Gobierno de Chile

Superintendencia de Educación

MPV/MRA/XBG/CNN/PCC/LDZ/HCJ/PBC/PSY

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°2196, DE FECHA 25 DE NOVIEMBRE DE 2016 Y APRUEBA POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN VERSIÓN N°2, EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0827

Santiago,

01 DIC 2017

VISTO:

Lo dispuesto en el DFL Nº 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en el Decreto con Fuerza Ley Nº 29, de 2004, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley Nº 18.834, sobre Estatuto Administrativo; en la Ley Nº 19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; en el Decreto N°571, de 2014, del Ministerio de Educación; en la Ley Nº 20.529, de 2011, del Ministerio de Educación, sobre el Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización; en el Decreto con Fuerza de Ley Nº 5, de 2012 ,del Ministerio de Educación; la Norma Chilena NCh-ISO 27001/2013, tecnología de la información-técnicas de seguridad-sistemas de gestión de la seguridad de la información; en la norma Chilena NCh-ISO 27002-2013, tecnología de la información- código de prácticas para la gestión de la seguridad de la información, y la Resolución N°1600 de 30 de octubre de 2008, de Contraloría General de la República, que fija las normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que, de acuerdo a lo dispuesto en el artículo 47 de la Ley N°20.529, sobre el Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su fiscalización, se crea la Superintendencia de Educación, como "un servicio público funcionalmente descentralizado y territorialmente desconcentrado, dotado de personalidad jurídica y patrimonio propio y que se relaciona con el Presidente de la Republica por intermedio del Ministerio de Educación".

2. Que, en atención a que los Órganos de la Administración del Estado tienen la obligación de respetar la normativa vigente respecto de la Seguridad de la Información, esta Superintendencia procedió a la designación de un Encargado de Seguridad de la Información, que actuará como asesor del Jefe de Servicio en las materias relativas a la seguridad de los documentos electrónicos y los activos de información institucionales.

3. Que, con fecha 25 de noviembre de 2016 se dicta Resolución Exenta N°2196, de esta Superintendencia que aprobó la Política de gestión de incidentes de seguridad de la información versión N°1.

4. Que, debido a una serie de cambios institucionales y a la revisión efectuada por el Encargado de Seguridad de la Información se ha estimado procedente, reestructurar y ajustar el contenido de la Política de gestión de incidentes de seguridad de la información versión N°1, aprobada mediante Resolución Exenta N°2196 de fecha 25 de noviembre de 2016.

RESUELVO:

1. **DÉJESE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 2196, de 2016 de la Superintendencia de Educación.

2. **APRUÉBASE,** la Política de gestión de incidentes de seguridad de la información versión N°2, de la Superintendencia de Educación, cuya transcripción, fiel, exacta e integra se adjunta a la presente Resolución.

3. **ESTABLÉZCASE,** la obligación de el/la Encargado/a de Seguridad de la Información de la Superintendencia de Educación, de difundir la política fijada por este instrumento y de velar junto con el comité de Seguridad de la Información por su estricto cumplimiento.

4. **DISPÓNGASE,** que el/la Jefe/a de la División de Administración General, deberá tomar todas las medidas y acciones tendientes a la implementación de esta política.

5. **DÉJESE,** expresa constancia que la presente Resolución Exenta no erogará gasto alguno para esta Superintendencia de Educación.

6. **PUBLÍQUESE,** una vez totalmente tramitada la presente Resolución Exenta, en la Intranet institucional y el sitio web www.supereduc.cl.

ANÓTESE, COMUNIQUESE Y ARCHÍVESE.

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACION
SUPERINTENDENTE

ALEXIS RAMÍREZ ORELLANA
SUPERINTENDENTE
SUPERINTENDENCIA DE EDUCACIÓN

Superintendencia de Educación
TOTALMENTE TRAMITADO

Distribución:
1. Gabinete.
2. División de Fiscalización.
3. División de Fiscalía.
4. División de Promoción y Resguardo de Derechos Educacionales.
5. Intendencia de Educación Parvularia.
6. División de Administración General.
7. Departamento de Finanzas.
8. Departamento Gestión de Personas.
9. Departamento de Administración.
10. Departamento de Tecnologías de Información.
11. Direcciones Regionales (15).
12. Departamento de Auditoría.
13. Coordinación de Gestión y Desarrollo.
14. Oficina de Partes.

