MVC y antecedentes

4

Gobierno de Chile

VMA/JJDA/KGR/JMS/JSP/PAP
12

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARÍA DE EDUCACIÓN Y DEJA SIN EFECTO DOCUMENTO QUE INDICA.

MINISTERIO DE EDUCACION
30 AGO 2016
DOCUMENTO TOTALMENTE TRAMITADO

Solicitud N° 4274

SANTIAGO, 11 AGO 2016

RESOLUCIÓN EXENTA N° 3862

VISTO:

Lo dispuesto en la Ley N° 18.956, que Reestructura el Ministerio de Educación Pública; en la Ley N° 19.223, que Tipifica Figuras Penales Relativas a la Informática; en la Ley N° 19.628, Sobre Protección de la Vida Privada; en La Ley N° 19.799, Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma; en la Ley N° 20.285, Sobre Acceso a la Información Pública; el DFL N° 29 de 2004, que fija el texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en el Decreto N° 181, de 2002, del Ministerio de Economía, que Aprueba el Reglamento de la Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha Firma; en el Decreto N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónico; en el Decreto N° 93, de 2006, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para la Adopción de Medidas Destinadas a Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos Masivos no Solicitados Recibidos en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios; en la Resolución Exenta N° 4.503, de 11 de julio de 2014, de este origen, que estableció la función de Encargado de Seguridad de la Información; en la Resolución Exenta N° 6.957, de 2015, de Educación, que modifica el Comité de Seguridad de la Información; y, en la Resolución N° 1.600, de 2008, de la Contraloría General de la República.

CONSIDERANDO:

Que, esta Secretaría de Estado, en conformidad a lo dispuesto en el artículo 1°, de la Ley N° 18.956, que Reestructura el Ministerio de Educación, tiene a su cargo entre otras funciones, el fomentar el desarrollo de la educación en todos sus niveles.

Que, con la finalidad de cumplir esas funciones, ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes Activos, que permiten interactuar con la comunidad escolar, la ciudadanía en general y, los integrantes del Ministerio de todo el país.

Que, por la relevancia de la información contenida en la plataforma tecnológica, se hace necesario establecer normas que regulen su correcto uso, a través de las distintas actividades que el personal del Ministerio de Educación realiza en el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los servicios e información.

Que, en definitiva, es necesario establecer los requisitos y condiciones generales de seguridad a las que se encuentra sujeto el Ministerio y sus funcionarios, 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.

Que, con el fin de apoyar la organización de la seguridad de la información, este Ministerio modificó mediante la Política de Seguridad de la Información, aprobada mediante la Resolución Exenta N° 6.957, de 27 de octubre del 2015, de Educación, el Comité de Seguridad de la Información.

Que, esta Subsecretaría 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 y almacenamiento. Por lo tanto, el personal que integra la organización será responsable de velar por su confidencialidad, integridad y disponibilidad según lo que su cargo y función le corresponda administrar y gestionar, de conformidad al marco legal actualmente vigente.

Que, para dar pleno cumplimiento a la obligación de resguardo antes descrita y con la necesidad de actualizar el manejo de datos al interior de esta subsecretaría de Educación, es necesario actualizar la política de seguridad que se encuentra actualmente vigente y, en ese sentido, dejar sin efecto el documento anterior que la contiene.

RESUELVO:

I. **Apruébese** la siguiente política de seguridad de la información para la Subsecretaría de Educación:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PARA LA SUBSECRETARÍA DE EDUCACIÓN.

