Superintendencia de Educación

Gobierno de Chile

Superintendencia de Educación
TOTALMENTE TRAMITADO

MIC/FTO/AAM/PBC/DLR

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0725, DE 2017, Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA DE PERÍMETROS DE SEGURIDAD FÍSICA, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN, EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0765

SANTIAGO, 27 DIC 2019

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 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; 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° 0725, que aprueba política perímetros de seguridad física versión N°1, 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 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, con fecha 02 de diciembre de 2019 se dicta Resolución Exenta N° 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° 0725, de 2017 de la Superintendencia de Educación.

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

Política perímetros de seguridad física

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

Como parte de las políticas de seguridad de la información, se debe velar por el resguardo físico de los equipos e instalaciones sensibles, para prevenir el acceso físico no autorizado, evitar daños o robo a los activos de información y procesamiento, a fin de velar por la integridad y disponibilidad de la información contenida en el sistema informático de la SUPEREDUC.

La siguiente política establece las directrices y requisitos para los perímetros de seguridad, controles de ingreso y protección física para proteger las áreas que contienen información

sensible y medios de procesamientos de información en la Superintendencia de Educación (SUPEREDUC).

2. Alcance

Esta política se aplica en particular, a las áreas definidas como seguras, ubicadas en los edificios de SUPEREDUC localizados en calle Morandé Nº 115, piso N°10, piso N°11 y piso N°12; calle Morandé N° 360 Piso Nº 5, sala de servidores (datacenter), ambas ubicadas en Santiago y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas[1].

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, que necesiten tener acceso a las instalaciones de la Superintendencia de Educación donde se procesa la información y que se entienden por:

- Oficinas de la SUPEREDUC donde existe procesamiento de información, unidad de compras, departamento de tecnología, fiscalización, oficina de parte, direcciones regionales, etc.
- Áreas con servidores, para procesamiento o de comunicación (red interna).
- Áreas donde se almacenan y guardan elemento de respaldos de datos (CD, discos duros, cintas, etc.)

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

- A.11.01.01 Perímetro de seguridad física.

3. Referencias normativas

- Política General de Seguridad de la Información de la Superintendencia de Educación vigente.
- Política Control de Acceso Físico de la Superintendencia de Educación vigente.
- Procedimiento de actualización de activos y evaluación de riesgos de la Superintendencia de Educación vigente.
- Procedimiento de administración de comunicaciones, emplazamiento y mantención de equipo 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.
- Procedimiento de acceso visitas Dirección Nacional 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
Perímetro de seguridad física	Está constituida por la zona cercada por los elementos físicos que en conjunto permiten diferenciar las instalaciones de la

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

Concepto	Descripción
	Superintendencia respecto del exterior, como paredes, puertas, accesos, salidas y entradas, protegidos con dispositivos de control de acceso magnético o biométrico, o un puesto manual de recepción
Visita	Se considerará como visita toda aquella persona externa a la SIE, que no cumpla funciones regulares o periódicas con el servicio. El servicio de vigilancia y control de acceso podrá mantener un registro con los antecedentes de visitas habituales, el que podrá ser utilizado solo para efectos de agilizar el registro de ingreso de las personas, previa confirmación de su identidad.
Áreas seguras	Corresponde a las áreas que contienen información sensible o crítica y las instalaciones de procesamiento de información. Dentro de las áreas establecidas como segura, se encuentran definidas las salas de servidores o data center de la SIE, cuyo acceso es administrado por personal del Departamento de Tecnología y Proceso, bodegas y archivos que almacenen activos críticos, cuyo acceso es administrado por cada una de las divisiones, intendencias y/o áreas internas.

5. Roles y Responsabilidades

Rol	Responsabilidades
Departamento de Administración.	a) Disponer el control de acceso físico general al edificio de SUPERDEDUC ubicados en calle Morandé N°115, piso N°10, N°11 y N°12; calle Morandé N°360 Piso N°5 sala datacenter. b) Difundir las directrices para los perímetros físicos definidos por SUPEREDUC. c) Mantener inventario actualizado de los bienes de la SUPEREDUC. d) Contraparte técnica del servicio de vigilancia y control de acceso dispuesto o contratado por la Superintendencia.
Departamento de Tecnologías y Procesos	a) Controlar y gestionar los accesos a las salas de procesamiento de datos y comunicaciones (datacenter) b) Mantener un registro de la nómina de funcionarios y personas contratadas por la Superintendencia de Educación con permiso de acceso a las dependencias del Servicio, según los perímetros de seguridad física establecidos.
Usuario	a) Personas, funcionarios, colaboradores, practicantes o personal externo que preste servicio permanente o temporal que, con debida autorización, acceden a las instalaciones físicas de la SUPEREUC, por lo que mantienen la responsabilidad de hacer cumplir lo establecido en esta política
Jefaturas de la SUPEREDUC	a) Definir áreas o espacios seguros bajo su dependencia b) Autorizar el acceso de personas externas a las áreas seguras bajo su dependencia 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.
Encargado/a de Seguridad de la Información.	a) Velar por la difusión y cumplimiento de esta política. b) Monitorear el correcto funcionamiento y operación respecto el cumplimiento del control de acceso a las instalaciones de la SUEPREDUC, en particular en cuanto al acceso a sistemas o información sensible que posee la institución.

