MIC/FTO/AAM/PBC/DLR

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0722, DE 2017 Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA ELIMINACIÓN O REUTILIZACIÓN SEGURA DE EQUIPOS, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN.

Superintendencia de Educación
TOTALMENTE TRAMITADO

RESOLUCIÓN EXENTA N° 0791

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 20 de octubre de 2017, se dicta Resolución Exenta Nº 0722, que aprueba política eliminación o reutilización segura de equipos versión Nº1, en el marco de la Seguridad de la Información.

3. Que, con fecha 23 de octubre de 2018, el Presidente de la Republica dicta el Instructivo Presidencial Nº 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.

4. Que, con fecha 02 de diciembre de 2019 se dicta Resolución Exenta Nº 0674, que designa a Encargada de Seguridad de la Información y Ciberseguridad para la Superintendencia de Educación.

5. 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 que se mantenga y mejore en el tiempo

RESUELVO:

1. **DÉJASE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0722, de 2017 de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°2 de la Política eliminación o reutilización segura de equipos en la Superintendencia de Educación, cuyo texto es el siguiente:

Política eliminación o reutilización segura de equipos

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 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, ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo empresas que prestan servicios a SUPEREDUC. Con el objetivo de resguardar que la información administradas por estos usuarios en sus medios de almacenamiento o equipos informáticos que ya no estén en uso, 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. Referencias normativas

- Política general de Seguridad de la información de la Superintendencia de Educación vigente.
- Política respaldo de información de la Superintendencia de Educación vigente.
- Procedimiento de creación, modificación, eliminación de cuentas e información y egreso de personas de la Superintendencia de Educación vigente.
- Política privacidad y protección de información personal identificable de la Superintendencia de Educación vigente.
- Política devolución de activos de información de la Superintendencia de Educación vigente.
- Política uso de medios removibles y dispositivo móviles de la Superintendencia de Educación vigente.

4. Definiciones

Concepto	Descripción
Activos de Información	Recursos del sistema de información que para la institución es considerada importante o de alta validez, que utiliza y son 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 (servicios). - Activos intangibles (credibilidad, conocimiento acumulado). Todo activo de información tiene un propietario, que es designado y responsable de hacer efectivo los controles de seguridad que se establezcan al interior de la SUPEREDUC.

Concepto	Descripción
Medios de almacenamiento de datos	Material físico donde se almacenan los datos que pueden ser procesados por una computadora, un dispositivo electrónico, o un sistema informático
Sobre escritura	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 sobrescrita. 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
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
Desintegración	Mecanismo de corte o triturado no uniforme que reduce el dispositivo a pedazos de tamaño y forma aleatorios
Pulverización	Proceso que consiste en machacar el material y que se utiliza para la destrucción de discos duros
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
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
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. Roles y Responsabilidades

Rol	Responsabilidades
División Administración General	a) Implementar de manera efectiva esta Política dentro de su área de competencia b) Incluir en los contratos con externos la eliminación de información sensible en sus medios de almacenamiento y equipos informáticos, si el caso del servicio requiere acceder a la información sensible de la Superintendencia de Educación.
Departamento de Tecnologías y Procesos	a) Mantener las condiciones ambientales optimas y de seguridad de acceso a los activos de información que estén bajo su responsabilidad. b) Coordinar, ejecutar y velar por la correcta gestión de los activos de información al interior de las salas del procesamiento de información (datacenter). c) 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. d) Generar las de medidas de destrucción, respaldo y cifrados que requieran los equipos informáticos y medios de almacenamiento de información. e) Mantener un reporte de todo los borrados y reutilización de equipos informáticos de la SUPEREDUC.
Jefaturas Directas	a) Facilitar un emplazamiento de equipos, evitando que personas no autorizadas vean el contenido durante su uso. b) Las jefaturas de las Divisiones, Intendencia, Direcciones Regionales, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política.