FIRMA DE LOS RESPONSABLES

ELABORADO POR Ricardo Cid Fuentes	REVISADO POR Ramón Rodríguez Matte	APROBADO POR Fernando Rojas Ochagavía
Encargado de Seguridad	Coordinador Nacional de Tecnologías e Innovación	Presidente Comité de Seguridad de la Información
REVISION (NRO. 2) Juan Antonio Serrano	REVISADO POR Jonny Heiss Schmidt	APROBADO POR Valentina Quiroga Canahuate
Encargado de Seguridad	Coordinador Nacional de Tecnologías	Jefe de Servicio
REVISION (NRO. 2) Juan Antonio Serrano	REVISADO POR Jonny Heiss Schmidt	APROBADO POR Valentina Quiroga Canahuate
Encargado de Seguridad	Coordinador Nacional de Tecnologías	Jefe de Servicio

CONTROL DE VERSIONES

REVISIONES DEL DOCUMENTO DE POLÍTICA				
Nº Revisión	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
0(Cero)	2010	Elaboración inicial	Todas	
1	3/11/2011	Modificación 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 la información (Nch-ISO 27001-2009).	Tapa, Índice, 6,8,8,10	Ricardo Cid
2	10/7/2015	Se actualiza Política de Seguridad de la Información según Norma Chilena NCh ISO 27001:2013. Se modifica la constitución del comité de Seguridad de la Información.	Todas	Jonny Heiss

3	20/07/2016	Se actualiza Política de Seguridad de la Información según Norma Chilena NCh ISO 27001:2013. Se realizan cambios mayores quedando la organización de la seguridad, gestión de la seguridad, y gestión de la continuidad.	Todas	Jonny Heiss

1. DECLARACIÓN INSTITUCIONAL.

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

De esta manera, reconoce que la información que posee es un bien estratégico para sus funciones, por lo que se requiere que sea protegida y resguardada durante todas las actividades en que es utilizada. Por lo tanto, todo el personal que integra la organización será responsable de mantener la estricta confidencialidad, integridad y disponibilidad de la información que, por cargo y función, les corresponde administrar y gestionar, de conformidad al marco legal actualmente vigente.

Para apoyar el cumplimiento de sus funciones, esta Subsecretaría de Educación ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacenan datos y antecedentes mediante diferentes activos, que permiten la interacción de la comunidad escolar, ciudadanía en general y los integrantes del Ministerio en todo el país, con la información requerida para dar cumplimiento a las funciones que el referido mandato legal exige, considerando que aquella resguardada, puede ser propia de los sistemas de esta Subsecretaría de Educación, de los servicios o sus procesos, así como también de los usuarios internos o externos.

Así, es de alta importancia el correcto manejo de los activos de información, entendiéndose por tales a todo elemento en que se registre, almacene y/o procesen datos, sea a través de medios tecnológicos u otros soportes, tales como: bases de datos y archivos, contratos y acuerdos, documentación de sistemas, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de continuidad operativa, información de auditorías, información archivada, activos de software, activos físicos como salas de computación, computadores y servidores, impresoras y redes de comunicaciones y servicios.

Debe considerarse además, que la Subsecretaría de Educación, tanto en sus sistemas de información, como en las respectivas redes, está enfrentando en

forma creciente, constantes amenazas de seguridad desde una amplia gama de fuentes, tales como hechos naturales, fallas propias en los equipos, aplicaciones, o bien ataques intencionales, por lo que sus sistemas informáticos requieren estar total e integralmente protegidos, asegurando la continuidad operacional de los procesos.

Lo anterior significa el deber de preparación adecuado, en orden a reaccionar adecuadamente en caso de situaciones o eventos inesperados que impliquen una interrupción de los procesos de provisión de productos estratégicos[1] . Para ello, es necesario desarrollar las estrategias y planes que reculsen necesarios para actuar de una manera eficaz, oportuna, ordenada y sistemática.

2. OBJETIVOS

Los objetivos de esta política son:

1. Establecer normas que regulen el uso y manejo de los activos de información de la Institución, a través de las distintas actividades que el personal de la Subsecretaría de Educación realiza en el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los mismos.
2. Establecer los requisitos y condiciones generales de protección y resguardo de seguridad a las que se encuentra sujeta esta Subsecretaría, 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.

