MIC/FTO/AAM/PBC/DLR

Superintendencia de Educación
TOTALMENTE TRAMITADO

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0720, DE 2017 Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA DE SEGURIDAD PARA LA GESTIÓN DE CAMBIOS A LOS SERVICIOS DEL PROVEEDOR, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0795

SANTIAGO, 30 DIC 2019

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 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; en 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; en las Resoluciones Exentas N°s 674 y 723, ambas de 2019, de la Superintendencia de Educación; en el Oficio Gab. Pres. N° 008, de 23 de octubre de 2018, del Presidente de la República, por el cual imparte instrucciones en materia de ciberseguridad y Oficio Gab. Pres. N°001 de 2019, de Presidencia, que proporciona lineamientos para la transformación digital de la Administración del Estado, y en las Resoluciones N°s 6 y 7, 2019, 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, con fecha 23 de octubre de 2018, el Presidente de la Republica dicta el Instructivo Presidencial N°008 que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

3. Que, con fecha 20 de octubre de 2017, se dicta Resolución Exenta N° 0720, que aprueba versión 1.0 de la política de seguridad para la gestión de cambios a los servicios del proveedor de la Superintendencia de Educación.

4. Que, mediante Resolución Exenta N° 0698, de fecha 10 de diciembre de 2019 se nombró al Comité de Seguridad de la Información Institucional, para que, en función del marco legal y tecnológico, proponga a este Jefe de Servicio, un Sistema de Seguridad de la Información y Ciberseguridad lo mantenga y mejore en el tiempo.

5. Que, debido a una serie de cambios institucionales y a la revisión efectuada por la Encargada de Seguridad de la Información y Ciberseguridad, se ha estimado procedente reestructurar, ajustar y actualizar el contenido de la Política de gestión de cambios a los servicios del proveedor.

RESUELVO:

1. **DÉJASE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0720, de 2017 de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°2 de la política de seguridad para la gestión de cambios a los servicios del proveedor en la Superintendencia de Educación, cuyo texto es el siguiente:

Política de gestión de cambios a los servicios del proveedor

Tabla de Contenidos

ELABORADO POR	REVISADO POR	APROBADO POR
Daniela Llano Recabal **Encargada de Seguridad de la Información y Ciberseguridad**	**Angie Aracena Medina** **Comité Operativo Seguridad de la Información**	**Mauricio Irarrazabal Cerpa** **Comité Directivo Seguridad de la Información**

1. Objetivo

Definir las reglas de seguridad para administrar los cambios a la provisión de servicios de parte de proveedores, manteniendo y resguardando 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 ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo empresas que presten servicios a 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.
- A.18.01.04 Privacidad y protección de la información de identificación personal

3. Referencias normativas

- Ley 19.628 sobre Protección de datos de carácter personal.
- Ley 19.886 de compras públicas y sus modificaciones.
- Política general de seguridad de la información vigente.
- Política de seguridad para las relaciones con los proveedores vigente.
- Política privacidad y protección de información personal identificable vigente.
- Instructivo de acuerdos de confidencialidad en contratos con terceros vigente.
- Manual de procedimientos de adquisiciones de la Superintendencia vigente.

4. Definiciones

Concepto	Descripción
Activos de Información	Recursos del sistema de información, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Una organización incluye diferentes tipos de activos: • Activos relacionados con el entorno (edificios, instalaciones, equipamientos) y personal. • Activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones). • Activos relacionados con la información (datos, metadatos y soportes). • Activos relacionados con las funcionalidades de la organización (productos, servicios). • Activos intangibles (credibilidad, conocimiento acumulado).
Incidente de seguridad	Evento único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer la operación de negocio y de amenazar la seguridad de la información. Por lo tanto, un incidente de seguridad se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información: un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información del organismo.

Concepto	Descripción
Integridad	Se entiende como la característica que implica la corrección y completitud de los datos o de la información manejada, contar con todas sus partes y estar completo.
Disponibilidad	Es el aseguramiento de que los usuarios autorizados tienen acceso a la información, sistemas y a los activos de la superintendencia, cuando es requerido.
Confidencialidad	Es la propiedad de la información, un documento o mensaje que únicamente está autorizado para ser leído o entendido por algunas personas o entidades. Mantiene la cualidad de mantenerse reservada para el conocimiento de una persona o de algunas, pero no debe ser expuesta en forma masiva.
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).
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.
Convenios Marco	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.
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.
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. Roles y Responsabilidades

Rol	Responsabilidades
Jefaturas	a) Definir a un funcionario o equipo, responsable de la administración de proyectos y los acuerdos de servicios en su área. b) Resguardar que el personal a cargo cumpla con las directrices establecidas en esta política
Funcionario o equipo responsable	a) Dar cumplimiento a los requisitos definidos en esta política en la administración de proyectos y los acuerdos de servicio.
Encargado/a de Seguridad de la Información y Ciberseguridad	a) Velar por la difusión y cumplimiento de esta política. b) Velar por la correcta aplicación de esta política. c) Revisar y actualizar la política, con la finalidad de asegurar su continua idoneidad, eficiencia y efectividad.

