

JAL/FTO/ AAM/PBC/DLR



Superintendencia de Educación
TOTALMENTE TRAMITADO

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0825 DE 2017 Y APRUEBA POLÍTICA DE USO DE COMPUTADORES VERSIÓN N°4, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N°

0796

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 01 de diciembre de 2019, se dicta Resolución Exenta N° 0825, que aprueba versión 1.0 de la política de uso de computadores 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:

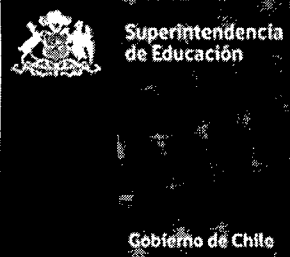
1. **DÉJASE**, sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0825, de 2017 de la Superintendencia de Educación.

	Política uso de computadores			
	Fecha revisión del documento	27 – 12- 2019	Páginas	1 de 8
			Versión	4
	Nivel de Confidencialidad	<i>Público</i>	Código	POL-DGI-16
Superintendencia de Educación				

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

Política uso de computadores	
Tabla de Contenidos	
1. Objetivo	2
2. Alcance.....	2
3. Referencias normativas	2
4. Definiciones.....	2
5. Roles y Responsabilidades.....	3
6. Directrices	3
7. Evaluación y Difusión.....	6
8. Revisión	6
9. Aceptación	6
10. Sanciones	7
11. Excepciones.....	7
12. Revisiones de la política	7

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 Irrazabal Cerpa Comité Directivo Seguridad de la Información

	Política uso de computadores			
	Fecha revisión del documento	27 – 12- 2019	Páginas	2 de 8
			Versión	4
	Nivel de Confidencialidad	<i>Público</i>	Código	POL-DGI-16
Superintendencia de Educación				

1. Objetivo

Los equipos computacionales de propiedad de la Superintendencia de Educación (SUPEREDUC), son asignados a cada uno de los usuarios para apoyar la realización de su trabajo dentro de la institución, debiendo ser utilizados solamente para esos fines, basados en la asignación de acuerdo a los perfiles de usuario definido por sus Jefaturas.

El objetivo de la presente política es mantener un estándar de seguridad coherente con las Políticas de Seguridad implementadas en la SUPEREDUC, con el fin de evitar incidentes de seguridad con los datos contenidos en las estaciones de trabajo y con la información y sistemas a los cuales se accede a través de ellos.

2. Alcance

Esta política se aplica a todas las áreas de la SUPEREDUC y a los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas.

Esta política aplica a todos los computadores de escritorio, notebooks, tablets que son entregados por la Institución a cada uno de los Usuarios: ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes a la SUPEREDUC, para el cumplimiento de sus labores, y otros trabajadores, incluyendo las empresas que presten servicios.

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


- A.08.01.03 Se deberían identificar, documentar e implementar las reglas para el uso aceptable de la información de los activos asociados a la información y a las instalaciones de procesamiento de información.
- A.11.02.05 Retiro de activos.
- A.11.02.06 Seguridad de los equipos y los activos fuera de las dependencias.
- A.11.02.08 Equipos de usuario no supervisados.

3. Referencias normativas

- Política general de seguridad de la información de la Superintendencia de Educación vigente.
- Política perímetros de seguridad física 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
- Procedimiento de respaldos usuarios y servidores.

4. Definiciones

Concepto	Descripción
Estaciones de trabajo y otros equipos	<p>Conjunto de elementos tecnológicos de hardware y software que lo componen.</p> <ul style="list-style-type: none"> - A nivel de Hardware: incluyen pantalla, teclado, mouse, parlantes, unidad central (CPU), disquetera, unidad de CD (externa o interna), impresoras, proyector, tv, scanner, teléfonos (IP y móvil), fax, Banda ancha móvil, notebooks, docking, candados y cables. - A nivel de Software: incluyen todos los programas, sistemas de información o aplicaciones, sistemas operativos y rutinas de comunicación o de uso general.