3. ALCANCE

La seguridad de la información es de responsabilidad de la totalidad de los (as) usuarios que se relacionan con la Subsecretaría de Educación y que tengan acceso a los Activos de Información de esta Cartera de Estado, sean estos (as) funcionarios (as) de planta, contrata u honorarios e incluyendo asesores (as), consultores (as), practicantes y, en general, toda aquella persona natural o jurídica que preste servicios a la Subsecretaría de Educación. Por tal razón, las políticas establecidas en este documento son de conocimiento y cumplimiento obligatorio para todos (as) los (as) funcionarios (as) y personas en general, a los que se les otorgue acceso a estos activos. En el caso de los (as) externos (as), dicha obligación deberá expresarse en los contratos y/o acuerdos respectivos.

[1] Se entenderá por procesos estratégicos aquellos identificados en la Ficha de Definiciones Estratégicas de la Subsecretaría de Educación (Formulario A1), que publica la Dirección de Presupuesto.

4. ROLES Y RESPONSABILIDADES

1. Subsecretario (a) de Educación.

En su calidad de Jefe (a) de Servicio le corresponde la aprobación de esta Política de Seguridad y de sus futuras modificaciones.

2. Encargado (a) de Seguridad de la Información.

Sin perjuicio de las funciones específicas definidas por la autoridad a través de Resolución Exenta que lo designe y, asimismo, de las competencias definidas para el cargo que desarrollará el Encargado de Seguridad de la Información, sus funciones incluirán a lo menos:

I. Tener a su cargo el desarrollo inicial de las políticas de seguridad y el control de su implementación, velar por su correcta aplicación y por su oportuna actualización, cuando los cambios externos lo requieran.

II. Coordinar la respuesta a incidentes de seguridad de la información.

III. 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.

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

3. El (a) Coordinador (a) Nacional de Tecnología.

Por su parte, el (la) Coordinador (a) Nacional de Tecnología tomará las medidas necesarias para resguardar los activos de información y mantener su disponibilidad, confiabilidad e integridad, de acuerdo a las directrices establecidas por la Resolución Exenta N° 4.505, de 2014, de este origen y, asimismo todas aquellas que se señalan en la presente Política, controladas por el Comité de Seguridad de la Información.

Por su parte y, en el ámbito de la seguridad de la información, sus funciones incluirán, a lo menos:

a) Asegurar el adecuado funcionamiento de las redes, enlaces y plataformas que permitan la efectiva operación del Ministerio de Educación;

b) Proponer la adquisición para la implementación y administración de la infraestructura informática necesaria que sustente la operación de los distintos sistemas;

c) Proponer y asegurar el funcionamiento de las medidas de seguridad que resguarden la confidencialidad, integridad y disponibilidad de la

información, en conformidad a las instrucciones impartidas por el Comité de Seguridad de la Información;

d) Proponer disposiciones generales para el uso de activos de información;

e) Proponer capacitaciones pertinentes para el personal de la Subsecretaría de Educación;

f) Realizar capacitaciones a dicho personal referidas a la política de seguridad informática y de procedimientos de la Coordinación Nacional de Tecnología (CNT), en las competencias requeridas conforme al perfil de cada cargo.

5. ORGANIZACIÓN DE LA SEGURIDAD

La Subsecretaría de Educación mantendrá una organización para la toma de decisiones y el gobierno de la Seguridad de la Información. De esta manera, mediante el denominado "***Comité de Seguridad de la Información y Continuidad del Servicio***", se determinará, autorizará y vigilará los controles y prácticas de seguridad que ayuden a mejorar los niveles de protección y resguardo de sus activos.

Este órgano deberá dictaminar marcos de trabajo sobre seguridad y continuidad, que incluya la relación con entidades externas a la institución y/o terceros que presten servicios de cualquier índole a esta Subsecretaría de Educación.

Asimismo, estará constituido por autoridades y funcionarios claramente definidos, que tendrán como misión "velar por la confidencialidad, integridad y disponibilidad de la información, y por la Continuidad de los Servicios del Ministerio, con foco en sus productos estratégicos.

6. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Subsecretaría de Educación mantendrá una organización para la gestión de la seguridad de la información basado en los requisitos de la norma NCh-ISO 27001:2013, a través de un programa de implementación de controles de seguridad basado en las recomendaciones NCh-ISO 27002:2013 y, en cumplimiento con lo establecido en la legislación vigente.

