Gobierno de Chile

Superintendencia de Educación

NPV/CNN/HCJ/PRC/PST

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

RESOLUCIÓN EXENTA N° 0723

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 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 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 respaldos de información.

RESUELVO:

1. **APRUÉBASE,** la Política respaldos de información, 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 RAMÍREZ 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 RESPALDO DE INFORMACIÓN

VERSIÓN 1.0

CONTROL ISO27001:2013
A.12.3.1

ÍNDICE

1. Objetivo:

Definir las directrices que rigen las acciones de respaldo de información en la Superintendencia de Educación (SUPEREDUC), que permitan proteger los datos y software contenido en los dispositivos de hardware que la soportan almacenan y distribuyen.

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 a toda la información contenida en los servidores, estaciones de trabajo y equipos de comunicaciones, que contengan datos, configuraciones, aplicativos y servicios críticos para SUPEREDUC.

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.12.03.01 Respaldo de información.

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.

3.1.2. Coordinar, ejecutar y velar por la realización de las pruebas y restauración de las copias de respaldo efectuadas utilizando las herramientas pertinentes para tales efectos.

3.1.3. Mantener un inventario de los activos de información sobre los que se realiza copia de seguridad.

3.1.4. Mantener las condiciones ambientales optimas y de seguridad de acceso a los activos de información que estén bajo su responsabilidad.

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.

[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.*

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 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) **Información:** Es todo conjunto de datos relacionados valorados por la Superintendencia de Educación.

b) **Integridad:** Propiedad de la información que busca proteger que no se modifiquen los datos de forma no autorizada.

c) **Disponibilidad**: Es la propiedad que hace referencia al acceso autorizado a la información y a los sistemas en el momento que se requiera.

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

e) **Base de Datos**: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

f) **OneDrive:** Es la nube de corporativa de SUPEREDUC provista por Microsoft que permite guardar archivos o documentos en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet con la identificación de usuario y password.

g) **Respaldo Full:** Operación de respaldo que guarda todos los archivos que sean especificados al momento de ejecutarse el respaldo.

h) **Respaldo Incremental:** Operación de respaldo que sólo copia los datos que han variado desde la última operación de respaldo de cualquier tipo.

i) **Retención:** Periodo por el cual permanece vigente el respaldo, pudiendo ser Semanal, Mensual, Semestral, Anual.

j) **Periodicidad**: Frecuencia con la que se ejecutara el respaldo de la información.

5. Documentos relacionados:

a) Política general de seguridad de la información.

b) Política uso de computadores.

c) Política de respaldos de servidores.

d) Política eliminación o reutilización segura de equipos.

e) Política perímetros de seguridad física.

6. Consideraciones generales:

Toda la información de los sistemas informáticos críticos en producción de SUPEREDUC deben ser protegidos de posibles fallos por lo que debe ser respaldada con cierta frecuencia, que permita asegurar un adecuado proceso de recuperación, estableciendo para ellos pruebas de manera regular.

El Departamento de Tecnologías de la Información (TIC), debe considerar soluciones de respaldo para equipos de escritorio, servidores, imágenes de sistemas y aplicaciones (códigos fuentes, bases de datos) que se consideren críticos para la institución. Así como también garantizar la disponibilidad de infraestructura adecuada de respaldo, para asegurar que estos estén disponibles incluso después de un desastre o la falla de un dispositivo.

La información que NO es relevante para el quehacer de la institución y que resida en los servidores y equipos de escritorio de SUPEREDUC, NO SERA respaldada. La utilidad de la información será determinada por el Departamento TIC, en conjunto con el responsable de la información de cada negocio.

Cada respaldo que se realice, manual o automático, deberá quedar registrado en los logs de los servidores y/o en un archivo electrónico (texto, planilla, etc.).

En las situaciones donde la confidencialidad es importante, se deberán proteger los respaldos mediante cifrado, u otra técnica.

6.1. Identificación de información crítica:

Los responsables de las unidades de negocio de SUPEREDUC, serán los encargados de identificar y mantener una relación actualizada de aquella información que sus divisiones o departamentos necesitan para mantener operativos sus procesos, durante eventuales procedimientos de restauración.

6.2. Plan de respaldo:

El Departamento TIC, define los tipos de respaldos a utilizar como estándar para SUPEREDUC. Cada estándar debe considerar la frecuencia del respaldo, las medias de almacenamiento, tipo de contenido, tiempo de retención y borrado de esta información.

Para los respaldos de los equipos o estaciones de trabajo de la institución, será utilizando la plataforma OneDrive que provee de una solución de respaldo en la nube, la cual es

instalada por el Departamento TIC en todas las estaciones de trabajo de la institución *"ver política uso de computadores".*

La periodicidad con que se realizan los respaldos de los sistemas informáticos y los equipos considerados críticos para la institución, no podrá ser menor a 1 respaldo full mensual.