Encargado/a de Seguridad de la Información y Ciberseguridad	a) Velar por el correcto funcionamiento y operación de la política de eliminación o reutilización segura de equipos así como la correcta aplicación de está al interior de la Superintendencia de Educación..
Funcionario/as	a) 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. b) Responsabilidad de notificar los incidentes de seguridad y potenciales debilidades de seguridad de la información que pudieran identificarse.

6. Directrices

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 físico y/o lógico en cuanto lleguen a finalizar su ciclo de vida útil o cuando la institución desecha o cambia estos medios, se deberán emplear mecanismos de destrucción y borrando para evitar que queden al alcance de terceros, de acuerdo a las siguientes directrices:

a. Se deben identificar las técnicas de borrado apropiadas para cada soporte (si es óptico, magnético, memorias externas, entre otros) y tipo de información que contiene. Como en cualquier otro proceso de destrucción, es necesario dejar constancia de los procedimientos de borrado realizados por el Departamento de Tecnología y Procesos, que apliquen los funcionarios de la Mesa de Servicio.

b. 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 del Departamento de Tecnología y Procesos, y en estricto cumplimiento del *"Procedimiento de creación, modificación, eliminación de cuentas e información y egreso de personas"*.

c. Para eliminar definitiva cualquier dato contenido en un medio de almacenamiento no es suficiente la acción de formateo, El Departamento de Tecnología y Proceso debe generar acciones para asegurar que no se pueda lograr la recuperación de los datos.

6.2. Consideraciones para eliminar información

a. 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.

b. 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.

c. 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 **sobre escritura** utilizadas para asegurarse de que se pueden aplicar a la tecnología de los medios de almacenamiento

d. 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.
e. 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 creación, modificación, eliminación de cuentas e información y egreso de personas"*.

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 de la SUPEREDUC ha sido debidamente eliminada de los mismos, para resguardar está eliminación se debe considerar:

a. Suscribirse un contrato por escrito entre la empresa de destrucción y la Superintendencia, 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. La destrucción debe realizarse al nivel adecuado conforme a la confidencialidad de los documentos y del material que se tiene que destruir.
d. El personal que lleva a cabo la recogida, transporte y destrucción debe contar con la formación adecuada, así como suscribir un compromiso de confidencialidad.
e. 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 por el Departamento de Tecnología y Procesos 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 digital

El Departamento de Tecnología y Procesos además **del borrado seguro del disco, deberá** 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:

- El proceso de cifrado sea lo suficientemente fuerte y que cubra a todo el disco (incluido el espacio despejado, los archivos de intercambio, etc.).
- Las claves de cifrado sean lo suficientemente largas como para resistir los ataques de fuerza bruta.
- 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. Evaluación y Difusión

La presente política será evaluada por el Superintendente de Educación al menos 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 el responsable de su elaboración deberá difundir al personal considerado en el alcance mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrán ser 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

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.

11. 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.

12. 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	Diciembre 2019	Revisión Política	Todas las Paginas.

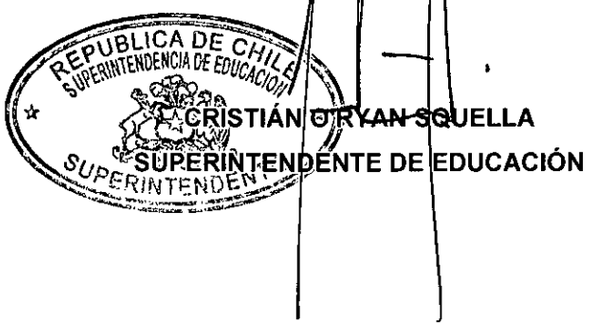
3. **ESTABLÉZCASE,** la obligación de el/la Encargado/a de Seguridad de la Información de la Superintendencia de Educación, de difundir la política fijada por este instrumento y de velar junto con el comité de Seguridad de la Información por su estricto cumplimiento.

4. **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.

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

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.



CRISTIÁN ORYAN 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.
- Encargada de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.