MIC/FTO/AAM/PSC/DLR

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0824, DE 2017 Y APRUEBA VERSIÓN N°4 DE LA POLÍTICA DE USO DE MEDIOS REMOVIBLES Y DISPOSITIVOS MÓVILES, EN EL MARCO DE LA SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0744

Santiago, 23 DIC 2019

Superintendencia de Educación
TOTALMENTE TRAMITADO

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 01 de diciembre de 2017, se dicta Resolución Exenta N° 0824, que aprueba política de uso de medios removibles y dispositivos móviles versión N° 3, 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, de esta Servicio, 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.

6. Que, debido a una serie de cambios institucionales y a la revisión efectuada por el Encargado de Seguridad de la Información y Ciberseguridad se ha estimado procedente reestructurar, ajustar y actualizar el contenido de la Política de uso de medios removibles y dispositivos móviles versión N°3, aprobada mediante Resolución Exenta N°0824, de fecha 01 de diciembre de 2017, de esta Superintendencia.

RESUELVO:

1. **DÉJESE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0824, de 2017 de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°4 de la Política de uso de medios removibles y dispositivos móviles de la Superintendencia de Educación, cuyo texto es el siguiente:

Política de uso de medios removibles y dispositivos móviles

Tabla de Contenidos

Superintendencia de Educación / Gobierno de Chile	**Política de uso de medios removibles y dispositivos móviles**			
	Fecha revisión del documento	18-12- 2019	Páginas	3 de 11
			Versión	4
	Nivel de Confidencialidad	*Interno*	Código	POL-DGI-05
	Superintendencia de Educación			

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 objetivo de la presente política es mantener un estándar de seguridad coherente con las políticas implementadas en la Superintendencia de Educación (SUPEREDUC) con el fin de establecer las normas que regulen el uso de los dispositivos móviles y medios removibles, dentro y fuera de la institución, permitiendo minimizar los riesgos asociados a estos y con el fin de evitar incidentes de seguridad con los datos contenidos en estos.

Los dispositivos móviles y medio removibles permiten facilitar las actividades relacionadas con la institución, no obstante, el uso de dichos dispositivos también implica algunos riesgos, que deben ser analizados y gestionados. Principalmente tener el cuidado de asegurar que la información institucional no se vea comprometida, evitando así la divulgación, modificación o la destrucción no autorizada de la información almacenada y/o procesada en ellos.

2. Alcance

Esta política se aplica a todas las áreas de SUPEREDUC y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas[1] y los procesos definidos en la Matriz de Riesgo Institucional. Norma la utilización de medios removibles (conectados por puerto USB, Bluetooth u otro medio) y dispositivos móviles que son entregados por la Institución a los Usuarios[2]; funcionarios, colaboradores, practicantes o personal externo que preste servicios permanentes o temporales, y/o aquellos utilizados dentro de las dependencias de la SUPEREDUC, específicamente:

- Pendrive.
- Discos duros portátiles.
- Dispositivos de banda ancha móvil.
- Teléfono móvil.
- Tablets.
- Cámara fotográfica.
- Grabadora de audio.
- Cámara de video.
- Grabador portátil CD/DVD/BlueRay,

[1] Publicado en el sitio web www.dipres.gob.cl Inicio / Evaluación y Control de Gestión / Definiciones estratégicas/ Superintendencia de Educación.
[2] 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.

Es aplicable a todos los usuarios de SUPEREDUC, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presten servicios a la SUPEREDUC.

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

- A.06.02.01 Política de dispositivos móviles.
- A.08.03.01 Administración de medios extraíbles.