	Política uso de computadores			
	Fecha revisión del documento	27 – 12- 2019	Páginas	3 de 8
			Versión	4
	Nivel de Confidencialidad	<i>Público</i>	Código	POL-DGI-16
Superintendencia de Educación				

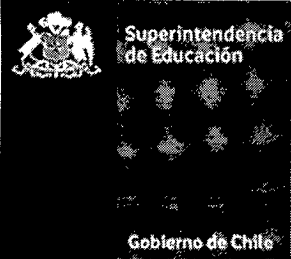
5. Roles y Responsabilidades

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) Velar por el cumplimiento de la política, estándares y procedimientos establecidos para la gestión del hardware en la SUPEREDUC. b) Coordinar y gestionar la entrega y la baja de los medios hardware dentro de la Superintendencia de Educación, manteniendo un registro digital de estos. c) Punto de contacto para orientar, asesorar, actualizar y restaurar los problemas que puedan presentar los computadores de la SUPEREDUC. d) Proponer e implementar configuraciones de seguridad para los computadores de la SUPEREDUC. e) Mantiene un catastro de Hardware de la SUPEREDUC. f) Realizar el mantenimiento de los equipos informáticos, hardware y software de SUPEREDUC.
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 a la entrega de computadores y las medidas de seguridad que se disponen para este equipamiento. c) Velar por la correcta aplicación de la política y apoyar a las unidades técnicas responsable de la administración y gestión de este tipo de equipamiento. 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 a la Superintendencia de Educación que, con debida autorización, usan computadores y por ende mantienen la responsabilidad de hacer cumplir lo establecido en esta política. b) Administran la información contenida en su computador de la SUPEREDUC, cumpliendo con las definiciones establecidas en esta política. c) Utilizar de manera permanente y proteger los medios de seguridad física, provistos por el Departamento de Tecnologías y Procesos para el uso de los dispositivos móviles (ejemplo: candados de seguridad). d) Reportar cualquier falla o deterioro del equipo o componente, a través de los canales formalmente establecidos.

6. Directrices

6.1. Gestión del equipamiento tecnológico

- Todo nuevo requerimiento de Hardware debe ser revisado y autorizado técnicamente antes y después de su compra por el Departamento de Tecnologías y Procesos, para garantizar que cumplan con los estándares definidos y su compatibilidad con los componentes y sistemas de la SUPEREDUC.
- El Departamento de Tecnologías y Procesos debe mantener un catastro actualizado del equipamiento tecnológico de la SUPEREDUC
- Debe existir un procedimiento de asignación de equipamiento, que regule la entrega y retiro de computadores de la SUPEREDUC a los usuarios.
- El equipamiento sólo será asignado al usuario, quedando descartada la asignación a una unidad administrativa.
- La configuración del computador de la SUPEREDUC dependerá del perfil del usuario y de las funciones que le sean asignadas en virtud de su cargo y lo que establezca su jefatura directa.
- El respaldo de los archivos almacenados en el disco local de las estaciones de trabajo, debe ser solicitado al Departamento de Tecnologías y Procesos de acuerdo a la Política de Respaldo vigente en la SUPEREDUC.

	Política uso de computadores			
	Fecha revisión del documento	27 – 12- 2019	Páginas	4 de 8
			Versión	4
	Nivel de Confidencialidad	<i>Público</i>	Código	POL-DGI-16
Superintendencia de Educación				