POLÍTICA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 2.0

CONTROL ISO27002:2013

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.6

A.16.1.7

INDICE

1. Objetivo:

Administrar eficaz y eficientemente los incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, sistemas de información, medios físicos de almacenamientos y las personas, que afecten la continuidad operacional de los procesos críticos de la Superintendencia de Educación (SUPEREDUC).

2. Alcance:

Esta política se aplica a todas las áreas de SUPEREDUC y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas, y a todas las dependencias y servicios de SUPEREDUC, afectados por cualquier incidente que comprometa la confidencialidad, integridad o disponibilidad de la información o de los sistemas, detectados en forma interna o externa.

Es aplicable a todos los Usuarios[1], ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo empresas que presten servicios a la SUPEREDUC.

Esta política contempla los siguientes controles definidos en la norma NCh-ISO 27001:2013

- A.16.01.01 Responsabilidades y procedimientos.
- A.16.01.02 Informe de eventos de seguridad de la información.
- A.16.01.03 Informe de las debilidades de la seguridad de la información.
- A.16.01.04 Evaluación de y decisión sobre los eventos de seguridad de la información.
- A.16.01.06 Aprendizaje de los incidentes de seguridad de la información.
- A.16.01.07 Recopilación de evidencia.

3. Roles y Responsabilidades:

- **Jefaturas Directas:**
  - Velar por el correcto cumplimiento de esta política.
- **Departamento de Tecnologías de Información:**
  - Dar solución a los incidentes de seguridad TI detectados y normalizar la entrega de los servicios.
  - **Gestor de Servicios TI:**
    - Registrar, clasificar y escalar los eventos de seguridad reportados.
- **Encargado de Seguridad de la Información**:
  - Debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

[1] Se entiende por Usuarios a los funcionarios/as en calidad jurídica planta, contrata, personas contratadas a honorarios suma alzada y terceros que trabajen para SUPEREDUC

- Debe evaluar todos los incidentes seguridad de acuerdo a sus circunstancias particulares y escalar al comité de incidentes de seguridad de la información aquellos en los que se considere pertinente.
- Velar por el correcto funcionamiento y operación de la gestión de incidentes de seguridad TI y no TI, mantener un registro de los incidentes reportados y gestionar la base de conocimiento generada por las lecciones aprendidas.
- Difundir esta política.

- **Comité de Incidentes de Seguridad de la información:**
  - Debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- **Usuarios**
  - Declarar cualquier evento sospechoso que pudiera desencadenar un incidente de Seguridad de la Información.

4. Definiciones:

a) **Integridad:** Es la propiedad que busca proteger que no se modifiquen los datos de forma no autorizada.

b) **Disponibilidad:** Es el acceso autorizado a la información y a los sistemas en el momento que se requiera por una persona autorizada.

c) **Confidencialidad:** Es la propiedad que impide la divulgación a individuos, entidades o procesos no autorizados. Es decir, asegura el acceso únicamente a aquellas personas que cuenten con una debida autorización.

d) **Incidente de seguridad:** Cualquier evento o situación que comprometa de manera IMPORTANTE la **disponibilidad**, **integridad** y/o **confidencialidad** de los activos de información (documentos, plataforma tecnológica, procesos, sistemas, etc.). También se considera un incidente de seguridad la violación o no cumplimiento de una política o procedimiento.

e) **Incidente de Alto Impacto:** Interrupción de los procesos de la institución que afecta a un número significativo de usuarios.

f) **Urgencia Alta:** Tiempo máximo de demora que puede aceptar el proceso para la resolución del incidente.

5. Documentos Relacionados

a) Procedimiento de contacto con autoridades.

b) Procedimiento de reporte de eventos y debilidades de seguridad de la información.

c) Procedimiento de evaluación e informe de incidentes.

d) Procedimiento de Gestión de Evidencias de Incidentes.

e) Documento Técnico N°91.

f) Ley de delitos informáticos.

g) Ley 18.834 sobre estatuto administrativo.

h) Documento Técnico Nº91- MINSEGPRES respecto delitos funcionarios.

