



FRO/PRIMARIAS/PFA/NBB/PFA



**DIVISIÓN JURÍDICA**

**MODIFICA POLÍTICA DE  
SEGURIDAD DE LA  
INFORMACIÓN APROBADA POR  
RESOLUCIÓN EXENTA Nº 5949,  
DE 2010, DEL MINISTERIO DE  
EDUCACIÓN.**

5159

**SANTIAGO,**

**RESOLUCIÓN EXENTA Nº**

005854 \*03.11.2011

**CONSIDERANDO:**

Que, de conformidad a lo establecido en la Ley Nº 18.956, que reestructura el Ministerio de Educación Pública, corresponde a esta Secretaría de Estado, entre otras funciones, fomentar el desarrollo de la educación en todos sus niveles.

Que, con el objeto de apoyar el cumplimiento de sus funciones, el Ministerio de Educación ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes Activos de Información, que permiten interactuar con la comunidad escolar, ciudadanía en general y el personal del Ministerio en todo el país.



*Handwritten signature*

Que, el Ministerio de Educación reconoce que la información que posee es un bien estratégico para sus funciones, por lo que se requiere que sea protegida tanto en su obtención, procesamiento, transmisión como almacenamiento.

Que, el Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, impone la obligación de establecer una Política de Seguridad que fije las directrices generales que orienten la materia de seguridad dentro de cada institución.

Que, la Resolución Exenta N° 5336, de 2010, del Ministerio de Educación, aprobó la Política de Seguridad de la Información de este Ministerio, a la que se ha estimado necesario incorporar modificaciones.

### **VISTO:**

Lo dispuesto en los artículos 32 N° 6 y 35 de la Constitución Política de la República de Chile, cuyo texto refundido, coordinado y sistematizado fue fijado por el Decreto N° 100, de 2005, del Ministerio Secretaría General de la Presidencia; en el Decreto con Fuerza de Ley N° 1/19.653 del año 2000, del Ministerio Secretaría General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N° 18.956, de 1990, que reestructura el Ministerio de Educación Pública; en la Ley N° 20.285, de 2008, sobre acceso a la Información Pública; en el Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia; en la Resolución Exenta N° 5336, de 2010, del Ministerio de Educación y en la Resolución N° 1600, de 2008, de la Contraloría General de la República.

### **RESUELVO:**

Artículo 1º: Introdúcense las siguientes modificaciones en la Política de Seguridad de la Información aprobada por Resolución Exenta N° 5336, de 2010, del Ministerio de Educación:

1. En el Índice, a continuación del numeral 2.8, agréganse los siguientes numerales 2.9 y 2.10:

2.9 Gestión de Incidentes de Seguridad.....9  
2.10 Cumplimiento de normas, políticas, estándares y procedimientos....10

2. Reemplázase la denominación de "Jefe de Seguridad de la Información" por la de "Encargado de Seguridad de Activos de Información", todas las veces en que aparece mencionada en su texto.

3. Reemplázase la letra a) del párrafo cuarto del numeral 2.1, por la siguiente:

a) "Tener a su cargo el desarrollo y actualización de las políticas de seguridad y el control de su implementación, utilizando como referente la Norma chilena sobre seguridad de información (NCh-ISO 27001-2009)".

4. Elimínase el penúltimo párrafo del numeral 2.3.

5. Agréguese a continuación del numeral 2.8, los siguientes numerales 2.9 y 2.10:

### **"2.9 Gestión de incidentes de seguridad**

Se entiende por incidentes de seguridad del Mineduc a todo evento que impida el normal funcionamiento de sus Activos de Información y que afecte la seguridad informática.

La gestión de incidentes de seguridad tiene por objeto restaurar la operación normal de los Servicios, con tanta rapidez como sea posible y minimizar el impacto adverso a sus procesos, asegurando así que se mantenga debidamente la confidencialidad, integridad y disponibilidad de la información del Ministerio.

El Comité de Seguridad de la Información definirá los procedimientos a seguir en la gestión de incidentes de seguridad, los que deberán ser implementados por el Departamento de Informática y Computación, bajo la coordinación del Encargado de Seguridad de Activos de Información.

El Encargado de Seguridad de Activos de Información coordinará los procedimientos de gestión de incidentes, en particular en lo referido a las formas de notificación de incidentes de seguridad de la información, y en todos aquellos aspectos que permitan una pronta detección y respuesta ante dichos incidentes.

