Gobierno de Chile

Superintendencia de Educación

MPV/CNN/HCJ/PAC/PSV

APRUEBA POLÍTICA CONTROL DE ACCESO LÓGICO, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN, EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0726

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 control de acceso lógico.

RESUELVO:

1. **APRUÉBASE,** la Política control de acceso lógico, 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.

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACION
SUPERINTENDENTE

ALEXIS RAMÍREZ ORELLANA
SUPERINTENDENTE
SUPERINTENDENCIA DE EDUCACIÓN

Distribución:
1. Gabinete.
2. División de Fiscalización.
3. División de Promoción y Resguardo de Derechos Educacionales.
4. Fiscalía.
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.

Intendencia de Educación
ENTE TRAMITADO

POLÍTICA CONTROL DE ACCESO LÓGICO

VERSIÓN 1.0

CONTROL ISO27001:2013
A.9.1.1

ÍNDICE

1. Objetivo:

Establecer las definiciones que regulen un adecuado acceso a los sistemas de información de la Superintendencia de Educación (SUPEREDUC), impedir el acceso no autorizado a los sistemas de información y concientizar a los usuarios respecto de su responsabilidad de acceso a la información frente a la utilización de contraseñas y equipos.

2. Alcance:

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

Esta política aplica a todos los usuarios[1] de SUPEREDUC, ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presenten servicios a la SUPEREDUC.

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

- A.09.01.01 Política de control de acceso.

3. Roles y Responsabilidades:

3.1. Jefe/a Departamento de Tecnologías de Información:

3.1.1. Disponer de los controles y reglas de control de acceso lógico.

3.1.2. Gestionar los derechos de acceso a los medios de procesamiento de información que tengan a su cargo según lo descrito en esta política.

3.1.3. Mantener un registro de los accesos definidos.

3.2. Jefaturas directas/Usuarios líderes de los sistemas de información:

3.2.1. Validar y aprobar los accesos a los sistemas de información a su cargo, cuidando de mantener una adecuada segregación de funciones.

3.2.2. Aprobar los cambios directos en las bases de datos de los sistemas a su cargo.

3.2.3. Definir los accesos a los datos por parte de los usuarios de SUPEREDUC cuidando de mantener una adecuada segregación de funciones.

3.3. Encargado/a de Seguridad de la Información:

3.3.1. Autorizar las excepciones a la segregación de funciones establecidas en esta política.

---

[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.*

4. Definiciones:

a) **Acceso a la información:** Se refiere al conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema: bases de datos, bibliotecas, archivos e Internet.

b) **Derechos de accesos**: Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recurso.

c) **Restringir el acceso:** Delimitar el acceso de los funcionarios/as, servidores públicos a honorarios y terceras partes a determinados recursos.

d) **Sistema informático:** uno o más computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.

e) **Usuario:** persona que utiliza un sistema informático y recibe un servicio, tales como: correo electrónico o red de conectividad proporcionado o administrado por la SUPEREDUC, ya sea que lo utilice en virtud de un empleo, de una función o de cualquier prestación de servicio, sin importar la naturaleza jurídica de ésta o del estatuto que lo rija.

5. Documentos relacionados:

a) Política general de seguridad de la información.

b) Política devolución de activos.

c) Política control de acceso físico.

d) Procedimiento de incidentes de seguridad de la información.

6. Política:

6.1. Cumplimiento de la legislación:

Las medidas de control de acceso lógico definidas deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales.

6.2. Control de acceso a la información:

Todos los usuarios de SUPEREDUC, incluso terceros, deben tener acceso **sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de SUPEREDUC**, de acuerdo al principio del **"need to know[2]".** La asignación de privilegios y accesos a los activos de información deben ser basados en las necesidades de las áreas y aprobados por el propietario de los activos.

[2] *El acceso a la información confidencial se debiera basar en el principio de mínimo conocimiento y debe ser autorizada por su supervisor.*

Estas necesidades de acceso deben ser determinadas por las respectivas Jefaturas, en función de las tareas asignadas al cargo del funcionario.

