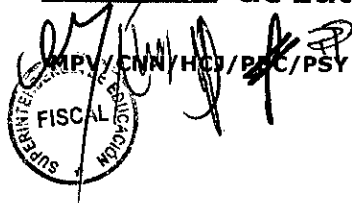


Gobierno
de Chile

Superintendencia
de Educación



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

RESOLUCIÓN EXENTA N° 0727

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 República 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 las cuales se encuentra la que regula la Política devolución de activos de información.

RESUELVO:

1. **APRUÉBASE**, la Política devolución de activos de información, versión N°1, en la Superintendencia de Educación, cuya transcripción, fiel, exacta e íntegra 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.



Distribución:

1. Gabinete.
2. División de Fiscalización.
3. División de Fiscalía.
4. División de Promoción y Resguardo de Derechos Educativos.
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 TRAMITADA



SuperIntendencia
de Educación

POLÍTICA DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN

Versión: 1.0

POLÍTICA DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN

VERSIÓN 1.0


CONTROL ISO27001:2013

A.8.1.4



INDICE

1. Objetivo:.....	5
2. Alcance:	5
3. Roles y Responsabilidades:	5
4. Definiciones:.....	6
5. Documentos relacionados:	7
6. Política:	7
6.1. Acceso a las dependencias:.....	7
6.2. Áreas seguras:	7
6.3. Controles de acceso para las áreas seguras:.....	8
6.4. Acceso a equipos TI y dispositivos en área seguras	8
6.5. Revisión y revalidación de accesos	8
7. Publicación y comunicación de esta política.....	9
8. Aceptación de la política.....	9
9. Revisión de la política	10
10. Sanciones aplicables.....	10
11. Control de versiones:	10
12. Responsabilidades de elaboración y aprobación del documento:.....	10

	POLÍTICA DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN
	Versión: 1.0

1. Objetivo:

Definir las directrices y requisitos en el marco del Sistema de Gestión de Seguridad de la Información, en la Superintendencia de Educación (SUPEREDUC), mediante la correcta gestión de la devolución de activos de información, respecto a las personas que trabajan o presten servicios en la institución.

2. Alcance:

Esta política se aplica a todas las áreas de SUPEREDUC y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas.

Es aplicable a todos los usuarios¹ de SUPEREDUC, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presente servicios a la SUPEREDUC.

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

- A.08.01.04 Devolución de activos.

3. Roles y Responsabilidades:

3.1. Jefatura de Unidad, Departamento o División:

- 3.1.1. Solicitar la creación/eliminación de la cuenta de correo institucional y los sistemas de información.
- 3.1.2. Recopilar y revisar los antecedentes mínimos para el inicio la solicitud de ingreso y accesos de derechos.

3.2. Funcionario/a designado/a Departamento Gestión de Personas:

- 3.2.1. Notificar cualquier ingreso/desvinculación de funcionarios al Departamento de Administración y al Departamento de Tecnología de Información.

3.3. Departamento de Tecnologías de Información:

- 3.3.1. Crear/eliminar los accesos básicos a los nuevos funcionarios.
- 3.3.2. Revisar y gestionar los permisos de acceso a los sistemas de información.
- 3.3.3. Eliminar los derechos de acceso a los funcionarios desvinculados o que egresen de SUPEREDUC.
- 3.3.4. Recuperar los activos de información tecnológicos de los funcionarios desvinculados o que egresen de SUPEREDUC.

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. Departamento de Administración:


- 3.4.1. Recuperar los activos de información de los funcionarios desvinculados o que egresen de SUPEREDUC.

3.5. Encargado/a de Seguridad de la Información:

- 3.5.1. Difundir esta política.
3.5.2. Coordinar revisiones periódicas en el cumplimiento de esta política.

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) **Bienes con cargo:** Todos aquellos activos físicos de patrimonio de SUPEREDUC necesarios para el desempeño de las funciones de un/a funcionario/a y que se asignan y mantienen bajo su responsabilidad. Ejemplos: mobiliario de oficina, dispositivos de escritorio, insumos de librería, celulares, entre otros/as.
- c) **Desvinculación:** Finalización de la relación laboral de un/a funcionario/a planta, contrata o persona a honorarios con la Institución.
- d) **Información de valor para la Institución:** Corresponde a una selección en versiones originales y finales de documentos físicos o archivos y/o registros digitales de carácter institucional cuyo valor se aprecia por disponer alguna/s de las siguientes características:
- I. Son estratégicos o altamente especializados (Ej: planes de fiscalización, rendición de cuentas).
 - II. Son únicos en las áreas que los generan, manipulan y/o conservan (Ej: memorándums, planilla de seguimiento).
 - III. Sustentan la generación o seguimiento de acciones civiles, administrativas y/o penales frente a terceros (Ej: antecedentes de una fiscalización, una investigación sumaria).
 - IV. Contienen datos sensibles de personas externas a la Institución (Ej: Antecedentes sociales de la comunidad educativa al realizar una denuncia).
 - V. Representan valor económico y/o respaldo de acciones financieras. (Ej: boletas de garantía).
 - VI. Involucran el cumplimiento de un requisito legal, normativo o contractual. (Ej: cualquier resolución de contrato).

 <p>Gobierno de Chile Superintendencia de Educación</p>	POLÍTICA DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN
	Versión: 1.0

VII. Correspondan a versiones originales de documentos oficiales de SUPEREDUC (Ej: Resoluciones).

e) **Movilidad interna:** Corresponde a todo movimiento de funcionario/a o persona a honorarios a nivel interno en SUPEREDUC.

5. Documentos relacionados:

- a) Política general de seguridad de la información.
- b) Procedimiento de egreso de personas.
- c) Procedimiento de enrolamiento cuentas de usuarios.

