Superintendencia de Educación
TOTALMENTE TRAMITADO

Superintendencia de Educación
Ministerio de Educación
Gobierno de Chile

MIC/FTO/AAM/BBC/DLR

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0726, DE 2017 Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA CONTROL DE ACCESO LÓGICO, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0766

SANTIAGO, 27 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 el Decreto de Nombramiento del Superintendente de Educación, en trámite, 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 N° 0726, que aprueba versión 1.0 de la política control de acceso lógico de la Superintendencia de Educación.

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, 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 y Ciberseguridad lo mantenga y mejore en el tiempo.

5. Que, debido a una serie de cambios institucionales y a la revisión efectuada por la Encargado/a de Seguridad de la Información y Ciberseguridad, se ha estimado procedente reestructurar, ajustar y actualizar el contenido del procedimiento revisión de los requisitos de legislación.

RESUELVO:

1. **DÉJASE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0726, de 2017 de la Superintendencia de Educación.

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

Política control de acceso lógico

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

El control de acceso lógico es la principal línea de seguridad para los sistemas, aplicaciones e instalaciones de procesamiento de información por lo que establece los requisitos de acceso, donde todo usuario interno de la institución deberá poseer una cuenta de usuario personal, que actuará como una credencial que lo identifique, y que le permitirá tener acceso a los recursos de la red corporativa de la Superintendencia de Educación.

La siguiente política establece las definiciones que regulan el adecuado acceso a los sistemas de información de la Superintendencia de Educación (SUPEREDUC), impedir el acceso no autorizado y concientizar a los usuarios respecto de su responsabilidad en el acceso a la información y 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[1].

Es aplicable a todos los usuarios, funcionarios, colaboradores, practicantes o personal externo que preste servicios permanentes o temporales, y/o aquellos utilizados dentro de las dependencias de 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. Referencias normativas

- Política general de seguridad de la información de la Superintendencia de Educación vigente.
- Política devolución de activos de la Superintendencia de Educación vigente.
- Política de control de acceso físico de la Superintendencia de Educación vigente.
- Procedimiento gestión de incidentes de seguridad de la información de la Superintendencia de Educación vigente.
- Procedimiento de administración de cuentas privilegiadas, VPN y accesos restringidos 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.

4. Definiciones

Concepto	Descripción
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.
Derechos de acceso	Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recurso.
Restringir el acceso	Delimitar el acceso de los funcionarios/as, servidores públicos a honorarios y terceras partes a determinados recursos.
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.
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.

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

5. Roles y Responsabilidades

Rol	Responsabilidades
Departamento de Tecnologías y Procesos de Información	a) Disponer de los controles y reglas de control de acceso lógico b) Gestionar los derechos de acceso a los medios de procesamiento de información que tengan a su cargo según lo descrito en esta política c) Mantener un registro de los accesos otorgados a los usuarios de la SUPEREDUC. d) Gestionar y administrar la información de autenticación de usuarios de la SUPEREDUC. e) Propone, define e implementa las medidas de seguridad a implementar, para resguardar las cuentas de usuarios y sus respectivas contraseñas. f) Punto de contacto para orientar, asesorar, actualizar y restaurar problemas relacionados con las contraseñas de los usuario de la Superintendencia.
Jefaturas de la SUPEREDUC	a) Validar y aprobar los accesos a los sistemas de información a su cargo, cuidando de mantener una adecuada segregación de funciones. b) Definir los accesos a los datos por parte de los usuarios de SUPEREDUC cuidando de mantener una adecuada segregación de funciones. c) 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
Departamento de Gestión y Desarrollo de Personas	a) Mantener un registro de la nómina de funcionarios y personas contratadas por la Superintendencia de Educación para que en virtud de sus funciones se le puedan otorgar permiso de acceso a los sistemas informáticos y activos de información de la institución.
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 entrega y utilización de contraseñas, evaluar circunstancias particulares al uso de estas y en caso de ser identificarse eventos de seguridad, activar el protocolo de incidentes de seguridad de la información vigente en la SUPEREDUC. c) Velar por la correcta aplicación de la política y apoyar en las unidades técnicas responsable de la administración y gestión de usuarios y contraseñas. d) Actualizar la política, con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.

