Gobierno de Chile

Superintendencia de Educación

MPV/CNN/HCJ/PRB/PSY

APRUEBA POLÍTICA DE EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN, EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0724

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 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 de emplazamiento y protección de equipos.

RESUELVO:

1. **APRUÉBASE,** la Política de emplazamiento y protección de equipos, 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.

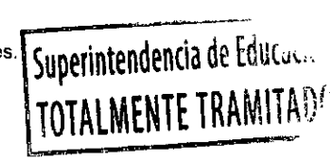
4. **DÉJESE,** expresa constancia que la presente Resolución Exenta no erogará gasto alguno para esta Superintendencia de Educación.

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 Fiscalía.
4. División de Promoción y Resguardo de Derechos Educacionales.
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.



[redacted]

POLÍTICA DE EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS

VERSIÓN 1.0

CONTROL ISO27001:2013
A.11.2.1

ÍNDICE

1. Objetivo:

Definir las directrices y requisitos en el marco del Sistema de Gestión de Seguridad de la Información, con la finalidad lograr niveles adecuados de integridad, confidencialidad y disponibilidad de los activos de información de la Superintendencia de Educación (SUPEREDUC), mediante el correcto emplazamiento de los equipos garantizando su protección y así reducir los riesgos de amenazas, peligros ambientales y las oportunidades de accesos no autorizado.

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.11.02.01 Emplazamiento y protección de equipos.

3. Roles y Responsabilidades:

3.1. Jefe/a División Administración General:

3.1.1. Implementar de manera efectiva esta Política dentro de su área de competencia, debiendo procurar que se asignen los recursos humanos, materiales y financieros para su implementación.

3.2. Jefe/a Departamento de Tecnologías de Información:

3.2.1. Mantener las condiciones ambientales optimas y de seguridad de acceso a los activos de información que estén bajo su responsabilidad.

3.2.2. Coordinar, ejecutar y velar por la correcta gestión de los activos de información al interior de las salas de procesamiento de información (datacenter).

3.2.3. Asegurar el emplazamiento de equipos de monitoreo de las salas de procesamiento de información (datacenter), velando que personas no autorizadas vean el contenido durante su uso.

---

[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.*

3.2.4. Realizar las mantenciones preventivas al equipamiento bajo su administración.

3.3. Jefaturas Directas:

Facilitar un emplazamiento de equipos, evitando que personas no autorizadas vean el contenido durante su uso.

3.4. Funcionario/as:

Tendrán la responsabilidad de cumplir con lo formalizado en esta Política y así garantizar que los activos de información que se encuentren a su cargo estén protegidos contra el mal uso, robo, falta de disponibilidad o destrucción. Además, tendrán la responsabilidad de notificar los incidentes de seguridad y potenciales debilidades de seguridad de la información que pudieran identificarse.

3.5. Encargado/a de Seguridad de la Información:

Monitorear y verificar el correcto cumplimiento de dicha política mediante inspecciones.

4. Definiciones:

a) **UPS:** Sistema de alimentación de energía ininterrumpida.
b) **KVM:** Sistema para acceder a un servidor en forma local o remota.
c) **Datacenter:** Es un centro de procesamiento de datos, una instalación empleada para albergar un sistema de información de componentes asociados, como telecomunicaciones y los sistemas de almacenamientos donde generalmente incluyen fuentes de alimentación redundante o de respaldo.
d) **Fuego Clase C**: Son incendios originados por equipamiento eléctrico energizado como, por ejemplo, computadores, servidores, herramientas eléctricas, microondas, etc.

5. Documentos relacionados:

a) Política general de seguridad de la información.
b) Política control de acceso lógico.
c) Política control de acceso físico.
d) Política perímetros de seguridad física.

6. Política:

6.1. Equipos críticos:

Todos los equipos que contienen información crítica en producción deben ser protegidos de posibles daños, por lo que se determinarán las directrices que permitan minimizar los riesgos de deterioro, daño o uso indebido de los equipos y dispositivos de procesamiento de información, a través del correcto emplazamiento y protección de los mismos, considerando aspectos tales como robos, incendios, agua, polvo, interferencia de suministro eléctrico y vandalismo.

6.2. Consideraciones de emplazamiento del equipamiento:

Para los equipos de procesamiento de información se deben considerar las siguientes medidas:

6.2.1. Las instalaciones de los equipos de procesamiento de información (estaciones de trabajo de usuarios) deben estar ubicadas estratégicamente con tal de que personas no autorizadas o ajenas a los procesos, las vean durante su uso.

6.2.2. Contar con controles de acceso para evitar el ingreso a los sistemas o equipos de forma no autorizada.

6.3. Sala de procesamiento de información:

Para minimizar los riesgos de posibles amenazas físicas y ambientales, se deben considerar las siguientes medidas:

6.3.1. Mantener el equipamiento aislado de muebles, repisas u objetos que puedan representar una amenaza.

6.3.2. Restricción visual al equipamiento, en específico a personas no autorizadas.

6.3.3. Mantener un sistema continuo de monitoreo de las condiciones ambientales que pudieran afectar adversamente la operación de dichas instalaciones.

6.3.4. La alimentación eléctrica debe ser independiente del resto de las oficinas.

6.3.5. Mantener un equipo auxiliar que permita la autonomía suficiente para apagar el equipamiento sin sufrir daños.

6.3.6. Queda prohibido fumar, beber y consumir cualquier tipo de alimentos al interior o en las proximidades de la sala de procesamiento de información.

Aspectos mínimos con los cuales debe contar la sala de procesamiento de información:

6.3.7. Tabiquería resistente al fuego.

6.3.8. Puertas de acceso resistentes al fuego.

6.3.9. Acceso biométrico.

6.3.10. Sensores de movimiento, humo, humedad y líquidos.

6.3.11. Equipos de aire acondicionado independientes.

6.3.12. Cámaras de seguridad al interior y en accesos.

6.3.13. Equipo UPS autónomo.

6.3.14. Extintor fuego Clase C.

6.3.15. Rack para servidores.

6.3.16. Sistema KVM.

6.4. Mantenciones:

Dado que todo el equipo de la sala de procesamiento de información cuenta con un ciclo de vida, **se deben realizar revisiones periódicas para comprobar su estado**. En este caso, se debe establecer un plan de revisión, al menos de forma anual. El estado de los equipos de la organización debe encontrase verificado, se genera un informe que indica que el equipo se encuentra revisado.

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 adquisiciones 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