MIC/FTO/AAM/PBC/DLR

Superintendencia de Educación
TOTALMENTE TRAMITADO

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0730 DE 2017 Y APRUEBA VERSIÓN N°2 DE LA POLÍTICA DE SEGURIDAD QUE REGULA LA RELACIÓN CON PROVEEDORES DE BIENES Y/O SERVICIOS, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN, EN LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0786

SANTIAGO, 30 DIC 2019

VISTO:

Lo dispuesto en el DFL N° 1/19.653, de 2000, del Ministerio Secretaria 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 el Decreto de nombramiento del Superintendente de Educación, en trámite, 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 20 de octubre de 2017, se dicta Resolución Exenta N° 0730, que aprueba versión 1.0 de la política de seguridad que regula la relación con proveedores de bienes y/o servicios de la Superintendencia de Educación.

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, 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° 0730, de 2017, de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°02 de la política de seguridad que regula la relación con proveedores de bienes y/o servicios en la Superintendencia de Educación, cuyo texto es el siguiente:

Política de seguridad que regula la relación con proveedores de bienes y/o servicios

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

Establecer los requisitos de seguridad de la información para cuando se realice la contratación de servicios externos, asociados al acceso de proveedores a los activos de información de la Superintendencia de Educación (SUPEREDUC), incluido todo el personal externo que trabaja para SUPEREDUC y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos de SUPEREDUC en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas administrados por SUPEREDUC.

2. Alcance

Esta política se aplica a todas las actividades desarrolladas por personal externo que presta servicios a SUPEREDUC y que pertenecen a empresas proveedoras de servicios, vinculadas a través del correspondiente contrato de provisión de

servicios y a todos los usuarios ya sean funcionarios/as de planta, contrata, honorarios, asesores, y practicantes que presten servicios a SUPEREDUC.

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

- A.15.01.01 Política de seguridad de la información para las relaciones con los proveedores.
- A.15.02.01 Supervisión y revisión de los servicios del proveedor.

3. Referencias normativas

- Ley 19.628 sobre Protección de datos de carácter personal.
- Ley 19.886 de compras públicas.
- Política general de seguridad de la información vigente.
- Política de uso de contraseñas vigente.
- Política de pantallas y escritorios limpios vigente.
- Política de uso de computadores vigente.
- Política de uso de medios removibles vigente.
- Manual de procedimientos de compras vigente.

4. Definiciones

Concepto	Descripción
Activos de Información	Recursos del sistema de información, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Una organización incluye diferentes tipos de activos: • Activos relacionados con el entorno (edificios, instalaciones, equipamientos) y personal. • Activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones). • Activos relacionados con la información (datos, metadatos y soportes). • Activos relacionados con las funcionalidades de la organización (productos, servicios). • Activos intangibles (credibilidad, conocimiento acumulado).
Incidente de seguridad	Evento único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer la operación de negocio y de amenazar la seguridad de la información. Por lo tanto, un incidente de seguridad se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información: un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información del organismo.
Integridad	Se entiende como la característica que implica la corrección y completitud de los datos o de la información manejada, contar con todas sus partes y estar completo.
Disponibilidad	Es el aseguramiento de que los usuarios autorizados tienen acceso a la información, sistemas y a los activos de la superintendencia, cuando es requerido.
Confidencialidad	Es la propiedad de la información, un documento o mensaje que únicamente está autorizado para ser leído o entendido por algunas personas o entidades. Mantiene la cualidad de mantenerse reservada para el conocimiento de una persona o de algunas, pero no debe ser expuesta en forma masiva.
Datos personales	Conjunto de datos que constituyen información que podría permitir identificar a una persona, ya sea directa o indirectamente. Además, dentro de los datos personales, existe una categoría de información que requiere de protección adicional (Ej: nombre y apellidos, nuestra fecha de nacimiento, nuestra dirección postal o de correo electrónico, el número de teléfono, el RUT, la patente de nuestro automóvil, entre otros).
Datos sensibles	Corresponden a datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o íntima, tales como hábitos

Concepto	Descripción
	personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