6. Política:

6.1. Registro de nuevos usuarios:

La Jefatura de la Unidad, Departamento o División es responsable de solicitar los accesos básicos para los nuevos funcionarios mediante el "Formulario de solicitud de creación/eliminación de accesos" firmado.

El área de Operaciones del Departamento de Tecnologías de información (TIC) es responsable de la creación de los accesos básicos de ingreso que incluye:

- a) Creación de cuenta de correo electrónico.
- b) Creación de usuario en Active Directory.
- c) Habilitación de estación de trabajo.

Las contraseñas de acceso temporales de ingreso se realizarán de acuerdo al "Procedimiento de enrolamiento cuentas de usuarios" además se informará al nuevo usuario sus responsabilidades implicadas en el uso de los sistemas de SUPEREDUC.

Las condiciones de uso incluyen:

- a) Mantener confidenciales las contraseñas secretas.
- b) Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Seguridad de la Información, en todo lo que sea de su competencia.
- c) No divulgar información perteneciente a SUPEREDUC.
- d) Comprender la responsabilidad funcionara, aun fuera de las dependencias de trabajo y fuera de horario normal de trabajo.

6.2. Registro de usuarios en los sistemas de información:

La Jefatura de la Unidad, Departamento o División es responsable de solicitar los accesos básicos para los nuevos funcionarios mediante el "Formulario de solicitud de creación/eliminación de accesos" firmado.



El Departamento TIC es responsable de chequear que el nivel de acceso solicitado es apropiado para el propósito institucional y que sea consistente con las Políticas de Seguridad de la Información.

6.3. Revisión de derechos de acceso del usuario.

La administración de los perfiles de usuario radica en los Usuarios líderes de los sistemas de información y las Jefaturas de División correspondientes.

Para administrar los accesos a los sistemas de información se definirán perfiles de acceso asignables a grupos de usuarios que, por su responsabilidad en la organización, presenten necesidades de acceso equivalentes.

El Encargado de Seguridad de la Información es responsable de que se efectúe la revisión de los derechos de acceso de acuerdo a los siguientes lineamientos:

- a) Se debe revisar los derechos de acceso de los usuarios cada 6 meses.
- b) Las autorizaciones para derechos de acceso con privilegios especiales se deben revisar a intervalos de 3 meses.
- c) Se debe chequear la asignación de privilegios para asegurar que no se hayan obtenidos privilegios no autorizados.
- d) Chequeo de IDs de usuarios y cuentas redundantes.
- e) Los accesos de cuentas con mayores privilegios, deben ser revisados al menos 2 veces al año.

Revisión después de cualquier cambio, como ascenso, remoción o terminación del empleo.

Los Usuarios Líderes de los sistemas, deben revisar en forma periódica los perfiles de usuarios del personal vigente y solicitar al Encargado del área de sistemas del Departamento de Tecnologías de Información la actualización de estos cada vez que ocurra un cambio en la definición de funciones.

6.4. Devolución de activos y revocación de derechos de acceso

Todo funcionario/a es responsable de devolver todos los activos pertenecientes a SUPEREDUC que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.

Si un funcionario/a posee conocimiento que es importante para las operaciones en curso, es su responsabilidad documentar dicha información y transferirla a SUPEREDUC.



6.5. Recuperación de activos y revocación de derechos de acceso

La Jefatura o el Coordinador Administrativo del área involucrada es responsable de informar cualquier desvinculación de funcionarios mediante el "Formulario de solicitud para creación/eliminación de accesos" esta notificación debe ser enviada simultáneamente a:

- a) Departamento Gestión de Personas.
- b) Departamento de Administración.
- c) Departamento de Tecnologías de Información.

Ante el informe de desvinculación de algún funcionario/a, el Departamento de Administración es responsable de gestionar la recuperación de los activos asignados al funcionario/a. entre otros, se encuentran:

- a) Documentos corporativos.
- b) Equipamiento.
- c) Teléfonos Móviles.
- d) Tarjetas de acceso.

Los activos recuperados deben ser registrados en el Sistema de Inventario.

El Departamento TIC, es responsable de eliminar los derechos de acceso a los sistemas de información, junto con recuperar los activos de información asignados al funcionario, entre otros se encuentran:

- a) Software.
- b) Licencias.
- c) Manuales.
- d) Cualquier información almacenada en medios electrónicos.

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 SUPE REDUC, 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

 Superintendencia de Educación	FORMULARIO: SOLICITUD PARA CREACIÓN/ELIMINACIÓN DE ACCESOS DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN DIVISIÓN DE ADMINISTRACIÓN GENERAL	FRM-CEA
	Versión: 1.0	Fecha: XX-XX-2017

FORMULARIO DE SOLICITUD PARA CREACIÓN/ELIMINACIÓN DE ACCESOS

1. TIPO DE SOLICITUD

CREACIÓN DE USUARIO		FECHA DE SOLICITUD	
ACCESO A SISTEMA			
ELIMINACIÓN DE ACCESO			

2. JEFATURA QUE SOLICITA

NOMBRE COMPLETO	
UNIDAD, DEPARTAMENTO, DIVISIÓN	
EMAIL	
FONO-ANEXO	

3. IDENTIFICACIÓN DEL FUNCIONARIO

NOMBRE COMPLETO	
RUT	
CARGO	
UNIDAD, DEPARTAMENTO, DIVISIÓN	
CALIDAD JURIDICA	
FECHA DE INGRESO A LA INSTITUCION	

4. SISTEMA(S) A LOS QUE SE SOLICITA ACCESO/ELIMINACION

1	
2	
3	
4	
5	

**FIRMA DE JEFATURA QUE
 SOLICITA**

**Ingresar solo 1 funcionario por solicitud*