3. Referencias normativas

- El marco legal para el Sistema de Seguridad de la información se señala en el documento "Listado de normativa vigente aplicable a la Superintendencia de Educación" publicado en la Intranet.
- Política General de Seguridad de la Información de la Superintendencia de Educación vigente.
- Política de Devolución de Activos Vigente.
- Procedimiento de creación, modificación, eliminación de cuentas e información y egreso de personas vigente.
- Norma Chilena NCh-ISO 27001/2013 tecnología de la información-técnicas de seguridad-sistemas de gestión de la seguridad de la información.
- Decreto Supremo N°83 del Ministerio Secretaría General de la Republica, que aprueba norma técnica para los órganos de la administración del estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Procedimiento de Gestión de Incidentes de Seguridad de la Información vigente.
- Política de eliminación o reutilización segura de equipos de la Superintendencia de Educación vigente.

4. Definiciones:

Concepto	Descripción
Medios removibles	Soportes o dispositivos de almacenamiento, independientes del computador y que pueden ser transportados libremente, diseñados para ser extraídos de la computadora sin tener que apagarla. Ejemplos: discos ópticos, tarjetas de memoria, memorias USB, discos duros externos, todo lo que permita transportar información.
Dispositivos móviles	Aparato de tamaño pequeño, fácilmente transportable, con algunas capacidades de procesamiento de datos, con conexión permanente o intermitente a internet y de memoria limitada que han sido diseñados para una función específica. Ej.: teléfonos celulares, Smartphone, tabletas, notebook, etc.
OneDrive	Herramienta para el almacenamiento de archivos e información, One Drive es la nube institucional que permite guardar archivos o documentos en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet con la cuenta de usuario que se utiliza para el acceso al sistema informático de la Superintendencia de Educación
Antivirus	Programa informático cuyo objetivo es detectar y eliminar virus que pueden contener los dispositivos móviles o removibles y computadores. Estos virus pueden perjudicar el correcto funcionamiento del sistema informático de la SUPEREDUC y afectar la disponibilidad de los recursos informáticos e información de la institución.

5. Roles y Responsabilidades:

Rol	Responsabilidades
Jefaturas de la SUPEREDUC	a) Las jefaturas de las Divisiones, Intendencia, Direcciones Regionales, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política.
Departamento de Tecnologías y Procesos	a) Definir los dispositivos removibles a utilizar en la SUPEREDUC, evaluar y autorizar su uso. b) Coordinar y gestionar la entrega y la baja de los medios de almacenamiento removibles y dispositivos móviles. c) Punto de contacto para orientar, asesorar, actualizar y restaurar los problemas que puedan presentar este tipo de equipamiento. d) Recibe y gestiona solicitudes de robo, hurto o extravío de este tipo de dispositivos. e) Proponer e implementar configuraciones de seguridad para los medios removibles. f) Aplicar las medidas de protección en la utilización de estos.
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 medios de almacenamiento removibles y dispositivos móviles, evaluar circunstancias particulares respecto al uso de estos equipamientos 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 este tipo de dispositivos. d) Actualizar la política, con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.
Usuarios	a) Personas, funcionarios, colaboradores, practicantes o personal externo que preste servicio permanente o temporal que, con debida autorización, usan medios de almacenamiento removibles o dispositivos móviles, por lo que mantienen la responsabilidad de hacer cumplir lo establecido en esta política. b) Utilizar los medios de respaldos y dispositivos móviles asignados por la SUPEREDUC, de acuerdo a lo establecido en esta política. c) Encargado de reportar cualquier evento, robo o hurto sobre este tipo de equipamiento, para que el Departamento de Tecnología y Procesos tome las medidas al respecto.

6. Directrices

6.1 Consideraciones generales

a) Los medios removibles no son alternativa de respaldo de información de la SUPEREDUC, siendo responsabilidad del usuario almacenar y mantener la información en la nube[3] institucional asignada por el Departamento de Tecnologías y Procesos. Está restringido el uso de dispositivos de almacenamiento removibles conectados a puertos USB tales como discos externos, celulares, cámaras, etc. Exceptuando aquellos dispositivos necesarios para la operación como mouse, teclados, impresoras que únicamente poseen puerto USB como mecanismo de conexión a la red. Se incluyen en esta política equipos que, mediante una solicitud a la mesa de ayuda, que deriva al Encargado/a de Seguridad de la Información y Ciberseguridad para que autorice su acceso.

