MIC/FTO/AAM/PEC/DLR

Superintendencia de Educación
TOTALMENTE TRAMITADO

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0719, DE 2017 Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA PROTECCIÓN DE REGISTROS, DE LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0730

SANTIAGO, 19 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 871, 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, 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.

3. Que, con fecha 23 de octubre de 2018, el Presidente de la Republica dicta el Instructivo Presidencial N°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, debido a una serie de cambios institucionales y a la revisión efectuada por la Encargada de Seguridad de la Información y Ciberseguridad se ha estimado procedente reestructurar, ajustar y actualizar el contenido de la Política de protección de registros, versión N°1, aprobada mediante Resolución Exenta N°0719, de fecha 20 de octubre de 2017, de esta Superintendencia.

RESUELVO:

1. **DÉJASE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0719, de 2017 de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°2 de la Política de protección de registros de la Superintendencia de Educación, cuyo texto es el siguiente:

Política de protección de registros

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 Irarrázabal Cerpa** **Comité Directivo Seguridad de la Información**

1. Objetivo

Considerando que los registros organizacionales, corresponden a un activo de información de alta criticidad, el objetivo de esta política es definir las acciones para que los activos de información de la Superintendencia no se vean comprometidos, resguardando con ello los niveles de integridad, disponibilidad, confidencialidad y disponibilidad.

Para ello se definen las directrices que rigen las acciones para proteger los registros organizacionales de la institución contra perdidas, destrucción, falsificación de accesos y publicación no autorizada (entre otros), de acuerdo a los requisitos legislativos, normativos y contractuales vigentes en la Superintendencia de Educación.

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 los procesos definidos en la Matriz de Riesgo Institucional, en específico a los siguientes registros:

a) Resoluciones emitidas por la SUPEREDUC.
b) Base de datos desistemas institucionales como SIAC, SIPA, SIFE, CRM, Rendición de cuentas, etc.
c) Registros contables
d) Registros de auditoria
e) Registros transaccionales
f) Procedimientos Operacionales

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. Referencias normativas

- El marco legal para el Sistema de Seguridad de la información se señala en el documento "Listado de normativa vigente aplicable a la Superintendencia de Educación" vigente
- Política General de Seguridad de la Información de la Superintendencia de Educación vigente.
- Ley N° 19.628 Sobre la protección de la vida privada, Ministerio Secretaria General de la Presidencia.
- Ley N° 20.285 Sobre acceso a la información pública, Ministerio Secretaria General de la Presidencia.
- Ley N° 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.
- Manual de operaciones y procedimientos de oficina de partes de la Superintendencia de Educación vigente.
- Política de respaldo de información de la Superintendencia de Educación vigente.
- Política de emplazamiento y protección de equipos de la Superintendencia de Educación vigente.
- Política eliminación o reutilización segura de equipos de la Superintendencia de Educación vigente.
- Plan anual de Auditoría de la Superintendencia.

[1] Se entiende por usuarios a los funcionarios/as en calidad jurídica planta, contrata, reemplazos ysuplencia, tanto para el personal a honorarios y terceros (proveedores, compra de servicios, etc.) que trabajen para SUPEREDUC.

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. 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.).
Incidente de seguridad	Evento único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer la operación de negocio y de amenazar la seguridad de la información. Por lo tanto, un incidente de seguridad se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información: un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información del organismo.
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 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 los vehículos institucionales, entre otros).
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. Roles y Responsabilidades

Rol	Responsabilidades
Departamento de Tecnologías y Procesos	a) Definir el estándar de respaldo de los servidores y equipos, aplicaciones, configuraciones de servicios y de los datos en ambiente de producción. Autorizar las solicitudes de respaldo especiales. b) Punto de contacto, entre usuarios de la SUPEREDUC y las Unidades del Departamento de Tecnología y Proceso, para orientar, asesorar, actualizar y restaurar los problemas que puedan presentar este los registros organizacionales. c) Proponer las directrices e implementar configuraciones de seguridad y ciberseguridad para resguardar los registros organizacionales que resguarda esta política.