Asimismo, el Encargado de Seguridad de Activos de Información deberá resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los Activos de Información del Mineduc acerca de las Políticas de Seguridad de la Información vigentes en el Ministerio, y en particular sobre las obligaciones que les correspondan en relación a la gestión de incidentes de seguridad.

Todo el personal que tenga conocimiento de incidentes de seguridad, deberá informarlo en la forma más rápida y expedita posible a la Mesa de Ayuda del Departamento de Informática y Computación, la que deberá aplicar el procedimiento de gestión de incidentes dispuesto para estos efectos.

### **2.10 Cumplimiento de las Políticas de Seguridad de la Información**

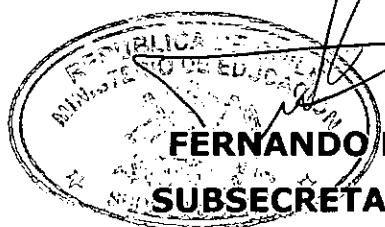
Las Jefaturas de las diferentes Divisiones, Departamentos, Secciones y Programas del Mineduc, deberán adoptar medidas tendientes a facilitar que las personas que trabajen bajo su dependencia, cumplan adecuadamente con las normas, políticas, estándares y procedimientos

aplicables en el Ministerio para proteger la confidencialidad, integridad y disponibilidad de la información.

La División Jurídica del Mineduc deberá ser debidamente consultada sobre la adecuación a la normativa vigente de las normas, políticas, estándares y procedimientos que se pretendan establecer en relación a las Políticas de Seguridad de la Información del Ministerio.

Artículo 2º: Reemplázase en el artículo 2º de la Resolución Exenta N° 653, de 2011, del Ministerio de Educación, que crea el Comité de Seguridad de la Información, la denominación de "Jefe de Seguridad de la Información" por la de "Encargado de Seguridad de Activos de Información".

**ANÓTESE Y COMUNÍQUESE**



**FERNANDO ROJAS OCHAGAVÍA**  
**SUBSECRETARIO DE EDUCACIÓN**

**Distribución:**

Oficina de Partes	1
- Gabinete Ministro	1
- Gabinete Subsecretario	1
- División Jurídica	1
- División Administración General	1
- Departamento Recursos Humanos	1
- Departamento Informática y Computación	1
- Coordinación Nacional Tecnología, Información e Innovación	1
<b>Total</b>	<b>8</b>

Solicitud N° 26433-2011

# **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**



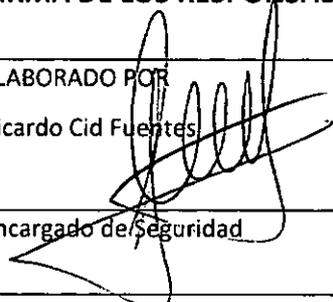
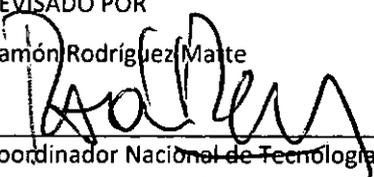
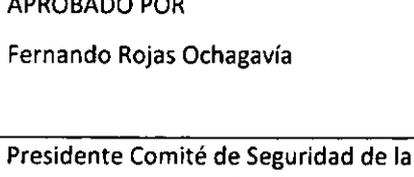
**2011**

**NOTA DE CONFIDENCIALIDAD**

La información contenida en este documento es de carácter reservada. Esta información es para uso exclusivo del Ministerio de Educación. Si usted recibe este documento por equivocación o error, no está autorizado a utilizar, distribuir o fotocopiar este documento

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 2/11

**FIRMA DE LOS RESPONSABLES**

ELABORADO POR Ricardo Cid Fuentes 	REVISADO POR Ramón Rodríguez Maite 	APROBADO POR Fernando Rojas Ochagavía 
Encargado de Seguridad	Coordinador Nacional de Tecnologías e Innovación	Presidente Comité de Seguridad de la Información

