Gobierno de Chile

Superintendencia de Educación

MPV/CNN/HCJ/PRC/PSY

APRUEBA POLÍTICA ELIMINACIÓN O REUTILIZACIÓN SEGURA DE EQUIPOS, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN, EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0722

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 eliminación o reutilización segura de equipos.

RESUELVO:

1. **APRUÉBASE,** la Política eliminación o reutilización segura de equipos, 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.

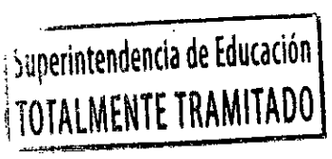
4. **DÉJESE,** expresa constancia que la presente Resolución Exenta no erogará gasto alguno para esta Superintendencia de Educación.

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.

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.



POLÍTICA ELIMINACIÓN O REUTILIZACIÓN SEGURA DE EQUIPOS

VERSIÓN 1.0

CONTROL ISO27001:2013
A.11.2.1

INDICE

1. Objetivo:

Definir las directrices y requisitos en el marco del Sistema de Gestión de Seguridad de la Información, sobre las medidas a considerar para eliminar y/o volver a disponer de manera segura los equipos que contengan medios de almacenamiento de la Superintendencia de Educación (SUPEREDUC), a fin de garantizar que cualquier tipo de datos sensibles y/o software licenciado se hayan extraído o sobrescrito de manera segura antes de su eliminación.

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 digital de los usuarios[1], contratistas o terceros que la SUPEREDUC tenga en su poder, dando cumplimiento a las reglamentaciones a que hubiere lugar, buscando garantizar la seguridad y privacidad de los datos custodiados por la Entidad, velando por que la información sea eliminada de forma segura y que no pueda ser recuperable posteriormente.

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

- A.11.02.07 Eliminación o reutilización segura de equipos.

3. Roles y Responsabilidades:

3.1. Jefe/a División Administración General:

3.1.1. Implementar de manera efectiva esta Política dentro de su área de competencia, debiendo procurar que se asignen los recursos humanos, materiales y financieros para su implementación.

3.2. Jefe/a Departamento de Tecnologías de Información:

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

3.2.2. Coordinar, ejecutar y velar por la correcta gestión de los activos de información al interior de las salas de procesamiento de información (datacenter).

3.2.3. Asegurar el emplazamiento de equipos de monitoreo de las salas de procesamiento de información (datacenter), velando que personas no autorizadas vean el contenido durante su uso.

3.3. Jefaturas Directas:

Facilitar un emplazamiento de equipos, evitando que personas no autorizadas vean el contenido durante su uso.

---

[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.*

3.4. 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.

3.5. Encargado/a de Seguridad de la Información:

Monitorear y verificar el correcto cumplimiento de dicha política mediante inspecciones.

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) **UPS:** Sistema de alimentación de energía ininterrumpida.

c) **Los medios de almacenamiento de datos** es el material físico donde se almacenan los datos que pueden ser procesados por una computadora, un dispositivo electrónico, o un sistema informático.

d) **La sobrescritura:** consiste en reemplazar los datos almacenados por un patrón binario de información sin sentido. La eficacia de este método depende del número de ciclos de sobrescritura. Existen procedimientos avanzados que permiten saber, con bastante precisión, la información que existía originalmente, por eso la información que se debe sobrescribir debe generar tal desorden en el soporte magnético que la recuperación de los datos originales sea prácticamente imposible. No se puede utilizar en soportes dañados ni en aquellos que no sean regrabables, como CDs y DVDs de solo escritura.

e) **La desmagnetización:** consiste en la exposición de los soportes de almacenamiento a un campo magnético suficientemente potente para modificar la polaridad de las partículas magnéticas y, por tanto, eliminar los datos almacenados, impidiendo la recuperación de los mismos. Válido para dispositivos magnéticos, como por ejemplo los discos duros o cartuchos de cinta. Tiene varios inconvenientes, como que se debe analizar qué campo electromagnético se tiene que utilizar para cada dispositivo, se tienen que trasladar los dispositivos al lugar donde se encuentre el desmagnetizador y en algunos medios de grabación magnética (aquellos con caché de memoria Flash) no se elimina toda la información almacenada.

f) **La desintegración:** mecanismo de corte o triturado no uniforme que reduce el dispositivo a pedazos de tamaño y forma aleatorios.

g) **La pulverización**: proceso que consiste en machacar el material y que se utiliza para la destrucción de discos duros.

h) **La fusión**: proceso mediante el cual el material se calienta a una temperatura que es menor que el punto de encendido, pero suficientemente alta para derretirlo, puede ser un medio efectivo de destrucción para los discos duros.

i) **La incineración:** puede destruir completamente todos los dispositivos y para todos los niveles de seguridad. Debe llevarse a cabo en incineradoras que hayan sido aprobadas en cuanto a impacto medioambiental, para plásticos y otros materiales.

j) **El triturado:** consiste en reducir el soporte a pedazos minúsculos de tamaño y forma uniformes. El uso de trituradoras está normalmente limitado a soportes de grosor fino, como los soportes de datos ópticos (DVDs o CDs).

5. Documentos relacionados:

a) Política general de seguridad de la información.

b) Política respaldo de información.

c) Procedimiento de eliminación segura de la información.

6. Política:

6.1. Eliminación de medios de almacenamiento de datos:

Toda la información que se encuentre en cualquiera de los siguientes medios de almacenamiento: discos duros internos y externos, memorias USB, memorias flash, documentación impresa o cualquier otro medio de almacenamiento de información fisico y/o lógico.