	d) Apoyar y gestionar eventos e incidentes de seguridad que tengan estrecha relación con registros organizaciones y sus respectivos sistemas o dispositivos de almacenamiento. e) Gestionar el adecuado nivel de calidad, seguridad, continuidad y rendimiento de los servicios de tecnologías que almacenan los registros organizacionales de la SUPEREDUC.
Jefaturas Directas	a) Las jefaturas de las Divisiones, Intendencia, Direcciones Regionales, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política, así como las políticas específicas, manuales y procedimientos asociados al SGSI
Funcionario/as	a) 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) Notificar a Mesa de Servicio TI los eventos y posibles incidentes de seguridad y potenciales debilidades de seguridad de la información que pudieran identificarse
Encargado/a de Seguridad de la Información y ciberseguridad	a) Analizar y evaluar el funcionamiento de esta política, con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de esta misma. b) Promover acciones, en materia de seguridad de la información y ciberseguridad que permitan reducir los riesgos e incidentes sobre los registros institucionales. c) Coordinar la implementación y correcta aplicación de esta política. d) Coordinar la oportuna respuesta y priorización al tratamiento de incidentes y eventos vinculados a los registros organizacionales y sistemas informáticos institucionales que almacenan estos activos.

6. Directrices

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 y físicos cuyo valor se establece 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.
f) Manuales y procedimientos que establecen la forma en que se debe llevar a cabo los procesos y en el que se definen actividades, duración y relaciones entre distintas áreas de la institución.

La clasificación, almacenamiento y retención de los registros digitales se mantendrá en el sistema de gestión documental de SUPEREDUC a cargo del Departamento de Tecnologías y Procesos, para los registros físicos se cuenta con una bodega con acceso restringido en la oficina de partes ubicada en el nivel central de la Superintendencia. Cabe mencionar que el propietario del proceso que genera o administra este tipo de registros debe colaborar para el cumplimiento de esta política, es responsable de que la información se

registre en los sistemas de gestión documental y, en caso de ser necesario, se almacenen en los espacios físicos correspondientes.

La protección de registros físicos para la documentación de la Dirección Nacional de la SUPEREDUC, se especifica en el "*Manual de operaciones y procedimientos de oficina de partes*" vigente.

6.2. Protección de registros de base de datos y transacciones

Consiste en dar seguridad a las bases de datos transaccionales de la Superintendencia y que sustentan la operación de los sistemas informaticos de la organización. Los profesionales del Departamento de Tecnología y Procesos deben velar y resguardar que las bases de datos sean protegidas mediante el control de acceso a ellas, cifrado de la información y monitoreo de sus transacciones.

Las Jefaturas de División e Intendencia de Educación Parvularia, en conjunto con el Departamento de Tecnologías y Procesos, deben definir los periodos de retención para las bases de datos de los sistemas institucionales. Los registros serán respaldados semanalmente o periódicamente dependiendo de la cantidad de información a respaldar de acuerdo a la "*Política de respaldo de información*" y a la "*Política de respaldo de servidores*" vigente en la institución.

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

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

Frente a cualquier incidente o evento de seguirdad, se debe generar las alertas y acciones mediante el "*Procedimiento de incidentes de seguridad de la información*" vigente.

6.3. Protección de registros de auditoria

El/la Jefe/a del Departamento de Auditoria de SUPEREDUC debe disponer 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 así como también su almacenamiento.

Respecto de las copias digitales de los informes de Auditoría, estas se almacenan en carpeta compartida administrada por el Jefe/a del Departamento de Auditoria, con los resguardos de acceso al equipo definidos para todos los equipos de la institución.

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 su continua idoneidad, eficiencia y efectividad.

Una vez que el documento entre en vigencia el/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 podrán ser intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

8. Revisión del cumplimiento de la Política

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 ésta 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 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 del procedimiento

REVISIONES DEL PROCEDIMIENTO			
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 Paginas.

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 irroga gasto alguno para esta Superintendencia de Educación.

5. **REMÍTASE,** copia de la presente Resolución Exenta todas las Divisiones, Intendencias, 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.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACION
SUPERINTENDENTE

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.
- Departamento Jurídico.
- Unidad de Transparencia.
- Encargado/a de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.