

**SERVICIO NACIONAL DE CAPACITACIÓN  
Y EMPLEO - SENCE**

**APRUEBA POLÍTICA DE SEGURIDAD DE LA  
INFORMACIÓN DEL SERVICIO NACIONAL DE  
CAPACITACIÓN Y EMPLEO - SENCE.**

**RESOLUCIÓN EXENTA Nº 12892**

**SANTIAGO, 30 DIC 2011**

**CONSIDERANDO:**

1.- Que las Áreas de Mejoramiento del "Programa de Mejoramiento de Gestión", sus sistemas y etapas se encuentran definidos en el Documento Técnico "Programa Marco Básico"-diciembre de 2011, disponibles en la página web de la Dirección de Presupuestos.

2.- Que este Servicio Nacional debe contar con un Sistema de Gestión de Seguridad de la Información que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional considerados relevantes, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios / clientes / beneficiarios.

3.- Que se deberá dar cumplimiento, para la implementación del Sistema de Seguridad de la Información, a las normas establecidas en las Leyes: Nº19.799, sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha Firma; Ley Nº 19.628 sobre Protección de la Vida Privada y Datos Personales; Ley Nº 19.880: Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; Ley Nº 17.336: Sobre Propiedad Intelectual; Ley Nº 17.336: sobre Propiedad Intelectual; Ley Nº 19.223: sobre Delitos Informáticos; Ley Nº 20.285: que Regula el Principio de Transparencia de la Función Pública y el Derecho de Acceso a la Información de los Órganos de la Administración del Estado

4.- Que el Servicio Nacional de Capacitación y Empleo, en virtud del Decreto Nº83 de junio de 2004 que aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, debe implementar una Política de Seguridad de la Información y a su vez establecer responsables en la materia.

**VISTO:**

Las facultades que me otorga el artículo 85 Nº5 de la Ley Nº 19518 y lo preceptuado en la Resolución Nº1.600, de 2008, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

## RESUELVO:

1.- Apruébase una "Política de Seguridad de la Información" para el Servicio Nacional de Capacitación y Empleo, cuyo texto se transcribe a continuación:

### POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La presente Política 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, los sistemas informáticos y el ambiente tecnológico del Servicio Nacional de Capacitación y Empleo.

La Política debe ser conocida y cumplida por todos los funcionarios y personal del Servicio, cualquiera sea su nivel jerárquico y su situación de revista.

#### Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma cada vez que lo requieran.

#### Evaluación de Riesgos

Se entiende por evaluación de riesgos, 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 del Servicio.

#### Administración de Riesgos

El proceso de identificación, control y minimización o eliminación, a un costo razonable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

#### Incidente de Seguridad

Es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

#### Política de Seguridad de la Información

##### Generalidades

La información es un recurso que, al igual que los demás activos, tiene valor para la Institución y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma 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 sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Servicio y de los titulares de los departamentos y unidades del Servicio para la difusión, consolidación y cumplimiento de la presente Política.

## **Objetivo**

Proteger los recursos de información de la Institución y la tecnología utilizada 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 de Seguridad del Servicio actualizada a efectos de asegurar su vigencia y nivel de eficacia.

## **Alcance**

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

## **Responsabilidad**

El Director Nacional, los Directores Regionales, los jefes de departamentos y encargados o sus equivalentes, tanto se trate de autoridades políticas o funcionarios o personal a honorarios y sea cual fuere su nivel jerárquico, son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información será de aplicación obligatoria para todos los funcionarios y personal del Servicio, cualquiera sea su situación de revista, el área a la cual se encuentre adscrito y cualquiera sea el nivel de las tareas que desempeñe.

La máxima autoridad de la Institución aprueba esta Política y es responsable de la autorización de sus modificaciones.

El **Encargado del Sistema de Seguridad de la Información** en la Institución será responsable de:

- a. Asesorar al Director Nacional del Servicio Nacional de Capacitación y Empleo en las materias relacionadas con la seguridad de los documentos electrónicos.
- b. Tener a su cargo el desarrollo inicial de las Políticas de Seguridad al interior de la organización y el control de su implementación y correcta aplicación.
- c. Coordinar las respuestas a incidentes computacionales
- d. Establecer puntos de enlace con los encargados de seguridad y otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
- e. Proponer la clasificación y procedimientos del caso para el procesamiento electrónico.
- f. Desarrollar e implementar las políticas de seguridad de los documentos electrónicos, en forma conjunta con el Comité de Gestión de Seguridad y Confidencialidad.

