Gobierno de Chile

Superintendencia de Educación

VPV/CNN/HCJ/PSC/PSY

APRUEBA POLÍTICA PROTECCIÓN DE REGISTROS, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN, EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0719

SANTIAGO, 20 OCT 2017

VISTO:

Lo dispuesto en el DFL N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en el Decreto con Fuerza Ley N° 29, de 2004, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en la Ley N° 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 N° 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 N° 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 protección de registros.

RESUELVO:

1. **APRUÉBASE,** la Política protección de registros, 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.

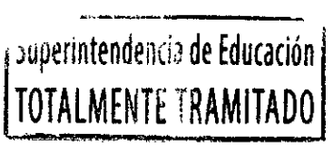
4. **DÉJESE,** expresa constancia que la presente Resolución Exenta no erogará gasto alguno para esta Superintendencia de Educación.

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.

ARIS 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.



POLÍTICA PROTECCIÓN DE REGISTROS

VERSIÓN 1.0

CONTROL ISO27001:2013
A.18.1.3

ÍNDICE

1. Objetivo:

Definir las directrices que rigen las acciones para proteger los registros contra perdidas, destrucción, falsificación accesos no autorizado y publicación no autorizada de acuerdo a los requisitos legislativos, normativos y contractuales.

2. Alcance:

Esta política se aplica a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas y en específico a los siguientes registros;

a) Resoluciones emitidas por la SUPEREDUC.
b) Base de datos: Sistema SIAC, SIPA, Rendición de cuentas.
c) Registros contables
d) Registros de auditoria

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 SUPEREDUC.

Esta política contempla el siguiente control definido en la norma NCh-ISO 27001:2013

- A.18.01.03 Protección de registros.

3. Roles y Responsabilidades:

3.1. Jefe/a Departamento de Tecnologías de Información:

3.1.1. Definir el estándar de respaldo de los servidores y equipos de hardware, que detalle los respaldos de software básico, de las aplicaciones, configuraciones de servicios y de los datos en ambiente de producción, autorizar las solicitudes de respaldo especiales

3.2. Jefaturas Directas:

Informar e instruir a los usuarios a su cargo de utilizar la solución en la nube (OneDrive) para respaldar la información sensible de la institución.

3.3. Funcionario/as:

Tendrán la responsabilidad de cumplir con lo formalizado en esta Política y así garantizar que los activos de información que se encuentren a su cargo estén protegidos contra el mal uso, robo, falta de disponibilidad o destrucción. Además, tendrán la responsabilidad

[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.*

de notificar los incidentes de seguridad y potenciales debilidades de seguridad de la información que pudieran identificarse.

3.4. Encargado/a de Seguridad de la Información:

Monitorear y verificar el correcto cumplimiento de dicha política mediante revisiones aleatorias.

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.

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.

5. Documentos relacionados:

a) Política general de seguridad de la información.

b) Ley 19.628 Sobre la protección de la vida privada, Ministerio Secretaria General de la Presidencia.

c) Ley 20.285 Sobre acceso a la información pública, Ministerio Secretaria General de la Presidencia.
d) Ley 19.880, Establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del estado, Ministerio Secretaria General de la Presidencia.
e) Instructivo de oficina de partes.
f) Instructivo retención de respaldos.

6. Política:

6.1. Protección de registros:

La protección de los registros institucionales específicos de SUPEREDUC, corresponden a una selección en versiones originales y finales de archivos y/o registros digitales, físicos cuyo valor se aprecia por disponer algunas de las siguientes características:

a) Contienen datos sensibles de personas externas a la institución, ejemplo: antecedentes de una denuncia y su respectiva respuesta.
b) Son técnicos o especializados, ejemplo: antecedentes de rendición de cuentas y sus informes de resultados.
c) Sustentan la generación de acciones civiles, administrativas y/o penales frente a terceros, ejemplo: los programas de fiscalización y los informes de fiscalización, actas y resoluciones.
d) Representan valor económico y/o respaldo de acciones financieras, ejemplo: comprobantes de transferencias electrónicas.
e) Involucran el cumplimiento de un requisito legal, normativo o contractual, ejemplo: cualquier resolución de contrato.

La clasificación, almacenamiento y retención de los registros digitales se mantendrá en el sistema de gestión documental de SUPEREDUC, para los registros físico se cuenta con una bodega con acceso restringido en la oficina de partes.

La protección de registros físicos para la documentación de la Dirección Nacional de la SUPEREDUC, se especifica en el "*Instructivo de oficina de partes*".

6.2. Protección de registros de base de datos y transacciones:

Las Jefaturas de División en conjunto con el Departamento de Tecnologías de Información (TIC), definen que los periodos de retención para las bases de datos de los sistemas del alcance son:

Sistema SIAC	:	10 años
SIPA	:	10 años
Rendición de cuentas.	:	10 años

Los registros serán respaldados semanalmente o periódicamente dependiendo de la cantidad de información a respaldar de acuerdo a la "*Política de respaldo*" y a la "*Política de respaldo de servidores*" vigente, la retención de los respaldos será realizará de acuerdo al "*Instructivo retención de respaldos*".

La protección de los medios de respaldos se realizará de acuerdo a lo indicado en la *Política de emplazamiento y protección de equipos.*

La eliminación de los medios de respaldo se realizará de acuerdo a lo indicado en la *Política eliminación o reutilización segura de equipos*.

6.3. Protección de registros de auditoria:

El/la Jefe/a del Departamento de Auditoria de SUPEREDUC ha dispuesto que todos los informes físicos de auditoria sean almacenados en sus respectivas carpetas de trabajo, las cuales se encuentran en las dependencias del departamento y su almacenamiento se define en el *programa de auditoria internas* y procedimiento de *seguimientos de auditorías internas* de SUPEREDUC.

Respectos de las copias digitales de los informes de Auditoría, se almacenan en la cuenta de OneDrive del Jefe/a del Departamento de Auditoria, con los resguardos de acceso al equipo definidos para todos los equipos de la institución.

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