Gobierno de Chile

Superintendencia de Educación

MPV/CNN/HCJ/DSC/PSY

APRUEBA POLÍTICA DE SEGURIDAD PARA LA GESTIÓN DE CAMBIOS A LOS SERVICIOS DEL PROVEEDOR, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN, EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0720

SANTIAGO, 20 OCT 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 Medica 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 17/10/2017 se dicta resolución exenta N°0703, de esta Superintendencia que aprobó la Política General de Seguridad de la Información.

4. Que, con la finalidad de hacer efectiva la política antes mencionada, resulta necesario establecer Políticas específicas de Seguridad de la Información, dentro de los cuales se encuentra la que regula la Política de seguridad para la gestión de cambios a los servicios del proveedor.

RESUELVO:

1. **APRUÉBASE,** la Política seguridad para la gestión de cambios a los servicios del proveedor versión N°1, en la Superintendencia de Educación, cuya transcripción, fiel, exacta e integra se adjunta a la presente Resolución.

2. **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.

3. **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.

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

5. **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 RAMIREZ ORELLANA
SUPERINTENDENTE
SUPERINTENDENCIA DE EDUCACIÓN

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.

Superintendencia de Educación
TOTALMENTE TRAMITADO

POLÍTICA GESTIÓN DE CAMBIOS A LOS SERVICIOS DEL PROVEEDOR

VERSIÓN 1.0

CONTROL ISO27001:2013
A.15.2.2

ÍNDICE

1. Objetivo:

Definir las reglas de seguridad para el resguardo de la información personal sensible para la gestión de los proyectos y monitoreo de los acuerdos de servicio, en los procesos relacionados de compra y administración de los servicios al interior de la Superintendencia de Educación (SUPEREDUC).

2. Alcance:

Esta política es aplicable a los proyectos o servicios donde se encuentre involucrado el uso o tratamiento de datos sensibles, según lo declara la Ley 19.628.

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

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

- A.15.02.02 Administración de cambios en los servicios del proveedor.

3. Roles y Responsabilidades:

3.1. Jefe de División o Departamento:

Definir a un funcionario o equipo, responsable de la administración de proyectos y los acuerdos de servicios.

3.2. Funcionario o equipo responsable:

Dar cumplimiento a los requisitos definidos en esta política en la administración de proyectos y los acuerdos de servicio.

3.3. Encargado/a de Seguridad de la Información:

Gestionar los incidentes de seguridad de la información relacionados a los incumplimientos de la presente política.

4. Definiciones:

a) **Activos de Información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información. Para el presente documento considera especialmente: bienes con cargo, los accesos habilitados a sistemas y recursos informáticos y la información de valor para la Institución que generen las personas como resultado de la evaluación que realiza el funcionario/a y su jefatura directa.

[1] Se entiende por Usuarios a los funcionarios/as en calidad jurídica planta, contrata, reemplazos y suplencia, tanto para el personal a honorarios y terceros (proveedores, compra de servicios, etc.) que trabajen para SUPEREDUC.

b) **Incidente de seguridad:** Cualquier evento o situación que comprometa de manera IMPORTANTE la **disponibilidad**, **integridad** y **confidencialidad** de la información, junto con la plataforma tecnológica, procesos y aplicativos que permitan acceder a esta en forma oportuna. En general es una violación de una política, estándar o procedimiento de seguridad que no permita dar un servicio computacional.

c) **Integridad:** Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas.

d) **Disponibilidad:** Acceso y utilización de los servicios sólo y en el momento de ser solicitado por una persona autorizada.

e) **Confidencialidad:** Información disponible exclusivamente a personas autorizadas.

f) **Datos personales:** Conjunto de datos que constituyen información que podría permitir identificar a una persona, ya sea directa o indirectamente. Además, dentro de los datos personales, existe una categoría de información que requiere de protección adicional (Ej: nombre y apellidos, nuestra fecha de nacimiento, nuestra dirección postal o de correo electrónico, el número de teléfono, el RUT, la patente de nuestro automóvil, entre otros).

g) **Datos sensibles**: Corresponden a datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o íntima, tales como hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

h) **Los Convenios Marco** son una modalidad de compra de bienes y servicios a través de un catálogo electrónico o tienda virtual y constituyen la primera opción de compra de los organismos públicos.

i) **Licitación Pública:** Es un procedimiento administrativo efectuado en forma autónoma por un organismo comprador, en el que invita a través de Mercado Público a los proveedores interesados a proporcionar un bien o servicio y selecciona y acepta la oferta más conveniente según los criterios que se establezcan en las bases de licitación. Las bases o términos de referencia establecen los requisitos, condiciones y especificaciones del producto o servicio a contratar. Gana la licitación la empresa o persona que haya ofrecido las condiciones más ventajosas según los criterios de evaluación descritos en las bases. Por ley, los organismos están obligados a realizar licitaciones públicas por contrataciones que superen las 1.000 UTM.