**CONTROL DE VERSIONES**

REVISIONES DEL DOCUMENTO DE POLÍTICA				
Nº Revisión	Fecha Aprobación	Motivo de la revisión	Páginas Modificadas	Autor
0(Cero)		Elaboración inicial	Todas	
1	13/07/2011	Modificación de logo del gobierno. Se reemplaza la denominación "Jefe de Seguridad de la Información" por la de "Encargado de Seguridad de Activos de Información" Se añade referencia a Norma Chilena sobre seguridad de información (NCh-ISO 27001-2009). Se añadieron temas de seguridad relativos a Gestión de Incidentes y Cumplimiento.	Tapa, Índice, 6, 8, 9, 10	Ricardo Cid
2				
3				

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 3/11

## ÍNDICE

<b>1. DECLARACIÓN INSTITUCIONAL.....</b>	<b>4</b>
1.1 Objetivos.....	5
1.2 Alcance.....	5
<b>2. POLÍTICA DE SEGURIDAD.....</b>	<b>5</b>
2.1 Organización y responsabilidades.....	5
2.2 Clasificación, registro y control de activos.....	7
2.3 Seguridad del personal.....	7
2.4 Seguridad física.....	7
2.5 Gestión de operaciones y comunicaciones.....	8
2.6 Control de accesos.....	8
2.7 Adquisición, desarrollo y mantenimiento de activo TIC.....	9
2.8 Continuidad de los servicios.....	9
2.9 Gestión de Incidentes de Seguridad.....	9
2.10 Cumplimiento de normas, políticas, estándares y procedimientos.....	10
<b>3. REVISIONES.....</b>	<b>10</b>
<b>4. DIFUSIÓN.....</b>	<b>10</b>
<b>5. GLOSARIO DE TERMINOS.....</b>	<b>10</b>

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 4/11

## 1. DECLARACIÓN INSTITUCIONAL.

El Ministerio de Educación, en conformidad a lo dispuesto en la Ley N°18.956 de 1990, que reestructura este Ministerio, es la Secretaría de Estado encargada, entre otras funciones, de fomentar el desarrollo de la educación en todos sus niveles.

Para apoyar el cumplimiento de sus funciones, el Ministerio de Educación (Mineduc) ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes Activos de Información, que permiten interactuar con la comunidad escolar, ciudadanía en general y los integrantes del Mineduc en todo el país, con la información requerida para dar cumplimiento a las funciones que el mandato legal exige, considerando que la información resguardada puede ser propia de los sistemas del Mineduc, de los servicios o sus procesos, así como también de los usuarios internos o externos.

El Mineduc reconoce que la información que posee es un bien estratégico para sus funciones, por lo que se requiere que sea protegida tanto en su obtención, procesamiento, transmisión como almacenamiento. Por lo tanto, todo el personal que integra la organización será responsable de la confidencialidad, integridad y disponibilidad de la información que, por cargo y función, les corresponde administrar y gestionar.

La información y los procesos de apoyo, representados por la Infraestructura Tecnológica de Información y Comunicaciones (TIC), son bienes de máxima importancia, que deben asegurar la confidencialidad, integridad y disponibilidad de la información, conforme a las exigencias que el marco legal impone al Mineduc.

Debe considerarse, además, que el Mineduc en sus sistemas de información y redes está enfrentado, en forma creciente, a las amenazas de seguridad desde una amplia gama de fuentes que van desde hechos naturales, pasando por fallas de equipos o aplicaciones, hasta ataques intencionales, por lo que sus sistemas informáticos requieren estar protegidos.

Para este Ministerio es de alta importancia el almacenamiento y tratamiento que se le da a los Activos de Información, entendiéndose por tales a todo elemento en que se registre, en que se almacene y/o procese datos e información, sea a través de medios tecnológicos o no, tales como: bases de datos y archivos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, plan de continuidad de negocio, información de auditorías, información archivada, activos de software, activos físicos y servicios.

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 5/11

## 1.1 Objetivos

Establecer normas que regulen el correcto uso de los servicios e información, a través de las distintas actividades que el personal del Mineduc realiza en el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los servicios e información.

Establecer los requisitos y condiciones generales de seguridad a las que se encuentra sujeto el Mineduc, de acuerdo a las normas legales y reglamentarias pertinentes, así como los riesgos a que están expuestos sus Activos de Información y los principios y objetivos internos para el resguardo de sus operaciones.

## 1.2 Alcance

La presente Política de Seguridad de la Información del Mineduc expresa, en forma clara y sucinta, los lineamientos generales con respecto al buen uso de los Activos de información, tanto compartidos como de cada uno de los usuarios internos o externos.