6. Política

6.1. Reporte de eventos y debilidades en la Seguridad de la Información

Todo el personal de SUPEREDUC, en coordinación con su jefatura, es responsable de notificar cualquier tipo de evento que pueda afectar el normal funcionamiento del Sistema de Seguridad de la Información. Esta notificación se realizará a través del email mesadeservicio@supereduc.cl o al anexo 55555, indicando todos los antecedentes del evento, el cual será derivado según su clasificación y criticidad. En la medida de lo posible, se debe evitar realizar acciones sin el apoyo técnico correspondiente.

Una vez realizado el análisis inicial de los antecedentes recopilados, se debe establecer si el evento corresponde a un requerimiento, una debilidad o un incidente de Seguridad de la Información.

6.2. Gestión de incidentes de seguridad

6.2.1. Registro y Clasificación del Incidente

a) **Registro:** El Gestor de Servicios TI debe registrar el incidente según lo descrito en el "*Procedimiento de reporte de evento y debilidades de seguridad de la información*".

b) **Clasificación:** El Gestor de Servicios TI debe clasificar el incidente de acuerdo al origen, tipo y nivel de criticidad.

Los tipos de incidentes y criticidad están detallados en el "*Procedimiento de evaluación de incidentes de seguridad de la información*".

6.2.2. Análisis y Gestión de Riesgo

Con los antecedentes recopilados se realizará un análisis respecto del tipo de incidente, alcance y nivel de criticidad y se determinará el tratamiento al riesgo, se asume, se transfiere, se mitiga o se elimina.

a) **Mitigar el riesgo**: Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

b) **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la Dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

c) **Transferir el riesgo a un tercero:** Asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

d) **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

6.2.3. Escalamiento

Si el Gestor de Servicios TI determinará si el incidente detectado requiere un tratamiento urgente, de ser así, debe procederse con la mayor celeridad posible e informar al Encargado de Seguridad de la Información quien instruirá la respuesta inmediata.
Cada vez que se registre un incidente de SI, se debe informar a los responsables de ejecutar las acciones inmediatas según sea el tipo de incidentes para su rápida resolución y respuesta.

En el caso de que no se pueda resolver el problema, se realiza un escalamiento interno. Para cada tipo de incidente se avisa a la persona correspondiente. El criterio principal del escalamiento es el de la transferencia a una persona de soporte más elevado, que tenga mayor conocimiento o experiencia, recursos para solucionar situaciones complejas y mayor poder en la toma de decisiones, de acuerdo a lo detallado en "*Procedimiento de reporte de eventos y debilidades de seguridad de la Información".*

6.2.4. Respuesta inmediata

La jefatura designada para la respuesta inmediata al incidente, es responsable del desarrollo de las siguientes acciones inmediatas: Registro de actividades de gestión de incidentes.

Actividad	Descripción
Contener el daño y minimizar el riesgo	Evitar que se propaguen los daños o efectos del incidente, coordinando las actividades necesarias para su disminución, probabilidad y consecuencia.
Reclasificar el incidente	Si es necesario, reclasificar según lo descrito en el *Procedimiento de Evaluación de Incidentes de Seguridad de la Información.*
Proteger las evidencias	Resguardar las evidencias recopiladas durante la gestión del incidente.
Notificar a terceros relevantes	Cuando sea necesario, notificar a organismos externos (carabineros, bomberos, PDI, etc.), según lo descrito en el *Procedimiento de Contacto con Autoridades Críticas.*

Actividad	Descripción
Compilar y organizar la documentación del incidente	Recopilar todos los antecedentes y evidencias relacionados con el incidente y entregarlos al Encargado de SI
Entregar lineamientos para la respuesta al incidente	El Encargado de SI, debe apoyar a la jefatura correspondiente en esta etapa, para responder de manera adecuada al incidente detectado.

6.2.5. Continuidad de las operaciones y servicios

En caso de que el incidente no pueda ser controlado y ponga en riesgo las operaciones y entrega de servicios de SUPEREDUC, el Encargado de SI, el Jefe del Departamento de Tecnologías de Información y el Comité de Incidentes de Seguridad de la Información evaluarán la pertinencia de activar el Plan de Continuidad de Operaciones.