j) **Licitación Privada:** En este caso el llamado a participar es específico a algunas empresas o personas, estableciéndose en esta invitación a un mínimo de tres proveedores del rubro. Una vez finalizado el plazo para presentar la oferta, se adjudica el proceso a quien entregó las mejores condiciones. Una vez finalizado el plazo se abren los sobres públicamente y se otorga la adjudicación del proceso a quien o quienes ofrecieron mejores condiciones.

5. Documentos relacionados:

a) Ley 19.628 sobre Protección de datos de carácter personal.
b) Ley 19.886 de compras públicas y sus modificaciones.
c) Política general de seguridad de la información.
d) Política de seguridad para las relaciones con los proveedores.
e) Política privacidad y protección de información personal identificable.
f) Instructivo de acuerdos de confidencialidad en contratos con terceros.
g) Manual de compras.
h) Procedimiento de monitoreo de contratos con tercero.

6. Política:

6.1. Seguridad de la información en la administración de proyectos:

En todo proyecto donde esté relacionado el uso o tratamiento de datos de carácter sensible, se debe abordar la seguridad de la información en el diseño, y administración del proyecto, sin importar el tipo de proyecto (proceso comercial, tecnologías de información, administración de instalaciones, procesos de apoyo, etc.). Se debe identificar y abordan los riesgos de seguridad de la información como parte del proyecto.

Dentro de la administración del proyecto se debe incluir:

6.1.1. Dentro de los objetivos del proyecto se deben incluir objetivos de seguridad de la información en concordancia con la información personal sensible tratada.

6.1.2. Una evaluación de los riesgos de para la protección de los datos sensibles para identificar los controles necesarios.

6.1.3. Una evaluación de los riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios.

6.1.4. La seguridad de la información debe ser parte de todas las etapas del proyecto, independiente de la metodología utilizada.

En este tipo de proyectos, la Jefatura responsable debe definir un funcionario que actuara como responsable para la seguridad de la información (puede ser el Jefe de proyecto o

parte del equipo del proyecto), quien será el responsable que el proyecto incluya las objetivos y requerimientos de seguridad de la información.

En los proyectos que requieran compras se deben seguir las pautas de seguridad de la información definidas a continuación en la presente política.

6.2. Seguridad de la información en los procesos de compras:

Los procesos de compra se llevarán a cabo de acuerdo a lo definido en "*manual de compras*" y sus modificaciones, a saber, compras a través de:

Convenio Marco
Licitación o propuesta publica
Licitación o propuesta privada

Además de incluir las cláusulas de confidencialidad establecidas en el "*Instructivo de acuerdos de confidencialidad en contratos con terceros*" Se deberán para aquellos procesos de compras asociados a proyectos donde se encuentre involucrado el manejo o. tratamiento de datos personales, incluir cláusulas que permitan proteger la información, dependiendo del tipo de compra:

6.2.1. Convenio Marco

Compras Menores a 1.000 UTM:

Antes de la compra debe existir una revisión del bien o servicio para asegurar que cumple con los requisitos de seguridad de la información definidos en las etapas tempranas del proyecto.

Grandes compras Mayores a 1.000 UTM:

Además de la revisión de los bienes y servicios, se deben definir los requisitos de seguridad de la información para resguardar la integridad, confidencialidad y disponibilidad de la información asociada al proyecto y deben ser establecidos en:

- Especificaciones técnicas y administrativas.
- Acuerdo complementario.

6.2.2. Compras a través de licitación o propuesta publica:

Antes de la compra debe existir una revisión del bien o servicio para asegurar que cumple con los requisitos de seguridad de la información definidos en las etapas tempranas del proyecto.

Además, se deben definir los requisitos de seguridad de la información para resguardar la integridad, confidencialidad y disponibilidad de la información en:

Licitación o propuesta pública menor a 100 UTM

- Términos de referencia.

Licitación o propuesta pública entre 100 y 1.000 UTM

- Bases de licitación.
- Contrato.

Licitación o propuesta pública entre 1.001 UTM y 4.999 UTM

- Bases de licitación.
- Contrato.

Licitación o propuesta pública mayor o igual a 5.000 UTM

- Bases de Licitación.
- Contrato.

6.2.3. Compras a través de trato o contratación directa:

Antes de la compra debe existir una revisión del bien o servicio para asegurar que cumple con los requisitos de seguridad de la información definidos en las etapas tempranas del proyecto.