Por lo anterior, las siguientes estipulaciones normativas se entienden parte de esta política.

1. La Política de Seguridad de la Información de esta Subsecretaría de Educación, contenida en este documento, establece los lineamientos generales con respecto al buen uso de los activos de información, tanto

compartidos como de cada uno de los (as) usuarios (as) internos o externos.

2. Estas directrices de carácter general, 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 su cumplimiento.
3. A partir de esta política general de seguridad de la información se elaborarán documentos específicos relativos a la materia, que establecerán los requisitos de seguridad y los dominios que la norma identifica.
4. Es responsabilidad de todos los (as) funcionarios (as) de la Subsecretaría de Educación y, los terceros relacionados con el manejo de los activos de información de la Institución, hacer uso de los mismos en forma autorizada y en directa y exclusiva relación con las funciones que desempeñan y, en concordancia con la normativa existente y el marco legal.
5. Asimismo, de reportar cualquier situación o evento que pueda exponer o afectar la integridad, confidencialidad o disponibilidad del mismo, de acuerdo a los procedimientos publicados en la Intranet para estos efectos. En relación a lo mismo, sólo funcionarios (as) específicos (as) tienen las atribuciones para determinar y calificar la real exposición de los activos en los eventos o situaciones que se informan.
6. Asimismo, la institución reconoce que las actividades de capacitación, concientización y sensibilización de sus funcionarios (as) en materias de seguridad de la información, es una tarea que debe realizarse de manera permanente, en el marco de los recursos disponibles.

7. GESTION DE LA CONTINUIDAD DE LOS SERVICIOS

La Subsecretaría de Educación establecerá lineamientos por medio de la dictación de una política específica y, asimismo, determinará las prácticas de gestión de continuidad del servicio mediante una estructura de gobernabilidad que administre los ciclos del Sistema de Gestión de Continuidad de Servicios (SGCS). Para tales efectos considerará aspectos tales como: identificación de las amenazas potenciales, evaluación del riesgo y su impacto en los procesos estratégicos de la subsecretaría de Educación, la definición de estrategias de continuidad en los ámbitos de personas, información y datos, infraestructura, tecnologías de información y comunicaciones, financiamiento y proveedores y

la elaboración de los planes y procedimientos de continuidad, en los niveles que corresponda.

Todo proceso de la institución que sea declarado como estratégico o que tenga relación con un servicio que sea prestado a la Comunidad, debe considerar:

1. La definición y documentación de las estrategias de prevención, contención y recuperación del servicio ante eventos detonantes de contingencias, desastres o emergencias.
2. El establecimiento de estrategias, reglas y planes para enfrentar desastres que comprometan la continuidad del servicio.
3. Los lineamientos esenciales establecidos mediante acuerdos tomados por el Comité de Seguridad de la Información y Continuidad del Servicio, en la construcción de planes de continuidad y de recuperación en relación a materias relacionadas a la criticidad de los servicios, los plazos de recuperación de los mismos y el nivel de servicio asociado, a modo de ejemplo.
4. Que cada Plan de Continuidad cuente con un responsable de su mantención y vigencia en el tiempo. Además, debe estar regularmente actualizado y difundido, de modo que no pierda operatividad con los cambios a los sistemas o procesos de negocio.
5. Asimismo, éstos deben probarse en forma recurrente de modo que todas las personas de la Institución que participan en él, estén preparados para su puesta en operación, cuando sea necesario.
6. Que, en el caso de fallas operativas normales y mantenciones de sistemas, sean los dueños de los servicios, las personas responsables por desarrollar y mantener los procedimientos de recuperación asociados.
7. Se debe planificar con anticipación, todos aquellos cambios a la capacidad de equipos, en orden a asegurar la disponibilidad de los recursos y, a la evaluación del posible impacto en los planes de contingencia y procedimientos de recuperación.

8. GLOSARIO DE TÉRMINOS

Activo: aquello que tenga valor para la organización.