[3] Almacenamiento online (One Drive de Office 365) que se compenetra perfectamente con las herramientas que usa a diario para crear, comunicarse y colaborar desde su equipo PC o Mac o su dispositivo iOS®, Android™ o Windows.

b) Los usuarios deben ser cuidadosos al utilizar dispositivos móviles en lugares públicos, salas de reuniones y otras áreas sin protección. Como también su manipulación, almacenamiento de estos en salidas o viajes que el funcionario deba participar en el cumplimiento de sus funciones.

c) Se debe contar con protección para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos. Protegiendo el acceso con claves, tokens, huella digital o el mecanismo que permita el dispositivo.

d) Debe formatearse por los funcionarios de mesa de ayuda, el medio removible y dispositivo móvil, cuando la información pierda vigencia de acuerdo con la "*Política de eliminación o reutilización segura de equipos*" vigente en la SUPEREDUC.

e) Los usuarios deben dar un buen uso a los medios removibles y dispositivos móviles asignados para el cumplimiento de sus funciones, en caso de que éstos presenten cualquier deterioro o evento de seguridad, debe informarlo oportunamente al Departamento de Tecnologías y Procesos, específicamente a la Mesa de Servicio. El cual aplicará el "*Procedimiento de Gestión de Incidentes de Seguridad de la Información*", vigente

f) En caso de pérdida o robo del equipamiento asignado por la SUPEREDUC, el usuario afectado, debe informar a su Jefatura directa, al Departamento de Tecnologías y Procesos específicamente al correo mesadeservicio@supereduc.cl, al anexo 55555 y, posteriormente Carabineros de Chile dejando en la constancia la información relativa al equipo (marca, característica, número de serie).

6.2 Marco de utilización de dispositivos móviles y medios removibles de almacenamiento.

a) Los dispositivos móviles y medios removibles son asignados a los funcionarios para apoyar la relación de su trabajo y deben ser utilizados solamente para estos fines.

b) Los usuarios que hagan uso de su móvil personal para apoyar su trabajo, debe tomar los resguardos que estén a su alcance, en relación a tener el cuidado de asegurar que la información institucional no se vea comprometida, evitando así la divulgación, modificación o la destrucción no autorizada de la información almacenada en el móvil.

c) El uso de un medio removible debe ser autorizado y justificado por la Jefatura directa del usuario, quien debe solicitarlo por email a mesadeservicio@supereduc.cl. Una vez que el Departamento de Tecnologías y Procesos reciba este requerimiento, solicitará validación al Encargado/a de Seguridad de la Información y Ciberseguridad y luego habilitará el acceso al medio removible.

d) La asignación de un medio removible debe ser autorizado, justificado y solicitado por la Jefatura directa del usuario al email mesadeservicio@supereduc.cl, el Departamento de Tecnologías y Procesos evaluará que se cumpla con el de estándar asignado para este tipo de medio, el que, en caso de contar con disponibilidad, será asignado al usuario, previa firma de recepción conforme, y registrado en el sistema que posee la mesa de servicio El Departamento de Tecnologías y Procesos informará la asignación del medio removible al Encargado/a de Seguridad de la Información y Ciberseguridad.

e) Es responsabilidad de cada usuario el buen uso y traslado de los dispositivos que tiene a su cargo, los cuales deben ser entregados por el Departamento de Tecnologías y Procesos, según sea el procedimiento que el área determine para ello.

f) Es responsabilidad de cada jefatura que solicita uso de medio removible y asignación de medio removible resguardar que el funcionario a su cargo realice un buen uso y cuidado en el traslado de los dispositivos a cargo.

g) Los dispositivos móviles y medios de almacenamiento removibles no se deben exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).

h) Cualquier falla o deterioro de los componentes o dispositivos móviles asignados, debe ser informada al Departamento de Tecnologías y Procesos, específicamente al correo mesadeservicio@supereduc.cl o al anexo 55555.