Además, se deben definir los requisitos de seguridad para resguardar la integridad, confidencialidad y disponibilidad de la información en:

Compras Menores a 1.000 UTM a través de Trato Directo:

- Resolución que aprueba el trato directo.

Compras Mayores a 1.000 UTM a través de Trato Directo

- Resolución que aprueba el trato directo
- Contrato.

6.3. Monitoreo y revisión de los servicios del proveedor:

En los servicios de proveedores donde se vea involucrado el uso o tratamiento de datos sensibles la División o Departamento encargada de la administración del acuerdo, debe mantener el control y la visibilidad suficientes en todos los aspectos de seguridad para la información o las instalaciones de procesamiento de información personal sensible y crítica que evalúa, procesa o administra un proveedor.

Para lo anterior, el Jefe de la División o Departamento debe definir un funcionario o equipo responsable de administrar las relaciones con el proveedor, quienes deberán monitorear, revisar y auditar la prestación de servicios del proveedor de manera regular.

Este monitoreo y revisión de los servicios debe garantizar que se incluyan términos y condiciones de seguridad de la información en los acuerdos definidos en los procesos de compra, y que estos se respeten y que los incidentes y los problemas de seguridad de la información se gestionen correctamente, esto incluye:

6.3.1. Monitorear los niveles de desempeño del servicio con el fin de verificar la adherencia a los acuerdos.

6.3.2. Revisar los informes de servicio producidos por el proveedor y organizar reuniones de avance de manera regular según lo requieren los acuerdos.

6.3.3. Realizar auditorías de los proveedores, en conjunto con la revisión de informes de auditores independientes, en caso de estar disponibles y, un seguimiento de los problemas identificados (para llevar a cabo esta acción se deberán incluir en los contratos que SUPEREDUC se reserva el derecho de auditar los servicios prestados, software o producto).

6.3.4. Proporcionar información sobre los incidentes de seguridad y revisar esta información según sea necesario conforme a los acuerdos ya cualquier pauta o procedimiento de apoyo;

6.3.5. Revisar los seguimientos de auditoria del proveedor y los registros de eventos de seguridad de la información, los problemas operacionales, seguimiento de todas las fallas e interrupciones relacionadas con el servicio entregado;

6.3.6. Resolver, gestionar y/o escalar cualquier problema, incidente o evento de seguridad de la información, identificados en los puntos anteriores; así como monitorear la realización de las acciones inmediatas y acciones correctivas/preventivas que permita la resolución de los mismos;

6.3.7. Asegurar que el proveedor cumple con las prohibiciones del uso secundario de la información sensible definidos en la compra del servicio, las procedimientos y controles específicos, la criticidad de la información, los sistemas y procesos involucrados.

6.3.8. Asegurarse de que el proveedor mantiene una capacidad de servicio suficiente junta con planes de trabajo diseñados para garantizar que se mantienen los niveles de continuidad en el servicio luego de grandes fallas o desastres en el servicio.

6.4. Administración de cambios en los servicios del proveedor:

Cuando existan cambios en la provisión de los servicios, estos deben ser administrados por el funcionario o equipo asignado para el monitoreo, y revisión de los servicios del proveedor. Esta administración de los cambios se debe realizar considerando la mantención y/o mejora de los requisitos de seguridad de la información definidos en la compra del servicio, los procedimientos y controles específicos, la criticidad de la información, los sistemas y procesos involucrados, junto con la reevaluación de los riesgos. Además de lo mencionado se deben considerar los siguientes aspectos:

a) Cambios a los acuerdos del proveedor;
b) Los cambios realizados por la organización por implementar:
   - Mejoras a los servicios que se ofrecen actualmente.
   - Desarrollo de cualquier nueva aplicación y sistemas.
   - Las modificaciones o actualizaciones de las políticas y procedimientos de la organización.
   - Controles nuevos o cambiados para resolver incidentes de seguridad de la información y mejorar la seguridad.

c) Cambios en los servicios del proveedor a implementarse.
   - Cambios y mejoras en las redes.
   - Uso de nuevas tecnologías.
   - Adopción de nuevos productos o nuevas versiones.
   - Nuevas herramientas y entornos de desarrollo.
   - Cambios en la ubicación física de las instalaciones de servicios.
   - Cambio de proveedores.
   - Cambios en el equipo del proveedor.
   - Subcontratación a otro proveedor.

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, pudiendo utilizarse los canales de difusión establecidos por la SUPEREDUC (www.supereduc.cl, 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 adquisición 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 2017

12. Responsabilidades de elaboración y aprobación del documento:

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