El **Comité de Gestión de Seguridad y Confidencialidad** en la Institución, será responsable de:

- a. Proponer roles y responsabilidades específicas para la seguridad de la información de la Institución.
- b. Acordar metodologías y procesos específicos para la seguridad de la información; como por ejemplo, evaluación de riesgos, sistema de clasificación de la seguridad, etc.
- c. Acordar y apoyar las iniciativas de seguridad de la información en toda la Institución;
- d. Garantizar que la seguridad sea parte del proceso de planificación de la información;
- e. Evaluar la adecuación de los controles de seguridad de una información específica y coordinar la implementación para los nuevos sistemas o servicios;
- f. Revisar los incidentes de seguridad de la información; y
- g. Promover el apoyo a la seguridad de la información.

## Política

El Servicio Nacional de Capacitación y Empleo, SENCE, contará con un Sistema de Gestión de Seguridad de la Información que permita los atributos de confidencialidad, integridad y disponibilidad para todos los activos de información institucional considerados relevantes, de manera tal que se aseguren los procesos de soporte y los procesos de provisión de bienes y servicios para los potenciales beneficiarios de esta Institución.

En ese marco, esta Institución realizará las siguientes acciones para clasificar y catastrar los activos de información:

- Formalizar la Estructura Organizacional
- Revisar y formalizar las normativas base en Seguridad de la Información
- Catastrar los elementos tecnológicos que intervienen en la continuidad del servicio tecnológico.
- Identificar las vulnerabilidades del perímetro internet
- Identificar las vulnerabilidades de servidores de soporte al portal web.
- Identificar las vulnerabilidades de bases de datos.
- Evaluación de seguridad en el Diseño de la Arquitectura de Red.
- Evaluación de vulnerabilidades de una muestra de aplicaciones web del portal.

La siguiente es la estructura del marco de políticas, estándares y procedimientos en materia de seguridad de la información a ser desarrollados por SENCE:

Ámbito	Política
Política de Seguridad	Política General de Seguridad
Organización de la Seguridad de la información	Política de Conexión con terceros
Administración de Activos de información	Política de Clasificación de la información Política de protección de información
Seguridad de Recursos Humanos	Políticas de Personal (selección, contratación, desvinculación) Política de Educación en Seguridad de la Información
Seguridad Física y ambiental	Política de Seguridad Física Política de Control de Acceso Físico

<b>Ámbito</b>	<b>Política</b>
<p>Administración de Operaciones y Comunicaciones</p>	<p>Política de Seguridad de Redes de Comunicación</p> <p>Política de Seguridad de Computadores Personales</p> <p>Política de Seguridad de Código Malicioso</p> <p>Política de Seguridad de Correo Electrónico</p> <p>Política de Seguridad de uso de Internet</p> <p>Política de Seguridad de Firewall</p> <p>Política de Seguridad de Administración de Medios Removibles</p> <p>Política de Seguridad de Respaldos de Información</p> <p>Política de Seguridad de Intercambio de Información</p>
<p>Control de Acceso</p>	<p>Política de Seguridad de Control de Acceso Lógico</p> <p>Política de Identificación y Autenticación</p> <p>Política de Cuentas de Usuarios</p> <p>Política de Escritorios y Pantallas Limpias</p> <p>Política de Seguridad de Acceso a Conexiones Remotas VPN</p>
<p>Adquisición, desarrollo y mantención de Sistemas de Información</p>	<p>Política de Seguridad de Desarrollo de Sistemas</p> <p>Política de Seguridad de Control de Cambios</p> <p>Política de Uso de Controles Criptográficos</p>
<p>Administración de Incidentes de Seguridad</p>	<p>Política de Incidentes de Seguridad</p>

La implementación de este proceso se realizará a través de:

1. Emitir una Resolución Exenta para nominar al Encargado de seguridad de los documentos electrónicos en conjunto con el Comité que apoyará las iniciativas en los temas.
2. Establecer un Glosario de Términos.
3. Diseñar e implementar un programa de capacitación sobre gestión de seguridad de la información.
4. Diseñar e implementar un programa comunicacional, para difundir la información a todos los funcionarios y personal del SENCE.

Como elementos relevantes para la gestión de seguridad, se deben considerar:

1. La Política de Gestión de Riesgos, cuyo foco se encuentra en la reducción de los riesgos, obedece al propósito de mejorar la gestión institucional, a fin de contribuir efectivamente al cumplimiento de sus objetivos estratégicos y con ello al logro de su misión.
2. La Política de Calidad del Servicio, que orienta las decisiones y acciones hacia la mantención de un Sistema de Gestión de Calidad, certificable bajo la Norma ISO 9001:2000, buscando el mejoramiento continuo. Esta definición tiene su alcance a los Sistemas del PMG susceptibles de ser implementados bajo Norma ISO;

La presente declaración se revisará cada tres años de modo de adecuarla a la cultura organizacional vigente, en cuanto a seguridad de la información.