	c) Velar por la correcta aplicación de la política y apoyar en las unidades técnicas responsable de la administración y aplicación de los controles de accesos necesarios para la SUPEREDUC. d) Actualizar la política, con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.

6. Directrices

6.1 Perímetros de seguridad

a) Los perímetros de seguridad de SUPEREDUC deben estar claramente definidos, la ubicación y la resistencia de cada uno de los perímetros dependerá de los requisitos de seguridad de los activos dentro del perímetro.

a) Todo perímetro de seguridad o equipo informático, debe tener algún tipo de seguridad física; seguridad de la oficina, seguridad de los equipos computacionales, equipos de control del medio ambiente, etc. Con el fin de evitar el acceso por personas no autorizadas, daño o interferencias a los recursos e infraestructura de información de la institución.

b) Las medidas de seguridad que se deban tomar para las áreas seguras, dependerán directamente del valor de los activos de información, su nivel de confidencialidad y disponibilidad.

6.2 Áreas seguras

Las áreas seguras de SUPEREDUC corresponden a las siguientes:

a) Las áreas o espacios establecidos en el Inventario de Activos de Información, sólo en casos que estos contengan activos críticos (confidenciales) a partir de su ubicación.

b) Las áreas o espacios físicos críticos definidos por las Jefaturas Superiores. Algunos de estos espacios son reconocibles por los activos que resguardan, por ejemplo: sala de servidores, caja fuerte, archivos de la oficina de partes, espacios con gabinetes eléctricos, equipos de comunicaciones o grupo electrógeno entre otros.

c) Las áreas establecidas por la Jefatura del Departamento de Tecnologías y Procesos que mantienen sistemas de información, equipos de cómputo y comunicaciones.

6.3 Controles de acceso para las áreas seguras

a) A partir de las áreas seguras, las Jefaturas Directas deben disponer el acceso restringido y controlado, que permita asegurar que solo ingresa personal o terceros, debidamente autorizados.

b) Las visitas autorizadas a ingresar al perímetro de seguridad con información sensible deben quedar registradas en recepción según establece "*procedimiento control de acceso a visitas*" vigente, detallando nombre, fecha y hora de ingreso y egreso. Durante su permanencia debe estar siempre acompañado por personal debidamente autorizado, a menos que su acceso se haya aprobado previamente.

c) En cualquier caso, al interior de estas áreas seguras, no se permite el uso de equipos de fotografía, video, o cualquier otro sistema de grabación. La excepción

a esta regla debe ser formalmente autorizada por la jefatura de departamento respectiva.

d) Las Jefaturas Directas, ante la situación de un cambio de cargo de funcionario, deben revisar sus permisos de acceso físico asignados y verificar que estos sigan siendo válidos de acuerdo a su nueva función. En cuanto advierta cambios en los privilegios del usuario o funcionario, debe informar al Departamento de Tecnología y Procesos quien administra las cuentas de los usuarios que mantienen acceso a los sistemas y activos de información de la SUPEREDUC.
e) 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. Con el objetivo que el Departamento de Tecnología y Procesos deshabilite los permisos y privilegios asignados al usuario en cuestión.
f) Se debe tener separado físicamente la operación de terceros o externos con la operación propia de la institución. En caso de existir actividades con externos, se deberán establecer controles por el funcionario responsable del outsourcing requerido.

6.4Protección contra amenazas externas y del ambiente[2]

a) Las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimentos.
b) Las puertas y ventanas deben estar cerradas, para evitar riesgos externos que se pueden generar desde el medio ambiente externo a la Superintendencia.
c) Todo lugar de trabajo en que exista algún riesgo de incendio, ya sea por la estructura del edificio o por la naturaleza del trabajo que se realiza, debe contar con extintores[3] de incendio, del tipo adecuado a los materiales combustibles o inflamables que existen o se manipulen.
d) En cuanto a los equipos informáticos se debe tener un control de la temperatura y humedad, dado que puede afectar la operación de la institución con una falla de estos. Es importante mantener un estricto monitoreo sobre estas variables.
e) El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan. Así como también los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas vigentes.

