MIC/FTO/AAM/BBC/DLR

Superintendencia de Educación
TOTALMENTE TRAMITADO

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0724, DE 2017 Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA DE EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0788

SANTIAGO, 30 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 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° 0724, que aprueba versión 1.0 de la política de emplazamiento y protección de equipos 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 de la política de emplazamiento y protección de equipos.

RESUELVO:

1. **DÉJASE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0724, de 2017 de la Superintendencia de Educación.

2. **APRUÉBASE**, la versión N°2.0 de la política de emplazamiento y protección de equipos en la Superintendencia de Educación, cuyo texto es el siguiente:

Política de emplazamiento y protección de equipos

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

Definir las directrices y requisitos, en el marco del Sistema de Seguridad de la Información, para el correcto emplazamiento y protección de los equipos de la Superintendencia de Educación (SUPEREDUC) con el objetivo de 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 por el Departamento de Tecnología y Procesos, ubicadas en los edificios de SUPEREDUC localizados en calle Morandé N° 115, piso N°10, piso N°11 y piso N°12 y calle Morandé N° 360 Piso N° 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.

Es aplicable a todos los usuarios ya sean funcionarios/as en calidad jurídica planta, contrata, reemplazos y suplencia, estudiantes en práctica, el personal a honorarios y terceros que trabajen para SUPEREDUC 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 Ubicación y protección del equipamiento.

3. Referencias normativas

- Política general de seguridad de la información vigente.
- Política control de acceso lógico vigente.
- Política control de acceso físico vigente.
- Política perímetros de seguridad física vigente.
- Procedimiento de administración de comunicaciones, emplazamiento y mantención de equipo vigentes.

4. Definiciones

Concepto	Descripción
UPS	Sistema de alimentación de energía ininterrumpida
KVM	Sistema para acceder a un servidor en forma local o remota
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 de respaldo
Fuego Clase C	Son incendios originados por equipamiento eléctrico energizado como, por ejemplo, computadores, servidores, herramientas eléctricas, microondas, etc.

5. Roles y Responsabilidades

Rol	Responsabilidades
División Administración General	a) 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.
Departamento de Tecnologías y Procesos	a) Mantener las condiciones ambientales óptimas y de seguridad de acceso a los activos de información que estén bajo su responsabilidad b) Coordinar, ejecutar y velar por la correcta gestión de los activos de información al interior de las salas de procesamiento de información (datacenter) c) 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. d) Realizar las mantenciones preventivas y correctivas al equipamiento bajo su administración.
Jefaturas Directas	a) Facilitar un emplazamiento de equipos, evitando que personas no autorizadas ven el contenido durante su uso. b) Resguardar que el personal a cargo cumpla con las directrices establecidas en esta política
Encargado/a de Seguridad de la Información y Ciberseguridad	a) Velar por la difusión y cumplimiento de esta política. b) Velar por la correcta aplicación de esta política. c) Revisar y actualizar la política, con la finalidad de asegurar su continua idoneidad, eficiencia y efectividad.

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

Usuarios	a) Cumplir con lo formalizado en esta Política y asi garantizar que los activos de información que se encuentren a su cargo estén protegidos contra el mal uso, robo, falta de disponibilidad o destrucción b) Notificar los incidentes de seguridad y potenciales debilidades de seguridad de la información que pudieran identificarse

6. Directrices

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, el Departamento de Tecnología y Procesos debe 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, de acuerdo al *"Procedimiento de administración de comunicaciones, emplazamiento y mantención de equipo"* vigente.

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 ésta 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

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.
- Encargada de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.