6. Directrices

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 para la protección de los datos sensibles y para identificar los controles de seguridad necesarios.

6.1.3. Una evaluación de los riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles de seguridad 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 debe definir un funcionario o equipo que actuará como responsable para la seguridad de la información (puede ser el Jefe de proyecto o parte del equipo del proyecto), quien será el encargado de que el proyecto incluya adecuadamente los objetivos y requerimientos definidos en el Sistema de Seguridad de la información de la SUPERED

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 procedimientos de adquisiciones de la Superintendencia de Educación*", a saber, compras a través de:

- Convenio Marco
- Licitación publica
- Licitación privada

Además de incluir las respectivas cláusulas de confidencialidad según lo establecido en el "*manual de procedimientos de adquisiciones de la Superintendencia de Educación*" se deberán incluir cláusulas específicas que permitan proteger la información para aquellos procesos de compras asociados a proyectos donde se encuentre involucrado el manejo o tratamiento de datos personales de acuerdo a lo establecido en la *Política privacidad y protección de información personal identificable*, lo que dependerá 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 pública:

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 pública menor a 100 UTM

- Términos de referencia.

Licitación pública entre 100 y 1.000 UTM

- Bases de licitación.
- Contrato.

Licitación pública entre 1.001 UTM y 4.999 UTM

- Bases de licitación.
- Contrato.

Licitación 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, Intendencia o Departamento encargado 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, Intendencia 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 de acuerdo a lo que se defina en el "*Manual de procedimientos de adquisiciones de la Superintendencia de Educación*",

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, así como también deberá resguardar 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 seguimiento de avances de manera regular según lo establezcan los acuerdos.

6.3.3. Realizar auditorías de los proveedores, en conjunto con la revisión de informes de auditores internos o 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 y a cualquier pauta o procedimiento de apoyo establecido en el Sistema de Seguridad de la Información.

6.3.5. Revisar los seguimientos de auditorías realizadas al 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. Evaluación y Difusión

La presente política será evaluada por el Superintendente de Educación una vez al año, o bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.

Una vez que el documento entre en vigencia e/la Encargado/a de Seguridad de la Información y Ciberseguridad deberá difundir al personal y externos considerado en el alcance, mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrían ser página web institucional, intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

8. Revisión

Con una periodicidad concordante a la de la evaluación definida en el punto anterior, y a través de auditorías, ya sean internas o externas, y en tanto los recursos institucionales se encuentren disponibles para ello, se revisará el cumplimiento de la presente política con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento de la misma.

9. Aceptación

Todos los usuarios de la SUPEREDUC, sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar esta 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, manuales y procedimientos vigentes de seguridad de la información y ciberseguridad 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.

10. Sanciones

11. El incumplimiento o violación a esta Política, de las Políticas específicas del Sistema, Procedimientos u otros documentos que se deriven de éstos, 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.

12. Excepciones

La presente Política, y las Políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el/la Encargado/a de Seguridad de la Información y Ciberseguridad y debidamente autorizados por la Jefatura de Gabinete.

13. Revisiones de la política

REVISIONES DE LA POLITICA			
N° Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
1.0	Octubre 2017	Versión inicial	Versión inicial
2.0	Julio 2018	Actualización de formatos	- Actualización de formatos - Punto 10, se incorpora: "Excepciones"
3.0	Diciembre 2019	Actualización Política	Todas las páginas.

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

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

5. **REMÍTASE,** copia de la presente Resolución Exenta todas las Divisiones, Intendencia, Direcciones Regionales, Departamentos, Unidades y de la Superintendencia de Educación, de acuerdo con la distribución indicada en la presente resolución.

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

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACION
SUPERINTENDENTE

CRISTIÁN O'RYAN SQUELLA
SUPERINTENDENTE DE EDUCACIÓN

Distribución:

- Gabinete Superintendente.
- Jefes/as de División.
- Intendente/a de Educación Parvularia.
- Directores Regionales I a XVI región.
- Jefe/a Departamento de Finanzas.
- Jefe/a Departamento Gestión y Desarrollo de Personas.
- Jefe/a Departamento de Administración.
- Jefe/a Departamento de Tecnologías y Procesos.
- Departamento de Gestión Institucional.
- Departamento de Auditoria.
- Unidad de Transparencia.
- Encargado/a de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.