Estas directrices de alto nivel, están destinadas a servir de guía para la definición de normas específicas que se contendrán en las disposiciones complementarias de carácter administrativo y técnico que se dicten para el cumplimiento de lo dispuesto en la presente Política.

La seguridad de la información es de responsabilidad de todos los usuarios que se relacionan con este Ministerio, ya sean usuarios externos, que sean identificables, que presten servicios o asesorías y que por sus funciones deban acceder a la Red de Área Extendida (WAN), o usuarios internos en la Red de Área Local (LAN,) con acceso a los Activos de Información del Mineduc. Por tal razón, las políticas establecidas en este documento son de conocimiento y cumplimiento obligatorio para todos los usuarios a los que se les otorgue acceso a estos activos. En el caso de los usuarios externos, dicha obligación deberá expresarse en los contratos y/o acuerdos respectivos.

## 2. POLÍTICA DE SEGURIDAD

### 2.1 Organización y responsabilidades

La seguridad de la información, abordada como responsabilidad institucional, hace necesaria la participación de todo el personal del Mineduc y de aquellos organismos externos que tienen los roles y responsabilidades establecidas en los respectivos contratos y/o acuerdos, en la contribución del logro de los objetivos de confidencialidad, disponibilidad e integridad de la información.

Con el propósito de optimizar la gestión de seguridad informática y darle la transversalidad organizacional que ésta requiere, se creará en el Mineduc, una vez que esta Política entre en vigencia, un Comité de Seguridad de la Información, presidido por el Subsecretario de Educación, coordinado por el Encargado de Seguridad de la Información y conformado además por un abogado del Mineduc y un representante del Departamento de Recursos Humanos designado por el Jefe de dicho Departamento.

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 6/11

El Comité de Seguridad de la Información tendrá por misión **“velar por la confidencialidad, integridad y disponibilidad de la información y los medios tecnológicos que la soportan”**, para lo cual, elaborará políticas específicas, procedimientos, medidas administrativas, determinará los medios tecnológicos a utilizar y dictará las demás disposiciones que se deriven de la presente política.

El Comité de Seguridad de la Información, sesionará una vez al mes o cuando sea necesario de acuerdo a las necesidades del Mineduc.

Sin perjuicio de las funciones específicas que desarrollará el Encargado de Seguridad de la Información en conformidad a la resolución que lo designe, sus funciones incluirán a lo menos:

- a) Tener a su cargo el desarrollo y actualización de las políticas de seguridad y el control de su implementación, utilizando como referente la Norma chilena sobre seguridad de información (NCh-ISO 27001-2009).
- b) Coordinar la respuesta a incidentes de seguridad.
- c) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

Por su parte, el Departamento de Informática y Computación, tomará las medidas necesarias para resguardar los Activos de Información y mantener su disponibilidad, confiabilidad e Integridad, de acuerdo a las directrices establecidas por el Comité de Seguridad de la Información. En el ámbito de la seguridad de la información, desarrollará las siguientes funciones:

- a) Propondrá disposiciones generales para el uso de Activos de Información;
- b) Propondrá capacitaciones pertinentes para el personal del Mineduc;
- c) Realizará capacitaciones a dicho personal referida a la política de seguridad informática y de procedimientos del área TIC, en las competencias requeridas conforme al perfil de cada cargo;
- d) Gestionará el procedimiento que se inicie en virtud de la denuncia de un incidente de seguridad.
- e) Realizará procesos internos de auditoría de acuerdo a las necesidades establecidas por el jefe del Departamento de Informática y Computación;
- f) Adoptará las medidas necesarias para resguardar los Activos de Información en conformidad a las instrucciones impartidas por el Comité de Seguridad de la Información.

Finalmente, cada usuario, ya sea interno o externo, será responsable de los equipos de procesamiento de datos entregados para su trabajo y de respetar las normas de seguridad respecto a la información que por su cargo deba acceder, procesar y/o generar.

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 7/11

## 2.2 Clasificación, registro y control de activos

El Departamento de Informática y Computación, mantendrá un registro de los Activos de Información del Mineduc, sus configuraciones e inventarios y personal responsable de cada uno de ellos.

De igual forma, propondrá las disposiciones necesarias para la correcta administración y uso de los equipos de procesamiento de datos por parte de los usuarios internos y/o externos, para el soporte por parte de la unidad de mantenimiento y para los cambios de configuraciones que se realicen a estos equipos.

