Superintendencia de Educación
Ministerio de Educación
Gobierno de Chile

Superintendencia de Educación
TOTALMENTE TRAMITADO

SUPERINTENDENCIA DE EDUCACIÓN FISCAL

MIC/FFO/AAM/BBC/DLR

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0729, DE 2017 Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA CONTROL DE ACCESO FÍSICO, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0764

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 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 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.

3. Que, con fecha 20 de octubre de 2017, se dicta Resolución Exenta N° 0729, que aprueba versión 1.0 de la política control de acceso físico de la Superintendencia de Educación.

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° 0729, de 2017 de la Superintendencia de Educación.

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

Política control de acceso físico

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

Con la finalidad de resguardar los activos de información, resulta fundamental dotar de condiciones físicas para resguardar los sistemas informáticos y los activos de información, para ellos se ha definido establecer la siguiente política, que establecer las definiciones que regulen el acceso físico de personas y/o equipos, evitando al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de procedimientos de seguridad, a las dependencias de la Superintendencia de Educación (SUPEREDUC) y en particular a las áreas seguras que así sean definidas por el Jefe/a del Departamento de Tecnología y Procesos.

2. Alcance

Esta política se aplica en particular, a las áreas definidas como seguras por la jefatura del Departamento de Tecnologías y Procesos, 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] y en la Matriz de Riesgo Institucional.

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

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 control de acceso lógico de la Superintendencia de Educación vigente.
- Inventario de Activos de Información vigente.
- Procedimiento de acceso visitas Dirección Nacional 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.
- 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 Superintendencia de Educación 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.
Tarjeta de acceso	Distintivo otorgado a las visitas que ingresan a las dependencias de la SIE, el cual deberá indicar expresamente el área a la cual tiene acceso la persona y un número de identificación (folio).
Servicio de vigilancia y control de acceso	Servicio dispuesto o gestionado por la SIE con el objeto de resguardar los accesos y bienes fiscales que se encuentren en las oficinas de la Dirección Nacional de la Superintendencia.
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
Jefatura del Departamento de Administración	a) Fomentar y efectuar las acciones necesarias para disponer el control de acceso físico general al edificio de SUPEREDUC ubicados en calle Morandé N°155, piso N°10, N°11 y N°12, calle Morandé N°360 Piso N°5 sala datacenter. b) Mantener inventario actualizado de los bienes de la SUPEREDUC. c) Contraparte técnica del servicio de vigilancia y control de acceso dispuesto o contratado por la Superintendencia.

Jefatura del Departamento de Tecnologías y Procesos de Información	a) Autorizar el traslado de equipos TI desde o hacia áreas seguras b) Asegurar el registro y mantención de una nómina de las personas con permiso de acceso particular las áreas seguras respecto del procesamiento tecnológico de información c) Mantener un catastro actualizado de los equipos TI ubicados en áreas seguras. d) Mantener un registro de la nómina de personas con permiso de acceso particular a áreas seguras respecto del procesamiento tecnológico de la información.
Departamento Gestión y Desarrollo de Personas	a) Mantener un registro de la nómina de funcionarios y personas contratadas por la Superitendencia de Educación con permiso de acceso a las dependencias del Servicio, según los perímetros de seguridad física establecidos.
Jefaturas de la SUPEREDUC	a) Autorizar el acceso de personas externas a las áreas seguras bajo su dependencia b) Las jefaturas de las Divisiones, Intendencia, Direcciones Regionales, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política.
Usuarios	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.
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 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. Control de acceso físico a las dependencias

a) El perímetro de seguridad física de SUPEREDUC definido en el alcance de esta política, deben ser resguardados mediante elementos físicos de seguridad, tales como: torniquetes de acceso, servicio de guardias en recepción, cámaras de seguridad, y el uso de tarjetas credenciales magnéticas o llaves en las puertas a las áreas de trabajo (oficinas) o espacios físicos (salas de reuniones, archivos y bodegas, etc.).

b) Los controles de acceso físico tendrán por lo menos, las siguientes características y resguardarán:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso.
- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.

b) Se utilizarán controles de autentificación para autorizar y validar accesos de externos, ejemplo; guardia con listado de personas habilitadas o por tarjetas magnética o inteligente y número de identificación personal. Además de contar con registro para permitir auditar todos los accesos dados.

c) El ingreso a los sectores restringidos por parte de los funcionarios se especifica en el *"Procedimiento de acceso visitas Dirección Nacional".*

d) Se establecerán normas para las distintas solicitudes de accesos que se solicitan a las dependencias de la SUPEREDUC. Clasificando la vista de acuerdo a la función de acceso (reunión, capacitación,

audiencia, mantención, etc.), horario (hábil o inhábil) y en los casos que se requieran se solicite la autorización a funcionarios o áreas de la SUPEREDUC.

e) Todo funcionario de la SUPEREDUC deberá tener acceso a una credencial de identificación; que contiene el nombre del funcionario, fotografía, departamento dependiente, logo institucional para que pueda acceder a las dependencias de la institución. Deberá portarla y utilizarla de manera visible.