5. Roles y Responsabilidades

Rol	Responsabilidades
Departamento de Administración	a) Dar cumplimiento a lo establecido en esta Política. b) Dar cumplimiento y velar por que el resto de la organización de cumplimiento a lo establecido en el manual de procedimientos de adquisiciones. c) Incluir en los contratos con terceros las respectivas cláusulas de confidencialidad según sea el caso. d) Incluir en los acuerdos con terceros, las medidas de supervisión y revisión de los servicios según sea el caso.
Proveedores	a) Dar estricto cumplimiento a las normas de seguridad descritas en la presente política y en la documentación del Sistema de Gestión de Seguridad de la Información.
Personal externo que presta servicios a SUPEREDUC	a) Dar estricto cumplimiento a las normas de seguridad descritas en la presente política y en la documentación del Sistema de Gestión de Seguridad de la Información.
Encargado/a de Seguridad de la Información y ciberseguridad	a) Gestionar los incidentes de seguridad de la información relacionados a los incumplimientos de la presente política
Usuarios	a) Todos los usuarios que interactúan con el personal de los proveedores debe dar estricto cumplimiento en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la SUPEREDUC. b) Monitorear, revisar y auditar la presentación de los servicios del proveedor de manera regular y de acuerdo a los lineamientos entregados por el Departamento de Administración.

6. Directrices

6.1. Personal externo

Todo personal externo que desarrolle labores para SUPEREDUC deberá tomar conocimiento de la Política General de Seguridad de la Información y el resto de las políticas y procedimientos del Sistema de Seguridad de la Información disponibles en el sitio web www.supereduc.cl y en la Intranet institucional, cumplir sus directrices y colaborar en su aplicación dentro de su ámbito de acción.

Para estos efectos, el trabajo o proyectos realizados por el proveedor, deben ser compatibles con los estándares de seguridad de la información establecidos por el Sistema de Seguridad de la Información de la SUPEREDUC.

6.2. Prestación de servicios en SUPEREDUC

6.2.1. Los proveedores sólo podrán desarrollar para SUPEREDUC aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios. De este modo, se entenderá que todas las

actividades desarrolladas para SUPEREDUC por personal perteneciente a empresas proveedoras se encuadra en los contratos de provisión de servicios que vinculan a SUPEREDUC con estos proveedores.

6.2.2. Las actividades desarrolladas por el personal perteneciente a empresas proveedoras se realizarán de acuerdo a lo establecido en las correspondientes bases y contratos de provisión de servicios.

6.2.3. La empresa proveedora proporcionará a SUPEREDUC periódicamente la relación de personas, perfiles, funciones y responsabilidades asociados al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzcan en dicha relación.

6.2.4. De acuerdo a lo establecido en las cláusulas asociadas al contrato de provisión de servicios, todo el personal externo que desarrolle labores para SUPEREDUC deberá cumplir con las directrices definidas en el presente documento y, las políticas y procedimientos del Sistema de Seguridad de la Información. En caso de incumplimiento de cualquiera de estas obligaciones, SUPEREDUC se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como las sanciones que se consideren pertinentes en relación a la empresa o persona contratada y la aplicación de multas según corresponda.

6.2.5. La empresa proveedora deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio, como de manera transversal en materia de seguridad de la información, para lo cual deberá asegurarse, al menos, de que todo el personal asociado al servicio conoce y se compromete a cumplir las Políticas de Seguridad de la Información de SUPEREDUC.

6.2.6. Cualquier tipo de intercambio de información que se produzca entre SUPEREDUC y las empresas proveedoras se entenderá que ha sido realizado dentro del marco establecido por el contrato de provisión de servicios correspondiente, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho contrato.

6.2.7. Para efectos de la aplicación de la presente política, se entenderá coma activo de información, todo lo relacionado con el entorno, con los sistemas de tecnologías de información, re

6.3. Confidencialidad de la Información

6.3.1. El personal externo que tenga acceso a información de SUPEREDUC deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Solo se podrá considerar como información

no confidencial aquella información de SUPEREDUC a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por SUPEREDUC.

6.3.2. Queda prohibido para los proveedores revelar, modificar, destruir o hacer mal uso de la información, cualquiera que sea el soporte en que se encuentre contenida.

6.3.3. El proveedor deberá resguardar por un tiempo indefinido la confidencialidad y no podrá difundir la información a la que tiene acceso, salvo que esté debidamente autorizado por el/la Encargado de Seguridad de la Información y Ciberseguridad.

6.3.4. El proveedor deberá minimizar el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros de acuerdo a lo establecido en la *Política de pantallas y escritorios limpios.*

6.3.5. Ningún proveedor, dará usos no propios de su responsabilidad, a ningún material o información propia o confiada a SUPEREDUC.