6.3 Configuración de los medios removibles y dispositivos móviles

a) La incorporación, deshabilitación o modificación de cualquier dispositivo de hardware o software, debe efectuarse sólo por el personal del Departamento de Tecnologías y Procesos. No está permitido que el usuario a cargo realice la instalación de aplicaciones, programas y/o software que no hayan sido previamente aprobados por el Departamento de Tecnologías y Procesos.

b) Todo dispositivo móvil debe contar con los mecanismos de control de acceso, y configurado el software antivirus o cualquier otro componente de seguridad, lo que será responsabilidad del Departamento de Tecnologías y Procesos.

c) Cuando un dispositivo móvil o de almacenamiento sea devuelto a la Superintendencia o dado de baja, el usuario deberá entregar el equipo con sus respectivas contraseñas, para que el personal del Departamento de Tecnologías y Procesos genere una eliminación de la información contenida en este.

d) Todo cambio u alteración a la configuración del dispositivo móvil, correctivo o no, debe ser solicitado y aplicado por el Departamento de Tecnologías y Procesos.

6.4 Traslado de medios removibles y equipos móviles.

a) Si el usuario viaja en bus o avión, los dispositivos móviles y medios removibles deben ir como equipaje de mano, siempre bajo la supervisión del usuario, y no en el compartimiento de equipaje. Además, los dispositivos se deben reguardar frente a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.)

b) Es responsabilidad del usuario la seguridad, almacenamiento y buen uso de los medios y dispositivos que utilice fuera de las instalaciones de la Superintendencia.

6.5 Reutilización de equipos móviles y medios removibles:

a) Toda reasignación de dispositivos móviles debe ser autorizado, ejecutado y debidamente registrado por el personal del Departamento de Tecnologías y Procesos. Dicho personal, además es responsable de resguardar, que el dispositivo ya no contenga información contenida y generada por el usuario que solicitó darlo de baja o lo devolvió.

b) El Departamento de Tecnologías y Procesos es responsable de velar por el correcto manejo de la información de todos los dispositivos móviles que están en condiciones de desecho o reutilización, según lo indica el *"Procedimiento de creación, modificación, eliminación de cuentas e información y egreso de personas"* vigente a la fecha.

6.6 Respecto al uso del teléfono móvil

a) Los usuarios deben evitar la difusión de información confidencial o privada por vía telefónica cuando se está en lugares públicos o fuera de las dependencias de la Superintendencia de Educación. Si se hace, se debe procurar tratar los temas en forma general y sin mencionar información sensible o confidencial.

b) Los usuarios deben procurar no almacenar información confidencial en los teléfonos móviles institucionales. Asimismo, y entendiendo que, dado el uso del teléfono móvil institucional, existe la posibilidad de que terceros accedan a la información contenida en él, se sugiere la utilización de claves

de acceso al equipo con un número limitado de intentos, de manera de minimizar el riesgo de acceso no autorizado.

c) Los usuarios no deben participar de juegos, concursos, cadenas u otros similares, utilizando el teléfono móvil otorgado por la SUPEREDUC.

d) Es responsabilidad del usuario dar buen uso y cuidado al teléfono móvil asignado.

e) Los usuarios no deben exponer el teléfono móvil a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.)

f) El Departamento de Tecnologías y Procesos deberán resguardar que los equipos proporcionados por la SUPEREDUC tengan, por defecto, bloqueados los servicios de mensajería de texto y roaming internacional.

g) Cuando un equipo móvil es utilizado en lugares públicos o privados, y es conectado a una red no administrada por la Superintendencia, el usuario de dicho equipo es responsable de la seguridad física y lógica del mismo y de la información que comparta con terceros a través de dicha red.

h) Terceras personas no están autorizadas a utilizar el dispositivo móvil que la SUPEREDUC asigne a un usuario

i) El usuario debe seguir las indicaciones de los fabricantes tanto en la utilización, actualización como en el cuidado del equipo móvil asignado para el cumplimiento de sus funciones.