Respecto al derecho de acceso a la información de los órganos de la Administración del Estado, deberán respetarse los principios establecidos en el artículo 11 de la Ley N° 20.285, de 2008, del Ministerio Secretaría General de la Presidencia.

## 2.3 Seguridad del personal

Con el objeto de reducir los riesgos de error humano o mal uso de los recursos informáticos, el Departamento de Informática y Computación, propondrá anualmente al Comité de Seguridad de la Información, los requerimientos de actualización de competencias para el personal de administradores de los sistemas informáticos, redes y seguridad, que les permita cumplir adecuadamente las misiones de su responsabilidad.

El Departamento de Recursos Humanos dispondrá de un proceso de inducción para el personal contratado por el Mineduc, en materias correspondientes a la confidencialidad de la información y sistemas informáticos, que sean puestos a disposición de los integrantes del Mineduc, para el desempeño de sus funciones.

De igual forma se considerará, dentro del proceso de inducción al personal que se incorpora anualmente al Mineduc, una capacitación por parte del Departamento de Informática y Computación, referida a la política de seguridad informática y de procedimientos del área TIC, en las competencias requeridas conforme al perfil de cada cargo.

En caso que el personal del Mineduc infrinja las normas de seguridad de la información, deberá instruirse un procedimiento sumario en conformidad a lo dispuesto en el Estatuto Administrativo a fin de aplicar la medida disciplinaria que corresponda, sin perjuicio de la responsabilidad civil o penal que pudiera existir. Para el caso de que las infracciones sean realizadas por personal externo, se procederá de acuerdo a lo establecido en los respectivos contratos y/o acuerdos vigentes a fin de determinar las sanciones pertinentes, sin perjuicio de las responsabilidades civiles o penales que puedan corresponder.

## 2.4 Seguridad física

Se considerará dentro de las áreas de acceso restringido, las instalaciones en las que se encuentren equipos de procesamiento o comunicaciones de datos. Dentro de estas áreas restringidas, se encuentran: sala de servidores, dependencias donde se encuentran equipos de comunicaciones pertenecientes al cableado estructurado de la red LAN, oficina de administradores y monitoreo, oficinas de desarrolladores, taller de soporte, estaciones

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 8/11

de trabajo de los usuarios y todas las instalaciones que el Comité de Seguridad de la Información determine que deban ser de acceso restringido.

## **2.5 Gestión de operaciones y comunicaciones**

El Departamento de Informática y Computación deberá gestionar los procedimientos de apoyo, servicios informáticos y de seguridad de la información, de acuerdo a las normas establecidas por el Comité de Seguridad de la Información.

Con el fin de reducir el riesgo en el uso de los Activos de Información, en el Departamento de Informática y Computación se separarán los roles de las áreas de desarrollo, prueba y administración.

A su vez, el Comité de Seguridad de la Información definirá los procedimientos a seguir en la gestión de incidentes de seguridad, los que deberán ser implementados por el Departamento de Informática y Computación, bajo la coordinación del Encargado de Seguridad de la Información.

Por su parte, el Departamento de Informática y Computación realizará procesos internos de auditoría de acuerdo a las necesidades establecidas por el Jefe del Departamento, sin perjuicio del rol de auditoría que le corresponde al Departamento de Auditoría del Mineduc.

El Departamento de Informática y Computación deberá implementar los mecanismos de protección preventiva y activa contra softwares maliciosos, que puedan llegar en forma física o lógica a la red o estaciones de trabajo.

La información de los sistemas y configuraciones de los servidores de servicios importantes para las funciones de este Ministerio, deberán ser respaldados periódicamente por el Departamento de Informática y Computación, conforme a los procedimientos definidos por el Comité de Seguridad de la Información.

A fin de asegurar el buen uso de los servicios informáticos por parte de los usuarios internos o externos, el Departamento de Informática y Computación, propondrá las normas de uso de los servicios TIC que estén a disposición del personal o de otras instituciones que hacen uso de los Activos de la Información, de comunicaciones e información del Mineduc, las que deberán ser aprobadas por el Comité de Seguridad de la Información.

## **2.6 Control de accesos**

Cada usuario de los Activos de Información, tendrá acceso a la información de las aplicaciones informáticas, conforme al rol de su cargo y de acuerdo al nivel de acceso definido por el Comité de Seguridad de la Información. Es decir, se asignarán los privilegios de acceso a los usuarios internos o externos, basados en su necesidad de uso, con un criterio de información mínima, conforme a su rol y funciones.