6.3.6. En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios tome conocimiento de información confidencial contenida en cualquier tipo de soporte, debe entenderse que es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información. Asimismo, el empleado deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación con SUPEREDUC de su empresa. La utilización continuada de la información en cualquier formato o soporte distinta a la pactada y sin conocimiento de SUPEREDUC no supondrá, en ningún caso, una modificación de este punto.

6.3.7. Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para SUPEREDUC.

6.3.8. El incumplimiento de estas obligaciones será sancionado en los términos establecido por las leyes vigentes.

6.3.9. Para garantizar la seguridad de los datos de carácter personal albergados en medios digitales (bases de datos, planillas electrónicas, reportes, etc.) el personal que pertenece a empresas proveedoras deberá observar las siguientes normas, además de las consideraciones ya mencionadas:

- El personal solo podrá crear registros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos registros temporales nunca serán ubicados en unidades locales de disco de los puestos PC del personal y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
- No se guardarán datos de carácter personal en las unidades locales de disco de los puestos PC de usuario.
- La salida de soportes digitales que contengan datos de carácter personal (pendrive, discos duros, CD, computadores, servidores, etc.), fuera de las instalaciones en las que se almacena

dicha información, únicamente podrá ser autorizada por el responsable de la información de acuerdo a lo establecido en la *Política de uso de medios removibles y dispositivos móviles.*

- Los soportes digitales que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido solo al personal autorizado de SUPEREDUC.

6.4. Propiedad intelectual

6.4.1. El personal externo deberá garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

6.4.2. Queda estrictamente prohibido el uso de programas informáticos en la SUPEREDUC que no cuenten con la debida licencia de uso.

6.4.3. Asimismo, queda prohibido el uso, reproducción, entrega, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización de SUPEREDUC.

6.5. Intercambio de información

6.5.1 Ninguna persona debe ocultar o manipular su identidad bajo ninguna circunstancia.

6.5.2 En relación al intercambio de información dentro del marco del contrato de provisión de servicios, se considerarán no autorizadas las siguientes actividades:

6.5.3. Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección intelectual.

6.5.4. Transmisión o recepción de toda clase de material pornográfico, mensajes o de una naturaleza sexual explicita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.

6.5.5. Transferencia de archivos a terceras partes no autorizadas de material de SUPEREDUC o material que ha sido definido como confidencial por el Sistema de Seguridad de la Información.

6.5.6. Transmisión o recepción de archivos que infrinjan la Ley de Protección de Datos de Carácter Personal (Ley N°19.628) o directrices de SUPEREDUC.

6.5.7. Transmisión o recepción de aplicaciones y/o juegos no relacionadas con las actividades de SUPEREDUC.

6.5.8. Participación en actividades de Internet como grupos de noticias, juegos, redes sociales u otras que no estén directamente relacionadas con el servicio contratado por la SUPEREDUC.

6.5.9. Quienes trabajen prestando servicios a la SUPEREDUC no deben divulgar información sobre los procesos internos que se desarrollan al interior de la institución.

6.5.10. Toda salida de información que contenga datos de carácter personal (tanto en soportes digitales como en papel o por correo electrónico) solo podrá ser realizada por personal autorizado y con la debida autorización del responsable de esa información.

6.5.11. Si el tratamiento de datos de carácter personal se llevase a cabo fuera de las instalaciones de SUPEREDUC, dicho tratamiento deberá ser autorizado expresamente por el responsable de esa información y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de información tratado.

6.5.12. La transmisión de datos de carácter personal, a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

6.6. Uso apropiado de los recursos

6.6.3. El proveedor se compromete a informar periódicamente a SUPEREDUC de los activos con los que proporciona el servicio.

6.6.4. El proveedor se compromete a utilizar los recursos dispuestos para la previsión del servicio de acuerdo a las condiciones para las que fueron diseñados e implantados.

6.6.5. Los recursos que SUPEREDUC pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplir las obligaciones y propósito de la operativa para la que fueron proporcionados. SUPEREDUC Implementará, en los casos que corresponda, mecanismos de supervisión y revisión de los servicios a través de medidas de control y auditoría que verifiquen el uso apropiado de estos recursos.

6.6.6. Todos los equipos del proveedor que se conecten a la red de producción de SUPEREDUC serán de las marcas y modelos autorizados por SUPEREDUC. El proveedor pondrá a disposición de la Unidad de Infraestructura y Operaciones de SUPEREDUC dichos equipos para que les instale el software homologado y las configure apropiadamente.