El Departamento TIC deberá implementar y ejecutar los procedimientos de respaldo específicos para cada plataforma (Correo, Onedrive, Azure) y/o sistemas de información, así como para carpetas compartidas consideradas críticas, junto con el registro de la realización de estos respaldos. *"ver política de respaldos de servidores"*

6.3. Respaldos en las estaciones de trabajo:

El Departamento TIC deberá implementar la solución de respaldo OneDrive que provee de una solución en la nube para equipos de escritorio. **Siendo los usuarios de la institución los responsables de alojar la información que necesita ser respaldada** en los lugares establecidos para ello *"ver política uso de computadores".*

Las Jefaturas Directas responsables de las unidades de negocio de SUPEREDUC deberán asegurarse de que la información de los funcionarios a su cargo se salvaguarda de forma satisfactoria.

6.4. Pruebas de las configuraciones de respaldo:

Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 1 año, para asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales.

Ante un cambio tecnológico que se produzca en los medios o plataforma de respaldo, que pueda generar obsolescencia tecnológica, deben generarse las acciones necesarias de resguardo de la información en ellos.

6.5. Protección de la información en medios de respaldos:

Para prevenir perdidas de información accidentales, se deben respaldar todos los archivos, bases de datos e información existente en los Sistemas relevantes para la institución, se debe disponibilizar la infraestructura adecuada de respaldo para cada caso, y asegurar su disponibilidad en caso de desastres o falla de un dispositivo.

Un nivel mínimo de información crítica (para asegurar la continuidad de las operaciones), deberá ser respaldada y almacenada en una ubicación remota, esta instalación deberá

estar emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal.

Dicho respaldo debe tener registros exactos y completos de las copias y procedimientos documentados de restablecimiento. En ámbitos críticos para la institución, se deberán almacenar al menos seis generaciones o ciclos de información de respaldo.

El respaldo de datos y software críticos se deben almacenar en un lugar protegido, con acceso controlado *"ver política perímetros de seguridad física"*.

Toda información crítica grabada en respaldos que son almacenados fuera de la institución, debe ser trasladada con los elementos de seguridad adecuados, ya sea utilizando métodos de encriptación en las comunicaciones o utilizar métodos apropiados para prevenir intentos de acceso físico no autorizado. El Departamento TIC deberá mantener un inventario actualizado de la información almacenada externamente.

6.6. Periodo de retención y existencia de respaldos:

La retención del respaldo de la información se debe mantener según lo indica la Circular N°051, del 09 de febrero de 2009, sobre disposiciones y recomendaciones referentes a conservación, transferencia y eliminación de documentos, de la Dirección de Bibliotecas, Archivos y Museos o aquella que la reemplace. Lo anterior, de acuerdo con el ordenamiento jurídico vigente y el uso eficiente del espacio físico disponible para el almacenamiento.

Se deberá establecer el periodo de existencia para las copias de seguridad y los procedimientos a seguir para su destrucción definitiva o eliminación de manera segura. Para dar soporte a este requisito, los responsables de las unidades de negocio deberán revisar, de forma periódica, el valor y la utilidad de la información almacenada *"ver política eliminación o reutilización segura de equipos"*.

6.7. Borrado de información:

La información contenida en los servidores centrales de la institución que no sea necesaria, debe ser borrada. Todo equipo computacional o medio de almacenamiento que sea dado de baja, debe ser examinado por el Departamento TIC, para comprobar que la información ha sido borrada.

La destrucción de medios de almacenamiento (como cintas, medios ópticos, etc.) que contienen información, debe ser efectuada de forma que impida el acceso al medio *"ver política eliminación o reutilización segura de equipos"*.

6.8. Pruebas de respaldos y restauración:

La realización de las pruebas de restauración de las copias de respaldo confirmará el funcionamiento correcto del proceso de recuperación de copias de datos y garantizará la integridad de los datos que contienen. Por lo que se deberán realizar pruebas respecto a la restauración de las copias de respaldo, de forma rotativa y con una periodicidad con una regularidad, a lo menos cada 1 año.

Las pruebas y los resultados de restauración deberán ser registrados por el Departamento TIC quien deberá documentar las incidencias que se hayan puesto de manifiesto durante su desarrollo.

6.9. Comprobación de restauración:

Para garantizar la eficacia de los procedimientos de restauración de SUPEREDUC y la capacidad para recuperar activos desde las copias de respaldo, el Departamento TIC deberá aplicar periódicamente el siguiente procedimiento de comprobación que se detalla a continuación:

a) Seleccionara al azar un activo de información almacenado en la copia de respaldo.
b) Ejecutará una restauración del activo sobre una ubicación temporal, comprobará la restauración del activo y lo eliminará posteriormente.
c) Almacenara el log de la herramienta de generación de copias con el resultado de la operación de restauración en el registro de operaciones de comprobaci6n periódicas del SUPEREDUC.

En caso que falle el proceso de restauración y/o provoque daños o pérdidas de los datos, el Departamento TIC deberá proceder a regularizar esta situación y comunicarlo al Encargado de Seguridad de la información.

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