La información de los sistemas que, bajo las condiciones anteriores, tenga acceso el personal, es para el uso exclusivo de las tareas que por rol le corresponde y no podrá ser

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 9/11

entregada o divulgada en forma integral o parcial a terceros que no sean sus respectivos jefes y sólo para fines del trabajo productivo.

El acceso a la información será conforme a un Plan de Cuentas, propuesto por el Departamento de Informática y Computación en conjunto con los Jefes de División y aprobado por el Comité de Seguridad de la Información. Los privilegios de acceso que se asignen a los respectivos mandos, se otorgarán de acuerdo a su ámbito de acción y responsabilidades.

## **2.7 Adquisición, desarrollo y mantenimiento de activo TIC**

Todo Activo de Información que se requiera incorporar al Mineduc, deberá ser evaluado por el Departamento de Informática y Computación desde el punto de vista de un análisis de riesgos, antes de su compra, a fin de considerar en el proceso de adquisición, los requerimientos de seguridad que involucren los nuevos Activos.

Los softwares operacionales, deberán ser controlados, administrados y mantenidos en una biblioteca técnica, junto a todas sus actualizaciones.

Los softwares computacionales, compilaciones de datos, adaptaciones y cualquier documento relacionado con ello, son de propiedad del Mineduc, por cuanto han sido realizados por el personal contratado por este Ministerio, en el desempeño de sus funciones, sea que éstos hayan sido realizados individualmente o de manera colectiva.

Los Activos de Información identificados como importantes para la continuidad del accionar del Mineduc, deberán contar con contrato de mantenimiento y/o soporte con los proveedores, a fin de asegurar su funcionamiento o reemplazo conforme a los niveles de servicio requeridos y su actualización.

## **2.8 Continuidad de los servicios**

El Departamento de Informática y Computación deberá aplicar una estrategia, aprobada por el Comité de Seguridad de la Información, que asegure la continuidad operacional de los procesos críticos de la institución. A su vez, deberá gestionar los planes de contingencia, conforme a la estrategia definida.

El Encargado de Seguridad de la Información, en su calidad de Coordinador del Comité de Seguridad de la Información, asumirá la responsabilidad de ejecución de la planificación de contingencia que permita asegurar la continuidad de los procesos críticos en el Mineduc.

## **2.9 Gestión de Incidentes de Seguridad**

Se entiende por incidentes de seguridad del Mineduc a todo evento que impida el normal funcionamiento de sus Activos de Información y que afecte la seguridad informática.

La gestión de incidentes de seguridad tiene por objeto restaurar la operación normal de los Servicios, con tanta rapidez como sea posible y minimizar el impacto adverso a sus procesos, asegurando así que se mantenga debidamente la confidencialidad, integridad y disponibilidad de la información del Ministerio.

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 10/11

El Comité de Seguridad de la Información definirá los procedimientos a seguir en la gestión de incidentes de seguridad, los que deberán ser implementados por el Departamento de Informática y Computación, bajo la coordinación del Encargado de Seguridad de Activos de Información.

El Encargado de Seguridad de Activos de Información coordinará los procedimientos de gestión de incidentes, en particular en lo referido a las formas de notificación de incidentes de seguridad de la información, y en todos aquellos aspectos que permitan una pronta detección y respuesta ante dichos incidentes.

Asimismo, el Encargado de Seguridad de Activos de Información deberá resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los Activos de Información del Mineduc acerca de las Políticas de Seguridad de la Información vigentes en el Ministerio, y en particular sobre las obligaciones que les correspondan en relación a la gestión de incidentes de seguridad.

Todo el personal que tenga conocimiento de incidentes de seguridad, deberá informarlo en la forma más rápida y expedita posible a la Mesa de Ayuda del Departamento de Informática y Computación, la que deberá aplicar el procedimiento de gestión de incidentes dispuesto para estos efectos.

## **2.10 Cumplimiento de las Políticas de Seguridad de la Información**

Las Jefaturas de las diferentes Divisiones, Departamentos, Secciones y Programas del Mineduc, deberán adoptar medidas tendientes a facilitar que las personas que trabajen bajo su dependencia, cumplan adecuadamente con las normas, políticas, estándares y procedimientos aplicables en el Ministerio para proteger la confidencialidad, integridad y disponibilidad de la información.