6. Directrices

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 que establece el sistema de Seguridad de la Información y Ciberseguridad de la Superintendencia de Educación.

6.2. Control de acceso a la información y sistemas informáticos.

a) Para todo sistema computacional y de procesamiento de la información, los usuarios de la SUPREDUC deberán señalar quién es (identificación), y luego deberá comprobar que es quien dice ser (autentificación) para recién autorizar sus acciones (autorización).

e) 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 con el principio del "**need to know2".** La asignación de privilegios y accesos a los activos de información, que otorgue el departamento de Operaciones dependiente del Departamento de Tecnología y Procesos, deben ser basados en las necesidades de las áreas y aprobados por el propietario de los activos. Estas necesidades de acceso deben ser determinadas por las respectivas Jefaturas, en función de las tareas asignadas al cargo del funcionario.

f) 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, dependiente del Departamento de Tecnologías y Procesos, será Encargado de autorizar y según corresponda el conceder los permisos de acceso.

g) Se concederá 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.

h) Toda cuenta de acceso de un usuario interno o tercero, deberá contar con una clave única, segura e intransferible de acuerdo a lo que establezca la *"política de uso de contraseñas"* vigente en la SUPEREDUC.

i) 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 del Departamento de Tecnología y Procesos, según corresponda.

j) El Comité Operativo 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.

k) Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas de información, base de datos, serán considerados como un incidente grave, por lo que debe reportarse de inmediato al encargado/a de Seguridad de la Información y Ciberseguridad, según lo descrito en el "*Procedimiento gestión de incidentes de seguridad de la información"* vigente y publicado en la intranet institucional.

6.3. Administración del Acceso

a) La administración de perfiles en las aplicaciones radica en el Departamento de Tecnología y Procesos, de los sistemas de información. Sin embargo, la mantención y asignación de un determinado perfil de usuario, lo autorizará las Jefaturas de División correspondientes.

b) 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", vigente y publicado en la intranet de la Superintendencia de Educación.

---

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

c) Para facilitar la administración de accesos, El Departamento de Tecnología y Procesos definirá accesos asignables a grupos de usuarios que, por sus responsabilidades en la organización, presenten necesidades de acceso equivalentes.

d) El Departamento de Tecnologías y Procesos, implementa las reglas de control de acceso solicitadas por los administradores de aplicaciones y las Jefaturas de División correspondientes.

6.4. Gestión de privilegios

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 de Tecnologías y Procesos. Debe ser solicitado por la Jefatura de División responsable, al Jefe/a del Departamento de Tecnologías y Procesos.

6.5. Administración de accesos a recursos restringidos

La solicitud de acceso temporal a recursos de Internet que se encuentren restringidos, será por un periodo máximo de 90 días y deben ser solicitados por la Jefatura de División responsable, al Jefe/a del Departamento de Tecnologías y Procesos justificando la solicitud, de acuerdo al "Procedimiento de administración de cuentas privilegiadas, VPN y accesos restringidos", y completando el "Formulario de solicitud de acceso a recursos restringidos de internet" el cual se encuentra publicado en la Intranet institucional.

6.6. Segregación de funciones

a) 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.

b) 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.

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

6.7. Revisión de los derechos de acceso

a) El Departamento de Tecnologías y Procesos, 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.

b) El Departamento de Tecnologías y Procesos es responsable de que se efectúe la revisión de los derechos de acceso de acuerdo con los siguientes lineamientos:

- Se debe revisar los derechos de acceso de los usuarios cada 6 meses.
- Las autorizaciones para derechos de acceso con privilegios especiales se deben revisar a intervalos de 3 meses.

- Se debe chequear la asignación de privilegios para asegurar que no se hayan obtenidos privilegios no autorizados.
- Chequeo de IDs de usuarios y cuentas redundantes.
- Los accesos de cuentas con mayores privilegios deben ser revisados al menos 2 veces al año.

6.8. Revocación de acceso lógicos

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

6.9. 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 de Tecnologías y Procesos, 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. 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/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 POLÍTICA			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
1.0	Octubre 2017	Versión inicial	Versión inicial
2.0	Diciembre 2019	Actualización 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 EDUCACION
SUPERINTENDENTE

CRISTIÁN CRYAN 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.