6.2. Control y recomendaciones con las visitas

a) Las visitas autorizadas a ingresar a las dependencias del edificio de SUPEREDUC (calle Morandé N°115, pisos 10, 11 y 12), se le entregará una credencial de visita, según las indicaciones del *"Procedimiento de acceso visitas Dirección Nacional."*, vigente.

b) En cualquier caso, mientras toda persona externa permanezca al interior de las dependencias, deberá portar en un lugar visible la credencial de visita o similar identificación proporcionada por SUPEREDUC. Esta credencial e identificación proporcionada es intransferible.

c) Se debe tener separado, físicamente la operación de personal externo con la propias de la institución, en caso de existir servicios con proveedores externos, el encargado del contrato o servicio outsourcing contratado por la institución, deberá establecer controles de seguridad, principalmente respecto a su acceso a las áreas seguras de la SUPEREDUC.

d) Todo empleado debe estar vigilante a la presencia de personas extrañas sin identificación visible dentro de las instalaciones de la SUPEREDUC y en caso de identificar una persona extraña sin la autorización adecuada, se debe reportar el caso inmediatamente a los responsables de seguridad de la institución en el Departamento de Administración.

e) Todo los visitantes o extraños deben ser acompañados durante su estadía en la SUPEREDUC, debido a la existencia de información confidencial y a la posibilidad de extravío o hurto.

f) Las visitas autorizadas a ingresar al perímetro de seguridad con información sensible se especifican en el *"Procedimiento de acceso visitas Dirección Nacional".*

6.3. Clasificación de las 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, deben mantener algún tipo de seguridad, por ejemplo: estar protegidos por barreras y controles físicos, para evitar ocupación física, inundaciones, y otro tipo de amenazas que afecte su normal operación.

d) Las medidas de seguridad que se deban tomar, dependerán directamente del valor de los activos de información, su nivel de confidencialidad y disponibilidad.

6.4. Accesos revocados

a) Cuando un usuario termina su relación laboral con SUPEREDUC, es responsabilidad de las Jefaturas Directas informar al Departamento Gestión y Desarrollo de Personas de estas situaciones, para proceder a revocar los accesos de acuerdo a lo establecido en el *"Procedimiento de creación, modificación y eliminación de cuentas"*.

b) Las Jefaturas pertinentes deben asegurar la revisión en forma periódica del estado contractual de los usuarios autorizados a acceder a las áreas críticas reconocidas, y realizar una actualización de estos cada vez que ocurra.

6.5. Acceso a equipos TI y dispositivos en áreas seguras

a) En las salas de servidores y/o comunicaciones (datacenter) todo el equipamiento que contenga información confidencial, debe estar configurado con el estándar de condiciones de seguridad definidas por SUPEREDUC y aprobadas por el Departamento de Tecnologías y Procesos, además deben tener un acceso restringido y monitoreado.

b) Las puertas de acceso al datacenter deben considerar características técnicas necesarias para resguardar el equipamiento de TI.

c) Cuando se requieran mantenimientos sobre los equipos informáticos, se deben realizar únicamente por personal autorizado y supervisado por el Departamento de Tecnología y Procesos, reguardando las instalaciones y siempre tener en cuenta que mantiene información sensible.

6.6. Identificación y traslado de equipos

Todo equipo de computación o comunicaciones debe estar rotulado para su identificación, el traslado debe estar autorizado por el Jefe del Departamento de Tecnologías y Procesos de Información o a quien este delegue formalmente dicha responsabilidad, debe ser efectuado por el personal de soporte interno y se debe informar al Departamento de Administración (responsable de la actualización del inventario), dicho evento, debe identificar al menos, la persona, el equipo trasladado y los lugares de origen y destino.

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 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 EDUCACIÓN

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.
- Unidad de Transparencia.
- Encargado de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.

Gobierno de Chile

Superintendencia de Educación

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

RESOLUCIÓN EXENTA N° 0729

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 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 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 especificas de Seguridad de la Información, dentro de los cuales se encuentra la que regula la Política control de acceso físico versión N°1.

RESUELVO:

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

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.

POLÍTICA CONTROL DE ACCESO FÍSICO

VERSIÓN 1.0

CONTROL ISO27001:2013

A.9.1.1

ÍNDICE

1. Objetivo:

Establecer las definiciones que regulen el acceso físico de personas y/o equipos, a las dependencias de la Superintendencia de Educación (SUPEREDUC) y en particular a las áreas seguras que así sean definidas.