6.6.7. Cualquier archivo introducido en la red de SUPEREDUC o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en las Políticas y procedimientos de Seguridad de la Información de la SUPEREDUC y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.

6.6.8. Se deberán restituir a SUPEREDUC todos los activos físicos y destruir o restituir a SUPEREDUC todos los activos de información, sin retraso injustificado, una vez que finalice el contrato. Todos los equipos personales a los que SUPEREDUC les haya instalado software se llevarán a la Unidad de Infraestructura y Operaciones de la SUPEREDUC para que se formatee el disco duro a la finalización del servicio de acuerdo a lo establecido en la *Política seguridad en la reutilización o descarte de equipos.*

Se prohíbe expresamente

6.6.9. El uso de los recursos proporcionados por SUPEREDUC para actividades no relacionadas con el propósito del servicio contratado.

6.6.10. La conexión a la red de producción de SUPEREDUC de equipos y/o aplicaciones que no estén especificados como parte del Software o de los estándares de los recursos informáticos propios de SUPEREDUC o bajo supervisión de SUPEREDUC.

6.6.11. Introducir en los Sistemas de información o la red de SUPEREDUC contenidos obscenos, amenazadores, inmorales u ofensivos.

6.6.12. Introducir voluntariamente en la red de SUPEREDUC cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todo el personal con acceso a la red de SUPEREDUC tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

6.6.13. Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que SUPEREDUC les haya asignado en el marco del cumplimiento de los servicios contratados.

6.6.14. Intentar acceder sin autorización explícita a áreas restringidas de los Sistemas de información y aplicativos de SUPEREDUC.

6.6.15. Intentar distorsionar o falsear los registros "log" de los Sistemas de información de SUPEREDUC.

6.6.16. Intentar descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de SUPEREDUC.

6.6.17. Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los recursos informáticos de SUPEREDUC.

6.6.18. Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos de responsabilidad de SUPEREDUC.

6.7. Responsabilidad del usuario (personal del proveedor)

Los proveedores de servicios deberán asegurarse de que todo el personal que desarrolla labores para SUPEREDUC respeten los siguientes principios básicos dentro de su actividad informática:

6.7.3. Cada persona con acceso a información de SUPEREDUC es responsable de la actividad desarrollada por su identificador de usuario de acuerdo a lo establecido en la *Política de uso de contraseñas* y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto del personal bajo ningún concepto.

6.7.4. Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario de acuerdo a la *Política de uso de contraseñas.*

6.7.5. Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.

Cualquier persona con acceso a información de responsabilidad de SUPEREDUC deberá seguir las siguientes directivas en relación a la gestión de las contraseñas de acuerdo a lo establecido en la *Política de uso de contraseñas:*

6.7.6. Seleccionar contraseñas de calidad de acuerdo a lo establecido en la *Política de uso de contraseñas.*

6.7.7. Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas de acuerdo a lo establecido en la *Política de uso de contraseñas.*

6.7.8. Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar viejas contraseñas de acuerdo a lo establecido en la *Política de uso de contraseñas.*

6.7.9. Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión ("login") de acuerdo a lo establecido en la *Política de uso de contraseñas.*

6.7.10. Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro de acuerdo a lo establecido en la *Política de uso de contraseñas.*

6.7.11. Notificar cualquier incidente de seguridad relacionado con sus contraseñas como perdida, robo o indicio de perdida de confidencialidad de acuerdo a lo establecido en el *Procedimiento de gestión de incidentes de seguridad de la información.*

Cualquier persona con acceso a información de responsabilidad de SUPEREDUC deberá velar para que los equipos queden protegidos cuando vayan a quedar desatendidos de acuerdo a lo establecido en la *Política de pantallas y escritorios limpios.*

Cualquier persona con acceso a información de responsabilidad del SUPEREDUC deberá respetar lo definido en las políticas y procedimientos del Sistema de Seguridad de la Información, con especial atención a las siguientes políticas: de *Pantallas y Escritorios limpios*, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles; de *uso de medios removibles* y reducir los riesgos de acceso no autorizado, perdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

6.7.12. Almacenar bajo llave los documentos en papel y los medios digitales con información de responsabilidad de SUPEREDUC en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo de acuerdo a lo establecido en la *Política de pantallas y escritorios limpios*.

6.7.13. No dejar desatendidos los equipos asignados a funciones criticas de SUPEREDUC, y bloquear su acceso cuando sea necesario de acuerdo a lo establecido en la *Política de pantallas y escritorios limpios*.