#### **Sanciones Previstas por Incumplimiento**

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de sanciones, conforme a la responsabilidad administrativa que pueda imputarse de acuerdo a la ley.

#### **Capacitación y Difusión de la Política Formación y Capacitación en Materia de Seguridad de la Información**

Todos los funcionarios y personal del Servicio y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la Institución, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la Institución. Esto comprenderá a los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo, su estación de trabajo.

El/la Encargado/a de la Unidad de Recursos Humanos del Servicio será el responsable de coordinar las acciones de capacitación que surjan de la presente Política.

Cada seis meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo a su necesidad.

El personal que ingrese al Servicio recibirá el material de capacitación, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información; antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todos los funcionarios y personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

**Respuesta a Incidentes y Anomalías en Materia de Seguridad**  
**Comunicación de Incidentes Relativos a la Seguridad**

Los incidentes relativos a la seguridad de la información serán comunicados a través de canales formales apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento, quien deberá indicar los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Todos los funcionarios y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

**Comunicación de Debilidades en Materia de Seguridad**

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, deberán registrar y comunicar las mismas al Responsable de Seguridad Informática.

Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

**Comunicación de Anomalías del Software**

Se establecerán procedimientos para la comunicación de anomalías de softwares, los cuales deberán contemplar:

- a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
- c) Alertar inmediatamente al Responsable de Seguridad Informática o del activo de que se trate.

Se prohíbe a los usuarios retirar un software supuestamente anómalo, a menos que se encuentren autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

<b>ELABORADO POR</b> <b>JEFE UNIDAD DE AUDITORÍA</b> <b>INTERNA</b>	<b>REVISADO POR</b> <b>ENCARGADO DE PMG</b> <b>INSTITUCIONAL</b>	<b>APROBADO POR</b> <b>DIRECTOR NACIONAL</b>
---	--	---

**GLOSARIO:**

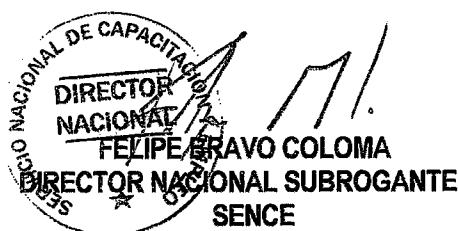
a) **Activos de Información:** Algunos ejemplos de activos son:

- **Recursos de información:** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- **Recursos de software:** software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

- **Activos físicos:** equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
  - **Servicios:** servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).
- b) **Autenticación:** proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.
  - c) **Confidencialidad:** Aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.
  - d) **Contenido del documento electrónico:** información, ideas y conceptos que un documento expresa.
  - e) **Continuidad del negocio:** continuidad de las operaciones de la Institución.
  - f) **Disponibilidad:** aseguramiento que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.
  - g) **Documento electrónico:** toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
  - h) **Documentos públicos:** Aquellos documentos que se encuentran a libre disposición de las personas.
  - i) **Documentos reservados:** aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del Servicio a la que sean remitidos
  - j) **Documentos secretos:** los documentos que tienen tal carácter de conformidad a una ley de quórum calificado.
  - k) **Ejecutivo:** autoridad dentro de la Institución.
  - l) **Identificador formal de autenticación:** mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.
  - m) **Incidentes de seguridad:** situación adversa que amenaza o pone en riesgo un sistema informático.
  - n) **Información:** contenido de un documento electrónico.
  - o) **Integridad:** salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados.
  - p) **Negocio:** función o servicio prestado por la Institución.
  - q) **Política de Seguridad:** conjunto de normas o buenas prácticas declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés o bien garantizar la realización periódica y sistemática de este conjunto.
  - r) **Repositorio:** estructura electrónica donde se almacenan documentos electrónicos.
  - s) **Riesgos:** amenazas de impactar y vulnerar la seguridad del documento electrónico y su posibilidad de ocurrencia.
  - t) **Sistema informático:** conjunto de uno o más computadores, softwares asociados, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
  - u) **Usuario:** entidad o individuo que utiliza un sistema informático.
  - v) **Activos de Información:** Algunos ejemplos de activos son:

- **Recursos de información:** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- **Recursos de software:** software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- **Activos físicos:** equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- **Servicios:** servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

**ANÓTESE, COMUNÍQUESE, PUBLÍQUESE EN LA PÁGINA WEB INSTITUCIONAL Y ARCHÍVESE.**



*[Handwritten signature]*  
 MVT/JdelaF/MSN

**Distribución:**

- Dirección Nacional
- Departamentos
- Unidades
- Unidad de Marketing y Comunicaciones
- Oficina de Partes