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.

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 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 Administración:

3.1.1. Fomentar y efectuar las acciones necesarias para disponer el control de acceso físico general al edificio de SUPEREDUC ubicados en calle Morandé Nº 115, piso N°10, N°11 y N°12; calle Morandé N° 360 Piso Nº5 sala datacenter.

3.1.2. Mantener un inventario actualizado de los equipos TI.

3.2. Jefe/a Departamento de Tecnologías de Información:

3.2.1. Autorizar el traslado de equipos TI desde o hacia áreas seguras.

3.2.2. Asegurar el registro y mantención de una nómina de las personas con permiso de acceso particular a áreas seguras respecto del procesamiento tecnológico de información.

3.2.3. Efectuar o coordinar el traslado de equipos TI desde o hacia áreas seguras.

3.3. Jefaturas Directas:

3.3.1. Autorizar el acceso de personas externas a áreas seguras bajo su dependencia.

3.3.2. Velar por el correcto cumplimiento de 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.*

3.4. Usuarios:

3.4.1. Cumplir con lo establecido en esta política.

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) **Perímetro de seguridad física:** Está constituida por la zona cercada por los elementos físicos que en conjunto permiten diferenciar las instalaciones de la 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.

b) **Áreas seguras:** Son áreas que contienen información sensible o crítica y las instalaciones de procesamiento de información. Dentro de las áreas establecidas como seguras, se encuentran definidas las salas de servidores o data center de la Superintendencia de Educación, cuyo acceso es administrado por personal TIC autorizado y calificado; bodegas y archivos que almacenen activos críticos, cuyo acceso es administrado por cada una de las divisiones y/o áreas al interior de cada una de ellas.

5. Documentos relacionados:

a) Política general de seguridad de la información.

b) Política control de acceso lógico.

c) Inventario de Activos de Información.

d) Instructivos para uso de credencial y control de acceso.

6. Política:

6.1. Acceso a las dependencias:

El perímetro de seguridad física de SUPEREDUC definido en el alcance de esta política, deben ser resguardados mediante elementos de seguridad, tales como: torniquetes de acceso, servicio de guardias en recepción, cámaras de seguridad, y el uso de tarjetas credenciales magnéticas o llaves en las puertas a las áreas de trabajo (oficinas) o espacios físicos (salas de reuniones, archivos y bodegas, etc).

6.2. Visitas:

Las visitas autorizadas a ingresar a las dependencias del edificio de SUPEREDUC (calle Morandé N°115, pisos 10,11 y 12), se le entregará una credencial de visita, según las indicaciones del *"Instructivo para uso de credencial y control de acceso"*.

En cualquier caso, mientras toda persona externa permanezca al interior de las dependencias, deberá portar en un lugar visible la credencial de visita o similar identificación proporcionada por SUPEREDUC.

6.3. Áreas seguras:

Las áreas seguras de SUPEREDUC corresponden a las siguientes:

6.3.1. 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.

6.3.2. 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.

6.3.3. Cualquier otra área que SUPERDUC defina.

6.4. Registro de acceso:

6.4.1. El ingreso a los sectores restringidos por parte de los funcionarios se especifica en el *"instructivo para uso de credencial y control de acceso"*

6.4.2. Las visitas autorizadas a ingresar al perímetro de seguridad con información sensible se especifican en el *"instructivo para uso de credencial y control de acceso"*

6.5. Accesos revocados:

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 egreso de personas*".

Las Jefaturas pertinentes deben asegurar la revisión en forma periódica del estado contractual de los funcionarios autorizados a acceder a las áreas críticas reconocidas, y realizar una actualización de estos cada vez que ocurra.

6.6. Acceso a equipos TI y dispositivos en área seguras:

En las salas de servidores y/o comunicaciones (datacenter) todo el equipamiento que contenga información confidencial, debe estar configurado con el estándar de condiciones de seguridad definidas por SUPEREDUC y aprobadas por el Departamento de Tecnologías de información, deben tener un acceso restringido y monitoreado.

Las Puertas de acceso al datacenter deben considerar características técnicas necesarias para resguardar el equipamiento de TI.

6.7. Identificación y traslado de equipos:

Todo equipo de computación o comunicaciones debe estar rotulado para su identificación, el traslado debe estar autorizado por el Jefe del Departamento de Tecnologías de Información o quien este delegue dicha responsabilidad, debe ser efectuado por el personal de soporte interno y se debe informar al Departamento de Administración (responsable de la actualización del inventario), dicho evento, debe identificar al menos, la persona, el equipo trasladado y los lugares de origen y destino.

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