6.7.14. Proteger, siempre que se utilice información de responsabilidad de SUPEREDUC, tanto los puntos de recepción y envío de información (correo postal, máquinas de scanner y fax) como los equipos de

duplicado (fotocopiadora, multifuncionales). La reproducción o envío de información con este tipo de dispositivos quedara bajo la responsabilidad del usuario.

6.7.15. Retirar, sin retraso injustificado, cualquier información confidencial que sea responsabilidad del SUPEREDUC, una vez impresa.

6.7.16. Los listados con datos de carácter personal o información confidencial responsabilidad del SUPEREDUC deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.

6.7.17. Los listados con datos de carácter personal o información confidencial que sea de responsabilidad de SUPEREDUC deberá eliminarse de manera segura una vez que ya no sean necesarios.

6.7.18. Las personas con acceso a sistemas y/o información de SUPEREDUC no deben, sin previa autorización expresa, realizar pruebas para detectar y/o utilizar una supuesta debilidad o incidente de seguridad, en caso de identificarse incidentes o debilidades que puedan suponerse relacionadas con la seguridad de la información. En caso de detectar incidentes de seguridad deberán informarlos de acuerdo a lo establecido en el *Procedimiento de gestión de incidentes*.

6.7.19. Ninguna persona con acceso a sistemas y/o información de SUPEREDUC intentará, sin previa autorización expresa, por ningún medio transgredir el sistema de seguridad y las autorizaciones. Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoria expresamente autorizadas por el Departamento de Tecnología y Procesos.

6.7.20. Ningún dato de carácter personal de responsabilidad de SUPEREDUC será almacenado en equipos de usuario personales ni soportes de información.

6.7.21. Todo el personal que acceda a la información y/o los sistemas de responsabilidad de SUPEREDUC deberá seguir las siguientes normas de actuación:

- Proteger la información confidencial perteneciente o cedida por terceros a SUPEREDUC de toda revelación no autorizada, modificación, destrucción o uso incorrecto ya sea accidental o no.
- Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
- Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o la información accedida.
- Conocer, aceptar y cumplir las Políticas y procedimientos de Seguridad de la Información antes de acceder a la información y/o los sistemas de SUPEREDUC.

6.8. Equipos de usuario

El proveedor de servicios en los casos que provea equipamiento informático deberá asegurarse de cumplir con los estándares mínimos y requisitos de seguridad para acceder a información, considerando las siguientes normas:

6.8.1. Cuando se desatienda un puesto durante un periodo corto de tiempo el sistema deberá activar su bloqueo de acuerdo a lo establecido en la *Política de uso de contraseñas.*

6.8.2. Ningún equipo de usuario dispondrá de herramientas que puedan transgredir el sistema de seguridad ni las autorizaciones dentro de los sistemas de la organización de acuerdo a lo establecido en la *Política de uso de computadores.*

6.8.3. Los equipos de usuario se mantienen de acuerdo a las especificaciones del fabricante de acuerdo a lo establecido en la *Política de uso de computadores.*

6.8.4. Todos los equipos de usuario están adecuadamente protegidos frente a malware de acuerdo a lo establecido en la *Política de uso de computadores.*

i. El software antivirus se deberá instalar y usar en todos los computadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
ii. Se mantendrán al día con las últimas actualizaciones de seguridad disponibles.
iii. El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática de los archivos de definición de virus.

Se velará especialmente por la seguridad de todos los equipos móviles de usuario que contengan información de responsabilidad de SUPEREDUC o permitan acceder a ella de algún modo, mediante las siguientes acciones:

6.8.5. Verificando que no incluyen más información de responsabilidad de SUPEREDUC que la que sea estrictamente necesaria.

6.8.6. Garantizando que se aplican controles de acceso a dicha información.

6.8.7. Minimizando los accesos a dicha información en presencia de personas ajenas al servicio provisto a SUPEREDUC.

6.8.8. Transportando los equipos en fundas, mochilas, bolsos o equipamiento similar que incorpore la apropiada protección frente a golpes de acuerdo a lo establecido en la *Política de uso de computadores.*

6.8.9. Tomando especiales precauciones en el exterior de las dependencias de SUPEREDUC para evitar la visión accidental por parte de terceras personas de la información de responsabilidad de SUPEREDUC de acuerdo a lo establecido en la *Política de uso de computadores.*

6.9. Gestión del equipamiento (hardware)

Los proveedores de servicios deberán asegurarse de que todos los equipos proporcionados por SUPEREDUC para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Para ello deberá cumplir con lo siguiente:

6.9.1. El proveedor deberá mantener una relación actualizada de equipos proporcionados por SUPEREDUC y usuarios de dichos activos, o responsables asociados en caso de que los activos no sean de uso unipersonal. Dicha relación podrá ser requerida por SUPEREDUC en cualquier momento.

