionales críticos e integrar los requerimientos de gestión de la seguridad de la información de la continuidad del negocio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y medios.

Las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio deben estar sujetos a un análisis del impacto en el negocio. Se deben desarrollar e implementar planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales. La seguridad de la información debe ser una parte integral del proceso general de continuidad del negocio, y otros procesos importantes dentro de la Institución.

La gestión de la continuidad del negocio debe incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debe limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos institucionales.

### 3.2.11 Cumplimiento

El objetivo es evitar los incumplimientos de cualquier ley, estatuto, regulación u obligación contractual legal y de cualquier requisito de seguridad a los cuales puede estar sujeto el diseño, operación, uso y gestión de los sistemas de información.

Se debe contar con asesoría sobre los requisitos legales específicos en el departamento jurídico de la institución, o a través de profesionales del derecho calificados.

De la misma, forma se debe asegurar que los sistemas cumplen con las normas y políticas de seguridad de la Institución, a través de revisiones regulares y auditorías que comprueben el cumplimiento de normas aplicables a la implementación de la seguridad y controles documentados.

Se deben establecer controles para salvaguardar los sistemas en producción y la integridad de las herramientas de auditoría durante las auditorías del sistema de información, y evitando el mal uso de ellas.

### 3.3.- Sanciones Previstas por Incumplimiento

El incumplimiento de la Política 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.

### 3.4.- Comunicación de la Política

La responsabilidad de la difusión de la Política de Seguridad de la Información al interior de la Institución es del Director Nacional del Servicio, quien se apoyará para estos propósitos en los Equipos Directivos de las Unidades Operativas a nivel nacional

Los funcionarios tendrán acceso a esta Política en su última versión vía Intranet.

Con el objeto de lograr un buen entendimiento de la Política y de una correcta aplicación de la misma, se organizarán charlas de difusión a las/os funcionarias/os; al mismo tiempo, en la Intranet Institucional se pondrá a disposición de las/os funcionaria/os tutoriales que expliquen de manera breve aspectos fundamentales del Sistema de Seguridad de la Información y de sus Políticas asociadas.

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

### 3.5.- Revisión de la Política

Uno de los pilares que sustenta la Política de Seguridad de la Información, es la mejora continua del documento, al respecto, se establecen los siguientes hitos de revisión y control de versiones:

El Comité de Seguridad de la Información de la Institución revisará **ANUALMENTE** 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.

# 4.- RESPONSABILIDADES

## 4.1.- Responsabilidad de los Directivos

Todos los Directivos tienen la responsabilidad de garantizar la implementación efectiva de 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, a través de la emisión y mantenimiento de esta **Política de Seguridad de la Información** en toda la Institución.

## 4.2.- Responsabilidades Individuales

La clave para lograr una adecuada implementación del Sistema de Seguridad de la Información en la Institución es una actitud positiva y un enfoque proactivo por parte de los funcionario de la Institución, cada uno de los cuales, tendrá la responsabilidad de 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.

## 4.3.- Responsabilidad de la Unidad Informática

La Unidad Informática de la Institución es responsable de apoyar al Encargado de Seguridad de la Información en la implementación, cumplimiento y control de aquellos aspectos de la Seguridad Informática que se aborden en la presente Política de Seguridad de la Información.

## 4.4.- Responsabilidad del Comité de Seguridad de la Información (CSI)

El Comité de Seguridad de la Información, tendrá la responsabilidad de gestionar la Política de Seguridad de la Información dentro de la Institución, a través de la ejecución de las siguientes funciones.

1. Supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información.

2. Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para implementar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas.

3. Arbitrar conflictos en materias de seguridad de la información y sus riesgos asociados, además de proponer soluciones.

4. Coordinarse con los Comités de Calidad y de Riesgos de la Institución para mantener alineamiento y 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 relevantes en esta materia y su solución.

**4.5.- Responsabilidad del Encargado de Seguridad de la Información**

El 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 de la Institución, a través de la ejecución de las siguientes funciones.

1. Coordinar las actividades del Comité de Seguridad de la Información.

2. Alinear 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.

4. Mantener coordinación con otras dependencias de la Institución para apoyar los objetivos de la seguridad de la información.

**4.6.- Responsabilidad de los Dueños de la Información**

Los Dueños de la Información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

**4.7.- Responsabilidad del Jefe del Departamento de Personas**

El Jefe del Departamento de Personas o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad de la información.

**4.8.- Responsabilidad del Jefe de la Unidad Informática**

El Jefe de la Unidad Informática cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Institución. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

**4.9.- Responsabilidad del Jefe del Departamento Jurídico**

El Jefe del Departamento Jurídico verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Institución con sus empleados y con terceros. Asimismo, asesorará en materia legal a la Institución, en lo que se refiere a la seguridad

de la información.

### 4.10.- Responsabilidad de usuarios de la Información y de los Sistemas

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

### 4.11.- Responsabilidad del Departamento de Auditoría

El Departamento de Auditoría, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.