Para todo medio de procesamiento de información al que se necesite conceder accesos (por ejemplo: servidores, aplicaciones, carpetas compartidas, etc.) el responsable de la información en conjunto con el área de operaciones y servicios TI dependiente del Departamento de Tecnologías de Información, será encargado de autorizar y según corresponda el conceder los permisos de acceso.

Solo se deben conceder accesos a terceros previa solicitud del responsable del medio de procesamiento de información y al responsable de la información, y nunca antes de haberse firmado un acuerdo de confidencialidad. Las cuentas de acceso a terceros deben tener especificado un tiempo de expiración el que debe ser controlado por el administrador de plataformas del área de operaciones y servicios TI, según corresponda.

El comité Directivo de Seguridad de la Información tiene las facultades de suspender o eliminar los accesos a cualquier usuario que represente riesgo en la confidencialidad, integridad o disponibilidad de la información.

Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas de información, bases de datos, serán considerados como un incidente grave, por lo que debe reportarse de inmediato según lo descrito en el *"Procedimiento de incidentes de seguridad de la información"*.

6.3. Administración del Acceso:

La administración de perfiles en las aplicaciones radica en los usuarios líderes de los sistemas de información y las Jefaturas de División correspondientes. La responsabilidad de asignar un determinado perfil de usuario corresponderá a la Jefatura de División solicitante o a quien se delegue.

No se podrá otorgar acceso a los sistemas a ningún usuario hasta que se haya completado el formulario el *"Formulario de solicitud de creación/eliminación de accesos"* firmado.

Para facilitar la administración de accesos, se debe definir de accesos asignables a grupos de usuarios que, por sus responsabilidades en la organización, presenten necesidades de acceso equivalentes.

El Departamento de tecnología de información (TIC), implementa las reglas de control de acceso solicitadas por los administradores de aplicaciones y las Jefaturas de División correspondientes.

6.4. Administración de accesos especiales:

El otorgamiento de accesos con mayores privilegios (por ejemplo, acceso a: base de datos, código fuente, etc.) a funcionarios/as que no pertenezcan al Departamento TIC. Debe ser solicitado por la Jefatura de División responsable o quien delegue, al Jefe/a del Departamento TIC y autorizado por el Encargado de Seguridad de la Información justificando la solicitud.

6.5. Segregación de funciones:

Los derechos de acceso deben ser asignados a perfiles individuales, de forma tal que las acciones realizadas con los accesos otorgados, sean de responsabilidad del usuario.

El otorgamiento de accesos respecto a recursos de información de SUPEREDUC debe considerar una adecuada segregación de funciones, de modo que un mismo usuario no pueda disponer por su voluntad, del control de un proceso de negocio completo.

Las excepciones a la regla anterior deben ser aprobadas por la jefatura de División correspondiente y autorizadas por el Jefe/a del Departamento TIC.

6.6. Revisión de los derechos de acceso:

El Departamento TIC, es responsable de los accesos de los administradores de aplicaciones, de tal forma que se establezca un control efectivo desde el registro inicial de la cuenta hasta el momento en que requiera ser modificada, revocada o eliminada *ver Política de devolución de activos.*

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.

6.7. Revocación de acceso lógicos:

Ante situaciones de cambio de cargo de un usuario, se debe revisar sus permisos de acceso lógico asignados y verificar que estos sigan siendo válidos de acuerdo a su nueva función.

Cuando un funcionario/a termina su relación laboral con SUPEREDUC, todos sus permisos de acceso a la información deben ser revocados.

Es responsabilidad de las Jefaturas Directas informar formalmente las desvinculaciones al Departamento de Gestión de personas o al coordinador regional de administración, según sea el caso.

6.8. Revisión de los accesos:

Los usuarios líderes de aplicaciones deben revisar en forma periódica los perfiles de usuario/a del personal vigente y solicitar al Departamento TIC, la actualización de estos cada vez que ocurra un cambio en la definición de funciones. Cualquier cambio en las funciones de una persona que acceda a información del negocio deberá verse reflejado en sus privilegios de acceso.

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 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