6.9.2. Siempre que un proveedor quiera reasignar algún equipo de SUPEREDUC que haya contenido información de responsabilidad de SUPEREDUC deberá devolver temporalmente a SUPEREDUC dicho activo para que se puedan llevar a cabo los procedimientos de borrado seguro necesarios de forma previa a su reasignación *ver Política eliminación o reutilización segura de equipos.*

6.9.3. En caso de que un proveedor cese en la prestación del servicio, deberá devolver a SUPEREDUC toda la relación de equipos recibidos, tal y como establecen los correspondientes contratos de prestación de servicios. Solo en el caso de activos de información el proveedor podrá proceder a su eliminación segura, en cuyo caso deberá notificar a SUPEREDUC dicha eliminación *ver Política eliminación o reutilización segura de equipos.*

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 política			
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.

13. Anexos

13.8. Anexo N°1

DECLARACIÓN JURADA DE RECONOCIMIENTO Y CONFIDENCIALIDAD

En _____, de Chile, a _____ de ____ de 20XX, don/ña _____ en representación de _____, RUT _____, declaro lo siguiente:

a) Declaro conocer, estar al tanto y aceptar el contenido de las Políticas de Seguridad de la Información actualmente vigentes publicadas en el sitio web institucional de la Superintendencia de Educación y que se ha informado de ellas a todos nuestros dependientes, quedando todos impedidos de alegar desconocimiento de ellas.

b) Que toda la información a la que pueda acceder tanto esta entidad como sus dependientes con motivo de la presente contratación deberá ser resguardada bajo absoluta confidencialidad, evitando absoluta, estricta, permanente e indefinidamente el uso y la divulgación por cualquier medio dicha información, incluso el emitir opiniones o difundir juicios sin que signifique necesariamente divulgar información.

c) Que, se entenderá por información confidencial a todos antecedentes obtenidos de manera oral, escrita o electrónica, que emane directa o indirectamente de y la Superintendencia hacia nosotros y que sea susceptible de ser revelada por escrito, de palabra o por cualquier otro medio o soporte, tangible o intangible, intercambiada entre ambas partes, incluidos los acuerdos suscritos por las partes o la correspondencia relacionada con el mismo incluyendo la identificación por el nombre o descripción de las partes, especialmente la información referida a los sistemas.

d) Adoptaré todas las medidas, dispositivos y procedimientos necesarios para proteger la información confidencial y tomar rigurosas precauciones para mantener la confidencialidad de todos los antecedentes a los cuales pueda tener acceso tanto durante la vigencia de la contratación como en el futuro, entendiéndose que de modo alguno podre divulgarla, salvo autorización expresa y por escrito otorgada por la Superintendencia.

e) Que, existe prohibición tanto para nosotros como para nuestros dependientes, copiar, informar directa o indirectamente, publicar, distribuir, divulgar, por sí o a través de terceros, ni difundir, ni por cualquier procedimiento ceder total o parte la información confidencial a un tercero, ni usar toda o parte de ella salvo autorización previa y por escrito de la Superintendencia. Y que la entrega de cualquier tipo de información por parte de la Superintendencia no supondrá ninguna licencia, cesión de uso o derecho bajo cualquier tipo de propiedad industrial o intelectual (tales como patentes, marcas, u otros derechos de propiedad industrial o intelectual).

f) Que, toda la Información permanecerá como propiedad de la Superintendencia y deberá ser devuelta inmediatamente después de que ella nos la solicite por escrito o destruida a su petición, haciendo entrega en ese momento de una

declaración donde confirmemos que dicha información y todas las copias hechas por cualquier medio que contengan esta información confidencial, ha sido destruida o devuelta.

g) Que, cualquier divulgación que no esté autorizada por la Superintendencia o el uso de la información confidencial, podría provocar numerosos y graves perjuicios y/o daños a la Superintendencia, quedando esta última habilitada para ejercer todas las acciones que estime pertinentes.

Firma representante (s) legal(es)

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 SUPERINTENDENTE

CRISTIAN O'RYAN SQUELLA
SUPERINTENDENTE 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/a de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.