6.2. Responsabilidades del usuario


- a) Los equipos, dispositivos o periféricos, son de uso exclusivo para el desarrollo de las funciones de los usuarios de la SUPEREDUC.
- b) El usuario de la SUPEREDUC no podrá alterar o modificar el hardware/software que se encuentra a su disposición. Debe a su vez cuidar física y lógicamente los recursos informáticos; pensando que estos son bienes y servicios públicos.
- a) El usuario es responsable de la información contenida en el o los equipos a su cargo, siendo obligación respaldar datos sensibles de la institución (asegurando la confidencialidad, integridad y disponibilidad) en la nube¹ asignada por el Departamento de Tecnologías y Procesos.
- b) El usuario es responsable de administrar la capacidad del disco duro de su equipo, considerando que archivos de audio, video o imagen podrían afectar el rendimiento y/o capacidad de almacenaje del mismo.
- c) Los archivos almacenados en el disco local de las estaciones de trabajo son de responsabilidad directa del usuario, quien es además responsable de eliminar periódicamente aquellos archivos que no utiliza.
- d) Cualquier requerimiento de reparación o corrección del computador de la SUPEREDUC, debe ser solicitada a mesadeservicio@supereduc.cl, o al anexo 55555, El usuario debe asegurarse de que cada vez que se ausente de su estación de trabajo, el equipo a su cargo cuente con la protección adecuada. Para ello debe:
 - i. Finalizar las sesiones activas cuando terminen, asegurándose del correcto funcionamiento del protector de pantalla protegido con contraseña. En caso de presentar fallas, éstas deben ser reportadas inmediatamente por email a mesadeservicio@supereduc.cl, o al anexo 55555, del Departamento de Tecnologías y Procesos de Información
 - ii. Cerrar sesión en las aplicaciones, sistemas y/o servicios de redes cuando ya no se utilicen y/o necesiten.
 - iii. Se debe usar responsablemente (no divulgar, no exponer, no compartir) las contraseñas de acceso al equipo, asegurándose de cambiarla periódicamente y no utilizar la contraseña inicial entregada por el Departamento de Tecnologías y Procesos.
- e) Los equipos personales de los usuarios, no tienen soporte o mantenimiento a cargo de la SUPEREDUC. Los usuarios podrán hacer uso de computadores personales, tablets y/o Smartphone de su propiedad para acceder a los servicios de correo electrónico, agenda, contactos, documentos, etc., protegiéndolos con contraseñas de acceso a la red corporativa. La Superintendencia no se hace responsable por fallas, extravíos o robo de estos equipos.
- f) En caso de pérdida o robo del equipamiento, el usuario afectado, debe informar al Departamento de Tecnologías y Procesos de Información, mesadeservicio@supereduc.cl, o al anexo 55555, y a Carabineros dejando en la constancia la información relativa al equipo (marca, característica, número de serie).

6.2.1. Los usuarios y sus prohibiciones

- a) Trasladar los equipos y/o periféricos fuera de las dependencias de la SUPEREDUC sin la autorización por escrito² de su Jefatura Directa. (Se excluyen a los usuarios que por las características de su función deben utilizar equipos portátiles para realizar su trabajo fuera de las dependencias de la SUPEREDUC, Ej. Fiscalizadores)

¹ 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.

² El usuario debe enviar un email solicitando autorización a su Jefatura directa, quién debe autorizarlo respondiendo por esta vía.

	Política uso de computadores			
	Fecha revisión del documento	27 – 12- 2019	Páginas	5 de 8
			Versión	4
	Nivel de Confidencialidad	<i>Público</i>	Código	POL-DGI-16
Superintendencia de Educación				

- b) Deshabilitar los mecanismos de control de acceso, el software antivirus o cualquier otro componente de seguridad física o lógica de un computador personal.
- c) Abrir los equipos o periféricos; así como extraer o cambiar componentes. En caso de desperfecto de los equipos o periféricos, el usuario debe comunicarlo al email mesadeservicio@supereduc.cl, o al anexo 55555.
- d) Dañar los equipos, partes, periféricos, eliminar o hacer ilegible la información perteneciente a la SUPEREDUC.
- e) Codificar carpetas, archivos de los equipos, que restrinjan el uso de la información provocando su indisponibilidad.

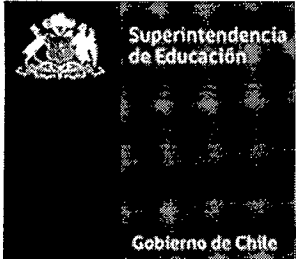
6.3. Ubicación de los equipos

- a) Los lugares de trabajo de los usuarios con equipos fijos o portátiles deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas no autorizadas. De esta forma se protege tanto el equipamiento tecnológico como los documentos que pudiera estar utilizando el usuario.
- b) Es responsabilidad de cada usuario el buen uso del equipo que tiene a su cargo, el cual debe ser entregado por el Departamento de Tecnologías y Procesos, previa firma de recepción conforme, según sea el procedimiento que el área determine para ello.
- c) No se debe exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, campos electromagnéticos fuertes, etc.).