6.2.6. Recolección de evidencia

La recolección de evidencia es responsabilidad del Encargado de SI. Ésta debe ser clara y suficiente para respaldar el incidente. Para ello se debe considerar lo siguiente:

Información en formato papel: El original se debe guardar de manera segura con información del individuo que encontró el documento, dónde y cuándo fue encontrado y quién fue testigo del descubrimiento. Se debe procurar que el documento original no sea adulterado intencional o accidentalmente.

Información en formato digital: Las imágenes o copias de cualquier medio removible, la información contenida en discos duros o en memorias, deben ser retenidas de manera segura para garantizar su disponibilidad. El registro de todas las acciones durante el proceso de copiado, se debe guardar y el proceso se debe realizar en presencia de testigos. Los medios originales y el registro se deben guardar de manera segura, evitando la adulteración de la evidencia.

Cualquier trabajo forense se debe realizar sólo sobre copias del material de evidencia. Se debe supervisar y registrar cuándo y dónde fue ejecutado el proceso, quién lo ejecutó y qué herramientas y/o programas se utilizaron.
Esta información es entregada al Comité de Incidentes de Seguridad de la Información, para la evaluación y aprendizaje del incidente y eventuales acciones legales y disciplinarias.

6.2.7. Resolución del incidente

La resolución de un incidente de seguridad de la información, se realizará de acuerdo a los procedimientos específicos definidos para cada caso.

6.2.8. Comunicación

Aquellos incidentes clasificados como **Alto Impacto** o **Urgencia Alta,** deben ser gestionados, informando a todos los involucrados durante el proceso de resolución y cierre de los mismos.

6.2.9. Análisis de causa y cierre

En esta etapa el Encargado de SI debe:

a) Realizar un análisis de causa del incidente.
b) En caso de ser necesario, debe diseñar e implementar un plan de acción adecuado que prevenga incidentes futuros.
c) Registrar el cierre del incidente en sistema de gestión de incidentes.
d) Aplicar lecciones aprendidas y ajustar los procedimientos y vías de comunicación con el objeto de contar con mejores herramientas para un eventual futuro incidente.
e) Tomar las medidas para que se cuantifiquen las pérdidas económicas, si las hubiere.
f) Preparar un Informe ejecutivo al Comité Directivo de Seguridad de la Información y Comité Operativo según corresponda, dependiendo de la magnitud e impacto del incidente.

7. Publicación y comunicación de esta política

La comunicación de esta política se efectuará de manera que los contenidos de la documentación sean accesibles y comprensibles para todos los usuarios, pudiéndose utilizarse los canales de difusión establecidos por la SUPEREDUC (Intranet, Email, circulares, etc).

8. Aceptación de la política

Todos los usuarios de la SUPEREDUC, sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar ésta política y procedimientos relacionados.

Para el caso de terceros y por solo hecho de participar en algún proceso de compras del servicio, el oferente debe dar cumplimiento a la política y procedimientos vigentes de seguridad de la información de la SUPEREDUC, publicados en el sitio web www.supereduc.cl y sus correspondientes modificaciones, la cuales se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

9. Revisión de la política

La presente política será evaluada y revisada al menos una vez al año, o cuando SUPEREDUC lo requiera, para asegurar su continuidad e idoneidad, considerando cambios externos o internos que puedan afectarla.

10. Sanciones aplicables

El incumplimiento o violación a esta política, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios/as de la SUPEREDUC, o al término anticipado del contrato por incumplimiento de obligaciones,

cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

11. Control de versiones:

Control de versiones		
Versión	**Resumen de cambios**	**Fecha**
1.0	- Versión inicial	Octubre 2016
2.0	- Punto 2.0, se incorpora al alcance las definiciones de Ficha A1 y los controles de la norma Nch:27.001 desarrollados en esta política. - Punto 5, se elimina NchISO27001:2013 y NchISO27002:2013. - Puntos 6.1, se modifica email de contacto y anexo de mesa de servicios TI. - Punto 9, se incorpora la evaluación y revisión anual de la política. - Punto 11, se modifica formato de tabla.	Noviembre 2017

12. Responsabilidades de elaboración y aprobación del documento:

Elaborado Por	Revisado Por	Aprobado Por
Encargado de Seguridad de la Información	Comité Operativo de SSI	Comité Directivo SSI