La División Jurídica del Mineduc deberá ser debidamente consultada sobre la adecuación a la normativa vigente de las normas, políticas, estándares y procedimientos que se pretendan establecer en relación a las Políticas de Seguridad de la Información del Ministerio.

## **3. REVISIONES**

El Comité de Seguridad de la Información efectuará una revisión de esta Política cada tres años, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad de la organización.

## **4. DIFUSIÓN**

Todo el personal del Mineduc deberá tomar conocimiento de la presente política y ésta quedará disponible para futuras consultas en la plataforma Intranet.

## **5. GLOSARIO DE TERMINOS**

Para los propósitos de esta Política, las siguientes palabras se entenderán en el sentido que a continuación se indica:

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 11/11

**Activo:** Cualquier elemento que tenga valor para la organización. Para el ámbito de seguridad de la información, se puede clasificar en:

- a) **Activos de Información:** Se entenderá por Activo de Información todo elemento en que se registre, en que se almacene y/o procese datos e información, sea a través de medios tecnológicos o no, tales como: bases de datos y archivos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, plan de continuidad de negocio, información de auditorías, información archivada, activos de software, activos físicos y servicios.
- b) **Activos de Software:** Constituidos por las aplicaciones de software, Software de sistemas y Herramientas de desarrollo y utilidades.
- c) **Activos Físicos:** Constituidos por el equipamiento computacional, Equipamiento de comunicaciones, Medios móviles y otros equipamientos.
- d) **Servicios:** Servicios de computación y comunicaciones. Utilidades generales (ej. electricidad, luz, aire acondicionado, etc.)
- e) **Personas:** Constituidos por los usuarios, que utilizan la estructura tecnológica, el área de comunicaciones y que gestionan la información.
- f) **Intangibles:** Constituidos por los activos referidos a la reputación e imagen de la institución.

**Amenaza:** Una causa potencial de un incidente no-deseado, el cual puede derivar en daño a un sistema u organización.

**Análisis de Riesgos:** Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

**Auditoria de Seguridad informática:** Proceso sistemático, independiente y documentado que permite realizar una evaluación detallada de la Arquitectura de Seguridad mediante un análisis a nivel técnico (servidores, networking, firewalls, routers) y a nivel de procedimientos (procesos de revisiones y actualizaciones, políticas de accesos, contraseñas, planes de contingencia, etc.)

**Confidencialidad:** Garantía de que accedan a la información sólo aquellas personas autorizadas a hacerlo.

**Integridad:** Mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.

**LAN:** Constituido por Redes de Área Local que interconectan distintos dispositivos entre sí, en el ámbito de un edificio.

**Disponibilidad:** Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	<b>Fecha</b> : 30-10-2010 <b>Cambio</b> : 1	<b>Identificación</b> : DIC – 001 <b>Página</b> : 12/11

**Mesa de Ayuda:** Unidad del Área de Soporte, que atiende y da solución a los requerimientos técnicos de los usuarios del Mineduc.

**Política:** Intención y dirección general expresada formalmente por la autoridad máxima en la institución.

**Riesgo:** Combinación de la probabilidad de un evento y su ocurrencia.

**Seguridad de la Información:** Preservación de confidencialidad, integridad y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad.

**Sistema Informático:** Constituido por el conjunto de computadores, software asociado, periféricos, terminales, 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.

**Software malicioso:** También conocido como **Malware** (del inglés "malicious software") entendiéndose por tal todo software que tiene como objetivo infiltrarse en un sistema informático y dañar la (o las) computadora(s) que lo sustenta(n) sin el conocimiento de su dueño, con finalidades muy diversas. En esta categoría, encontramos desde Virus informáticos hasta Troyanos y Spyware.

El Malware hace referencia a una variedad de software o programas de códigos hostiles e intrusivos. Se debe considerar que el ataque a la vulnerabilidad por malware, puede ser a una aplicación, una computadora, un sistema operativo o una red completa.

**Tecnología de la Información y de las Comunicaciones (TIC):** Constituida por la agrupación de los elementos y las técnicas utilizadas en el tratamiento y la transmisión de la información, principalmente de informática, internet y telecomunicaciones.

**WAN:** Redes de área extendida, que constituyen la interconexión de distintos tipos de redes, en un ámbito global.