6.4. Uso de Equipos portátiles

En el caso de uso de los equipos portátiles fuera de las dependencias de la SUPEREDUC, el usuario debe tener presente:

- a) La seguridad física del equipo móvil portátil por de la SUPEREDUC, es de responsabilidad del usuario al que se le asigna y será quien debe evitar los daños o hurto, debiendo estar siempre alerta ante posibles riesgos.
- b) El usuario debe mantener el equipo portátil, bajo su cuidado, como si fuera su billetera, teléfono o bolso personal. Debe tener especial cuidado en lugares públicos. Tenga presente que este tipo de equipamiento puede ser robado en una fracción de segundos, ya sea en la vía pública, recintos privados o en el mismo vehículo que usa para trasladarse.
- c) Si por algún motivo debe dejar temporalmente su equipo portátil en alguna oficina, sala de reuniones, habitaciones de hoteles, aunque sea por un corto período, utilice cables de seguridad para equipos portátiles o algún dispositivo con similares características para amarrar o trabar en algún sitio que lo permita de forma segura.
- d) Se debe asegurar el equipo portátil cada vez que deje de utilizarlo, en lo posible guárdelo en un lugar seguro. Nunca deje el equipo portátil a la vista o en un vehículo para evitar hurtos.
- e) Preocuparse de transportar el equipo portátil en el bolso que le ha asignado de la SUPEREDUC para reducir accidentes de transporte, evitando golpear el equipo.
- f) Mantenga la información relativa a la marca, modelo y número de serie del equipo asignado por la SUPEREDUC. Si el equipo es robado, o extraviado, notifique inmediatamente al Departamento de Tecnologías y Procesos de Información mesadeservicio@supereduc.cl, o al anexo 55555, y a Carabineros dejando en la constancia la información relativa al equipo (marca, característica, número de serie).

	Política uso de computadores			
	Fecha revisión del documento	27 – 12- 2019	Páginas	6 de 8
			Versión	4
	Nivel de Confidencialidad	<i>Público</i>	Código	POL-DGI-16
Superintendencia de Educación				

6.5. Configuración de los equipos.

- a) Toda estación de trabajo conectada a la red de SUPEREDUC debe usar la configuración definida por el Departamento de Tecnologías y Procesos, de acuerdo al estándar correspondiente a las funciones del usuario al cual está asignada.
- b) Cualquier requerimiento de cambio de configuración debe ser previamente autorizado y justificado por el superior respectivo y efectuado por el Departamento de Tecnologías y Procesos.

6.6. Reutilización de Equipos

- a) Toda reasignación de equipos debe ser autorizado, ejecutado y debidamente registrado por el Departamento de Tecnologías y Procesos.
- b) Se debe establecer la debida eliminacion de información sensible y software de los equipos que serán reutilizados por usuarios de la SUPEREDUC.
- c) El Departamento de Tecnologías y Procesos es responsable de velar por el correcto manejo de la información de todos los equipos 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.

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.

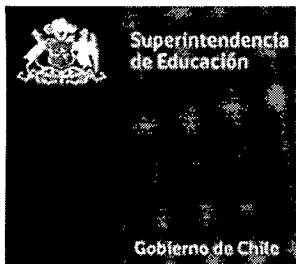
8. Revisión

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.

	Política uso de computadores			
	Fecha revisión del documento	27 – 12- 2019	Páginas	7 de 8
			Versión	4
	Nivel de Confidencialidad	<i>Público</i>	Código	POL-DGI-16
Superintendencia de Educación				

10. Sanciones

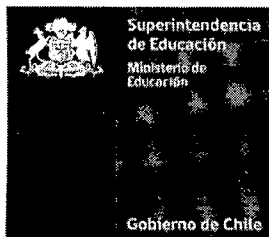
El incumplimiento o violación a esta Política, de las Políticas específicas del Sistema, Procedimientos u otros documentos que se deriven de éstos, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios/as de la 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	Agosto 2015	Versión inicial	Versión inicial
2.0	Octubre 2016	Actualización Política	Actualización Política
3.0	Noviembre 2017	Revisión Política	- Punto 2.0, se incorpora al alcance las definiciones de Ficha A1 y los controles de la norma Nch:27:001 desarrollados en esta política. - Puntos 6.2, 6.2.1, 6.4, se modifica email de contacto y anexo de mesa de servicios TI - Punto 9, se incorpora la evaluación y revisión anual de la política. - Punto 11, se modifica formato de tabla.
4.0	Diciembre 2019	Actualización de Política.	Todas las Páginas.



1. **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.
2. **DÉJESE**, expresa constancia que la presente Resolución Exenta no eroga gasto alguno para esta Superintendencia de Educación.
3. **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.
4. **PUBLÍQUESE**, una vez totalmente tramitada la presente Resolución Exenta, en la Intranet institucional y el sitio web www.supeduc.cl.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

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