Se deben identificar las técnicas de borrado apropiadas para cada soporte (si es óptico, magnético, memorias externas...) y tipo de información que contiene. Como en cualquier otro proceso de destrucción, es necesario dejar constancia de los procedimientos de borrado realizados.

La eliminación de información de medios de almacenamiento que contenga información confidencial, critica, sensitiva, o de uso interno de la SUPEREDUC, debe ser llevada a cabo únicamente por personal autorizado, y en estricto cumplimiento del *"Procedimiento de eliminación segura de la información"*.

6.2. Consideraciones para eliminar información:

Anterior a eliminar o dar de baja un equipo, se debe realizar una revisión para asegurarse de que no contiene medios de almacenamiento. Los medios de almacenamiento que contienen información confidencial o con derecho de autor se deberían destruir físicamente o bien, la información se debería destruir, eliminar o sobrescribir mediante

técnicas para hacer que la información original no se pueda recuperar en vez de utilizar la función de eliminación o formateo normal.

Dependiendo del medio en que se encuentre la información, se aplicara a los equipos de procesamiento de información cualquiera de los siguientes métodos según sea conveniente:

- Desmagnetización.
- Destrucción Física.
- Desintegración, pulverización, fusión e incineración.
- Trituración.
- Sobre-escritura.

Las técnicas para sobrescribir los medios de almacenamiento de manera segura pueden diferir de acuerdo con la tecnología de los medios de almacenamiento. Se debe revisar las herramientas de sobreescritura utilizadas para asegurarse de que se pueden aplicar a la tecnología de los medios de almacenamiento.

Los métodos de destrucción física pueden ser completamente seguros en cuanto a la destrucción real de los datos, pero tienen algunos inconvenientes como que los residuos generados deben ser tratados adecuadamente, que implican la utilización de distintos métodos industriales de destrucción según el soporte o que obligan a un transporte de los dispositivos a un centro de reciclaje adecuado, lo que hay que hacer con las medidas de custodia adecuadas para asegurar el control de los dispositivos.

Se deben destruir todas las copias de los documentos cuya eliminación esté autorizada, incluidas las copias de seguridad, las copias de conservación y las copias de seguridad electrónica.

La descripción de estos métodos se encuentra establecida en el *"Procedimiento de eliminación segura de la información"*.

6.3. Eliminación de medios de almacenamiento por parte de terceros:

No se confiará a terceros la destrucción de sus medios informáticos de almacenamiento, sin antes asegurarse que la Información Confidencial, crítica o de uso Interno ha sido debidamente eliminada de los mismos.

a) Debe suscribirse un contrato por escrito entre la empresa de destrucción y el cliente, en el que se regulen todas las transacciones. En él se debe dar información sobre las actividades, los medios de transporte, de custodia, de destrucción, así

como de los compromisos asumidos y la entrega de los correspondientes certificados de destrucción.

b) Se debe exigir que un representante del responsable de los documentos presencie la destrucción de los documentos y compruebe las condiciones en que se realiza y los resultados.

c) Se debe garantizar la destrucción de los documentos en sus instalaciones y con medios propios, sin subcontratos que conlleven el manejo de los documentos por parte de otras empresas sin conocimiento del responsable de los documentos.

d) La destrucción debe realizarse al nivel adecuado conforme a la confidencialidad de los documentos y del material que se tiene que destruir.

e) El personal que lleva a cabo la recogida, transporte y destrucción debe contar con la formación adecuada, así como suscribir un compromiso de confidencialidad.

f) Resulta evidente que a las empresas de destrucción se les debe exigir que cumplan con la legislación que les aplica por su actividad, por el tratamiento de los datos que realizan y por el potencial impacto medioambiental.

Todas las operaciones de manejo y transporte de los documentos durante el traslado y hasta el momento de la destrucción deben estar realizadas por personal autorizado e identificable. El medio de transporte debe utilizarse exclusivamente para aquellos documentos que se van a eliminar y contar con sistemas de seguridad (vehículos cerrados, con sistemas de alarma e inmovilización, por ejemplo).

A la empresa se le debe exigir un certificado de destrucción de los documentos donde conste que la información ya no existe, y dónde, cuándo y cómo ha sido destruida. Es imprescindible dejar constancia de las actividades realizadas, y sirve para la auditoría y evaluación del cumplimiento de los requisitos acordados entre la empresa y el archivo.

6.4. Registro de los medios eliminados:

Tratándose de medios informáticos de almacenamiento que contengan información crítica o sensitiva, su destrucción, así como el mecanismo elegido para ello, deben ser documentados en un registro formal que se llevará para tales efectos, a fin de que éste constituya un registro de auditoría.

6.5. Cifrado de información:

Además del borrado seguro del disco, se recomienda utilizar el cifrado del disco completo, el cual reduce el riesgo de divulgar información confidencial cuando se elimina o vuelve a implementar el equipo, siempre que se considere los siguiente:

a) el proceso de cifrado sea lo suficientemente fuerte y que cubra a todo el disco (incluido el espacio despejado, los archivos de intercambio, etc.).
b) las claves de cifrado sean lo suficientemente largas como para resistir los ataques de fuerza bruta.
c) las claves de cifrado en sí se mantengan de manera confidencial (es decir, que nunca se almacenen en el mismo disco).

6.6. Prohibición de acumular medios de almacenamiento para su eliminación:

Una vez autorizada por la SUPEREDUC la eliminación de los medios de almacenamiento de información esta debe hacerse de manera gradual, aun cuando se trate de información no sometida a requerimientos de confidencialidad, esto porque la acumulación de información no sensitiva puede dar a conocer información clasificada como confidencial. Por ende, no se recomienda la acumulación de información a ser eliminada, sin antes prever y proveer protección para la misma.

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 adquisiciones 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