6.7 Respecto al uso de dispositivos de almacenamiento removibles.

a) Los usuarios tendrán prohibición de utilizar dispositivos de almacenamiento personales y será de su responsabilidad mantener respaldar la información en la nube[4] institucional asignada por el Departamento de Tecnologías y Procesos.

b) No está permitido almacenar información institucional en los dispositivos de almacenamiento personales, sólo debe usarse para facilitar el porte de información funcional. (ej. presentaciones, documentos de trabajo, etc.)

c) En general la SUPEREDUC no proveerá de pendrives o discos duros externos o cualquier medio de almacenamiento externo, por el riesgo que estos representan a la seguridad de la información.

d) Los discos duros externos ya existentes en las Unidades, deben ser gradualmente eliminados y su información traspasada a la red institucional provista para ello.

e) Para los dispositivos que ya estén en la institución y que han sido asignado a usuarios no se debe exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.)

f) Todo medio de almacenamiento removible que sea utilizado fuera de la plataforma tecnológica de la institución, debe ser revisado por posible presencia de virus, a través del escaneo de éste por el antivirus instalado por el Departamento de Tecnologías y Procesos en su equipo.

g) El responsable del medio de almacenamiento removible, deberá velar por el buen uso de la información almacenada en el mismo, manteniendo su adecuado control y distribución limitada. Deberá usar mecanismos de protección, como el uso de contraseñas y/ encriptación de archivos.

h) El responsable del medio de almacenamiento removible, deberá adoptar las medidas que se encuentren a su alcance para asegurarse que los archivos contenidos en él se encuentren libres de virus, software y/o código malicioso, que puedan poner en riesgo la confidencialidad, integridad y

[4] Almacenamiento online (One Drive de Office 365) que se compenetra perfectamente con las herramientas que usa a diario para crear, comunicarse y colaborar desde su equipo PC o Mac o su dispositivo iOS®, Android™ o Windows.

disponibilidad de la información, como también exponer a los equipos informáticos de la SUPEREDUC a eventos de vulnerabilidad.

i) Los usuarios deberán eliminar los activos de información de carácter restringida, y contenida en un medio de almacenamiento removible, regulada de acuerdo al *Procedimiento de clasificación de información y análisis de riesgo* vigente en la SUPEREDUC.

j) El usuario debe cuidar el equipamiento y guardarlo en lugares seguros cuando no lo esté utilizando, preferentemente muebles con llave.

6.8 Uso de cámaras fotográficas, de video y grabadoras

a) Para los dispositivos que ya estén en la institución y que han sido asignado a usuarios, no se deben exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).

b) El usuario debe cuidar el equipamiento y guardarlo en lugares seguros cuando no lo esté utilizando, preferentemente muebles con llave.

c) El usuario debe seguir las indicaciones de los fabricantes tanto en la utilización como en el cuidado del equipo.

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 del cumplimiento de la Política

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 del procedimiento

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
1.0	Agosto 2015	Versión inicial	Versión inicial
2.0	Octubre 2016	Actualización Política	Actualización Política
3.0	Noviembre 2017	Actualización Política	- Punto 2.0, se incorpora al alcance las definiciones de Ficha A1 y los dispositivos de banda ancha móvil. - Punto 5, se incorpora Política de devolución de activos, se elimina; Procedimientos internos o estándares en construcción. - Puntos 6.1, 6.2, 6.3, se modifica email de contacto y anexo de mesa de servicios TI. - Punto 6.6, letra d: se elimina la frase en ningún caso se debe guardar información confidencial ni sacar fuera de las instalaciones de la SUPEREDUC. - Punto 9, se incorpora la evaluación y revisión anual de la política. - Punto 11, se modifica formato de tabla.
4.0	Diciembre 2019	Actualización Política	Todas las Paginas.

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. **DÉJASE,** expresa constancia que la presente Resolución Exenta no irroga 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.

[redacted]

6. **PUBLÍQUESE,** una vez totalmente tramitada la presente Resolución Exenta, en la Intranet institucional y el sitio web www.supereduc.cl.

ANÓTESE, COMUNÍQUESE Y ARCHÍVASE.

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