6.5Trabajo en área críticas

a) El responsable de cada dependencia, que tenga a su cargo, es quien define las áreas críticas (si aplica). Cada vez que se defina un área de trabajo como critica el responsable de la dependencia debe informar al Encargado/a de Seguridad de la Información y Ciberseguridad de esta clasificación del área.

---

[2] Reglamento interno de Higiene y Seguridad.
[3] El número total de extintores dependerá de la superficie a proteger de acuerdo a lo señalado en el artículo 46 del Decreto Supremo N°594.

b) Las áreas críticas de SUPEREDUC corresponde a aquellas donde se encuentren ubicados los activos de información definidos como críticos y deben ser protegidos bajo las directrices definidas en esta política, contar con un acceso restringido y controlado, que solo permita el acceso a personal autorizado.

c) SUPEREDUC define como un área critica la sala de procesamiento de datos del Nivel Central, donde se almacenan equipos de procesamiento de datos. El control de acceso a la sala de procesamiento de datos se debe realizar de acuerdo al *"Procedimiento de administración de comunicaciones, emplazamiento y mantención de equipos"* vigente y publicado en la Intranet.

d) Todo empleado debe estar vigilante a la presencia de personas extrañas, sin identificación visible dentro de la instalación de la Superintendencia y en estos casos se debe reportar inmediatamente a la seguridad física que establezca la SUPEREDUC.

e) Todo visitante o extraño que se le facilite acceso a un área critica debe ser acompañados durante su estadía en la institución, debido a los riesgos que representa en cuanto que acceda a información confidencial.

6.6Áreas de acceso público, de entrega y de carga

a) El acceso a la entrega y carga desde fuera del edificio debe ser restringido a personal debidamente identificado y autorizado.

b) Todo elemento que ingrese a la SUPEREDUC debe ser inspeccionado el funcionario a cargo de recibir la carga, con el fin de identificar material peligroso y que coincida con su respectiva autorización de ingreso.

c) La carga o material entrante debe ser registrado, con el fin de mantener el listado de inventario actualizado.

d) Donde sea aplicable, las puertas externas deben ser aseguradas cuando se abran las puertas internas, el material que ingrese debe ser inspeccionado para evitar posibles amenazas antes de ser ingresado a su lugar de utilización.

e) Donde sea aplicable los envíos entrantes y salientes deben segregarse físicamente.

6.7Acceso a equipos TI y dispositivos en área seguras

a) En las salas de servidores o comunicaciones deben existir sistemas de detección de intrusos de acorde a estándares internacionales y deben cubrir todos los lugares que permitan el acceso. Las áreas de procesamiento de información gestionadas por SUPEREDUC deben estar físicamente separadas de aquellas gestionadas por terceras partes.

b) Todo ingreso o egreso de equipos de computación o de comunicaciones, debe ser autorizado y coordinado por el Departamento de Tecnologías y Proceso.

c) Los traslados de equipos deben ser adecuadamente registrados, considerando por lo menos, la identificación del equipo trasladado, su origen y destino, así como la identificación de la persona que lo traslada. Estos deben ser informados al Departamento de Administración para mantener actualizado su inventario.

6.8Revisión y revalidación de accesos

a) Cuando un funcionario/a termina su relación laboral con SUPEREDUC, es responsabilidad de las Jefaturas Directas informar al Departamento Gestión de Personas de estas situaciones, para proceder a revocar los accesos de acuerdo a lo establecido en el *"Procedimiento de creación, modificación, eliminación de cuentas e información y egreso de personas"* publicado en la Intranet.

b) Las Jefaturas pertinentes deben asegurar la revisión en forma periódica del estado de los funcionarios autorizados a acceder a las áreas críticas reconocidas, y realizar una actualización de estos cada vez que ocurra. La mantención de los accesos lógicos lo administra el departamento de Tecnología y Procesos.

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 POLITICA			
Nº 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 EDUCACION SUPERINTENDENTE

CRISTIÁN O'RYAN SQUELLA
SUPERINTENDENTE 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 Proceso.
- Departamento de Gestión Institucional.
- Departamento de Auditoria.
- Unidad de Transparencia.
- Encargado de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.