MIC/FTO/AAM/PBC/DLR

Superintendencia de Educación
TOTALMENTE TRAMITADO

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0723 DE 2017 Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA RESPALDO DE INFORMACIÓN, EN EL MARCO DE LA SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0794

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 0723, que aprueba política respaldo de información 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° 0723, de 2017 de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°2 de la Política respaldo de información en la Superintendencia de Educación, cuyo texto es el siguiente:

Política respaldo de información

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

Los medios de almacenamiento contienen uno de nuestros activos más preciados: la información. Estos dispositivos pueden verse involucrados en situaciones como robos, incendios, inundaciones, fallos eléctricos, rotura o fallo del dispositivo, virus, borrados accidentales, etc. En estos casos sería imposible acceder a la información de la Superintendencia de Educación, llegando a ponerse en peligro la continuidad de está.

La siguiente política establece 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[1] 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, 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. Referencias normativas

- Política general de seguridad de la información de la Superintendencia de Educación vigente.
- Roles y responsables implementación y administración del gobierno de datos.
- Política uso de computadores de la Superintendencia de Educación
- Política perímetros de seguridad física 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.
- Norma Chilena NCh-ISO 27001/2013 tecnología de la información-técnicas de seguridad-sistemas de gestión de la seguridad de la información
- Procedimiento de respaldos usuarios y servidores.

4. Definiciones

Concepto	Descripción
Activo 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. Una organización incluye diferentes tipos de activos: - Activos relacionados con el entorno (edificios, instalaciones, equipamientos, etc.) y personal. - Activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones, etc.). - Activos relacionados con la información (datos, metadatos y soportes). - Activos relacionados con las funcionalidades de la organización (servicios). Activos intangibles (credibilidad, conocimiento acumulado, etc.).

[1] Publicado en el sitio web www.dipres.gob.cl Inicio / Evaluación y Control de Gestión / Definiciones estratégicas/ Superintendencia de Educación.

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 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.
OneDrive	Herramienta para el almacenamiento de archivos e información, One Drive es la nube institucional que permite guardar archivos o documentos en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet con la cuenta de usuario que se utiliza para el acceso al sistema informático de la Superintendencia de Educación.
Respaldo Full	Operación de respaldo que guarda todos los archivos que sean especificados al momento de ejecutarse el respaldo.
Respaldo Incremental	Operación de respaldo que sólo copia los datos que han variado desde la última operación de respaldo de cualquier tipo.
Retención	Periodo por el cual permanece vigente el respaldo, pudiendo ser semanal, mensual, semestral, anual.
Periodicidad	Frecuencia con la que se ejecutará el respaldo de la información.

5. Roles y Responsabilidades

Rol	Responsabilidades
Departamento de Tecnologías y Procesos	a) 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 b) Autorizar las solicitudes de respaldo especiales c) 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 d) Mantener un inventario de los activos de información sobre los que se realiza copia de seguridad e) Mantener las condiciones ambientales optimas y de seguridad de acceso a los activos de información que estén bajo su responsabilidad
Jefaturas Directas	a) 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. 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 la difusión y cumplimiento de esta política. b) Monitorear el correcto funcionamiento y operación respecto la ejecución de respaldos de servidores y equipos de funcionarios de la SUPEREDUC. c) Velar por la correcta aplicación de la política y apoyar a las unidades técnicas responsable de la administración y gestión de respaldo al interior de la Superintendencia de Educación. d) Actualizar la política, con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.
Funcionario/as	a) Cumplir con los 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) Personas, funcionarios, colaboradores, practicantes o personal externo que preste servicio permanente o temporal que, con debida autorización, usan información y sistemas informáticos de la SUEPREDUC, por lo que mantienen la responsabilidad de hacer cumplir lo establecido en esta política. c) Utilizar los medios de respaldos asignados por la SUPEREDUC, de acuerdo a lo establecido en esta política.

6. Directrices

6.1. Disposiciones 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 y Procesos, 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 será respaldada**. La utilidad de la información será determinada por el Departamento de Tecnologías y Procesos, en conjunto con el responsable de la información de cada unidad o área de la Superintendencia de Educación

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.) que contenga el registro de las actividades de respaldos generadas tanto en servidores y como escritorio de cada funcionario o usuario de la SUPEREDUC.

En las situaciones donde la confidencialidad es importante, se deberán proteger los respaldos mediante cifrado, u otra técnica de respaldo de información seguro que disponga y establezca el Departamento de Tecnología y Procesos.

6.2. Identificación de información crítica

Los responsables de las áreas o departamento de SUPEREDUC, serán los encargados/as 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, rigiéndose por el "*Procedimiento de actualización de inventario y análisis de riesgo*" vigente en la SUPEREDUC.

6.3. Plan de respaldo

El Departamento de Tecnologías y Procesos, 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 de Tecnologías y Procesos en todas las estaciones de trabajo de la institución *"Ver política uso de computadores"* y *"Procedimiento de respaldo usuarios y servidores"* vigente y publicados en la Intranet.

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, establecido en el *"Procedimiento de respaldo de usuarios y servidores"* vigente en la SUPEREDUC.

El Departamento de Tecnologías y Procesos deberá implementar y ejecutar los procedimientos de respaldo específicos para cada plataforma (Correo, OneDrive) y/o sistemas de información, así como para carpetas compartidas consideradas críticas por el propietario del activo de información, junto con el registro de la realización de estos respaldos.

6.4. Respaldos en las estaciones de trabajo

El Departamento de Tecnologías y Procesos 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" y "Procedimiento de respaldo usuarios y servidores"* vigente en la SUPEREDUC.

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

6.5. 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.

6.6. 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 Superintendencia de Educación, se debe poner a disposición 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 SUPEREDUC, 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 de Tecnologías y Procesos deberá mantener un inventario actualizado de la información almacenada externamente.

6.7. 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.

El responsable del activo de información en conjunto con el Departamento de Tecnología y Procesos 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 y áreas de la Superintendencia de Educación deberán revisar, de forma periódica, el valor y la utilidad de la información almacenada *"Ver: Procedimiento de creación, modificación, eliminación de cuentas e información y egreso de personas"* vigente y publicada en la Intranet.

6.8. 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 de Tecnologías y Procesos, 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"* y *"Ver Procedimiento de creación, modificación, eliminación de cuentas e información y egreso de personas"* vigente y publicados en la Intranet.

6.9. 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 de Tecnologías y Procesos, quien deberá documentar las incidencias que se hayan puesto de manifiesto durante su desarrollo.

6.10. Comprobación de restauración

Para garantizar la eficacia de los procedimientos de restauración de la Superintendencia de Educación y la capacidad para recuperar activos desde las copias de respaldo, el Departamento de Tecnologías y Procesos 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 de Tecnologías y Procesos deberá proceder a regularizar esta situación y comunicarlo al Encargado/a de Seguridad de la información y Ciberseguridad.

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

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 Encargado/a de Seguridad de la Información y debidamente autorizados por la Jefatura de Gabinete.

12. Revisiones de la política

REVISIONES de la política			
N° Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
1.0	Octubre 2017	Versión inicial	Versión inicial
2.0	Diciembre 2019	Actualización de 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 EDUCACIÓN

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.