Activo de información: todo elemento en que se registre, almacene y/o procese datos e información, sea a través de medios tecnológicos u otros soportes, tales como: bases de datos y archivos, contratos y acuerdos, documentación de

sistemas, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de continuidad operativa, información de auditorías, información archivada, activos de software, activos físicos como salas de computación, computadores y servidores, impresoras y redes de comunicaciones y servicios

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Continuidad del servicio: capacidad de la organización para continuar entregando productos o servicios a niveles aceptables predefinidos tras un incidente que interrumpa.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del servicio y amenazar la seguridad de la información.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Sistema de Gestión de Continuidad de Servicios: parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del servicio.

Sistema de Gestión de Seguridad de la Información: parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, *operar, monitorear, revisar, mantener y mejorar la seguridad de la información.*

9. ACCIONES DISCIPLINARIAS.

La infracción a las obligaciones establecidas anteriormente, podrá constituir una violación al principio de probidad administrativa y por ello, será sancionada en conformidad a lo dispuesto en el D.F.L. N° 29, de 2004, del Ministerio de Hacienda, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo, respecto de los dependientes que detentan la calidad de funcionarios públicos, ya sea Titulares o a Contrata. Todo lo anterior, sin perjuicio de la responsabilidad civil o penal que pudiera concurrir.

Por su parte y, respecto del personal a Honorarios o de carácter Externo a la subsecretaría de Educación, la infracción a las obligaciones que son materia de

la presente política, podrá constituir causal suficiente para producir el término inmediato y anticipado del respectivo contrato que los vincule con la subsecretaría de Educación, sin perjuicio de otras responsabilidades civiles o penales, que la infracción pudiere irrogarles.

En esta materia, la Coordinación Nacional de Tecnología aplicará las medidas necesarias para monitorear el cumplimiento de esta política, mantendrá a los usuarios informados sobre nuevas amenazas y cuidados con respecto al resguardo de los activos de información, de manera de evitar incidentes producidos por el no cumplimiento de esta Política.

10. VIGENCIA.

Esta política entra en vigencia, una vez que el acto administrativo que la contiene, se encuentre totalmente tramitado.

Las revisiones de la presente Política de Seguridad de la Información se realizarán cada tres años, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad de la organización. Todo el personal de la Subsecretaría de Educación, deberá tomar conocimiento por escrito de la presente política, la cual se encontrará en formato electrónico en la Intranet para futuras consultas.

11. LEGISLACIÓN.

Ley N° 17.336, de Propiedad Intelectual, y sus actualizaciones

Ley N° 19.223, que Tipifica Figuras Penales relativas a la Informática.

Ley N° 19.628, sobre Protección de la Vida Privada. Última Modificación 17-FEB-2012 Ley 20.575.

Ley N° 19.799 Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

Ley N° 20.285, sobre Acceso a la Información Pública.

D.F.L. N° 29, de 2004, de Hacienda, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo.

Decreto Supremo N° 83 del 2005 Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

Decreto Supremo N° 93 del 2006 Ministerio Secretaría General de la Presidencia, que aprueba Norma Técnica para la Adopción de Medidas Destinadas a

Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos Masivos no Solicitados Recibidos en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios.

Norma Chilena NCh-ISO27001:2013 sobre "Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos".

Norma Chilena NCh-ISO22301:2013 sobre "Seguridad de la sociedad - Sistemas de gestión de la continuidad del negocio – Requisitos".

II. **Déjese sin efecto** la Resolución Exenta N° 6.957, de 2015, de Educación.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

REPUBLICA DE CHILE
MINISTERIO DE EDUCACIÓN
SUBSECRETARIA

VALENTINA KARINA QUIROGA CANAHUATE
SUBSECRETARIA DE EDUCACIÓN

Distribución:

- Gabinete Sra. Ministra
- Gabinete Sra. Subsecretaria de Educación
- División Jurídica – Comité de Control, Transparencia y ADP.
- División de Administración General.
- Coordinación Nacional de Tecnología Subsecretaría de Educación.
- Oficina de Partes y Archivos Nivel Central.
- Archivo.
  Expediente N°s 23.352-2016