Gobierno de Chile

Superintendencia de Educación

FISCAL

MPV/CNN/HCJ/PSC/PSV

APRUEBA 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° 0730

SANTIAGO, 20 OCT 2017

VISTO:

Lo dispuesto en el DFL N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en el Decreto con Fuerza Ley N° 29, de 2004, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en la Ley N° 19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; en el Decreto N°571, de 2014, del Ministerio de Educación, en la Ley N° 20.529, de 2011, del Ministerio de Educación, sobre el Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización; en el Decreto con Fuerza de Ley N° 5, de 2012 ,del Ministerio de Educación; la Norma Chilena NCh-ISO 27001/2013 tecnología de la información-técnicas de seguridad-sistemas de gestión de la seguridad de la información; en la norma Chilena NCh-ISO 27002-2013, tecnología de la información- código de prácticas para la gestión de la seguridad de la información, y la Resolución N°1600 de 30 de octubre de 2008, de Contraloría General de la República, que fija las normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que, de acuerdo a lo dispuesto en el artículo 47 de la Ley N°20.529, sobre el Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Medica y su fiscalización, se crea la Superintendencia de Educación, como "un servicio público funcionalmente descentralizado y territorialmente desconcentrado, dotado de personalidad jurídica y patrimonio propio y que se relaciona con el Presidente de la Republica por intermedio del Ministerio de Educación".

2. Que, en atención a que los Órganos de la Administración del Estado tienen la obligación de respetar la normativa vigente respecto de la Seguridad de la Información, esta Superintendencia procedió a la designación de un Encargado de Seguridad de la Información, que actuará como asesor del Jefe de Servicio en las materias relativas a la seguridad de los documentos electrónicos y los activos de información institucionales.

3. Que, con fecha 17/10/2017 se dicta resolución exenta N°0703, de esta Superintendencia que aprobó la Política General de Seguridad de la Información.

4. Que, con la finalidad de hacer efectiva la política antes mencionada, resulta necesario establecer políticas específicas de Seguridad de la Información, dentro de los cuales se encuentra la Política de seguridad que regula la relación con proveedores de bienes y/o servicios.

RESUELVO:

1. **APRUÉBASE,** la Política de seguridad que regula la relación con proveedores de bienes y/o servicios, versión N°1, en la Superintendencia de Educación, cuya transcripción, fiel, exacta e integra se adjunta a la presente Resolución.

2. **ESTABLÉZCASE,** la obligación de el/la Encargado/a de Seguridad de la Información de la Superintendencia de Educación, de difundir la política fijada por este instrumento y de velar junto con el comité de Seguridad de la Información por su estricto cumplimiento.

3. **DISPÓNGASE,** que el/la Jefe/a de la División de Administración General, deberá tomar todas las medidas y acciones tendientes a la implementación de esta política.

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

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

ANÓTESE, COMUNIQUESE Y ARCHÍVESE.

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACION
SUPERINTENDENTE

ALEXIS RAMIREZ ORELLANA
SUPERINTENDENTE
SUPERINTENDENCIA DE EDUCACIÓN

Distribución:
1. Gabinete.
2. División de Fiscalización.
3. División de Fiscalía.
4. División de Promoción y Resguardo de Derechos Educacionales.
5. Intendencia de Educación Parvularia.
6. División de Administración General.
7. Departamento de Finanzas.
8. Departamento Gestión de Personas.
9. Departamento de Administración.
10. Departamento de Tecnologías de Información.
11. Direcciones Regionales (15).
12. Departamento de Auditoría.
13. Coordinación de Gestión y Desarrollo.
14. Oficina de Partes.

Superintendencia de Educación
TOTALMENTE TRAMITADO

POLÍTICA DE SEGURIDAD QUE REGULA LA RELACION CON PROVEEDORES DE BIENES Y/O SERVICIOS

VERSIÓN 1.0

CONTROL ISO27001:2013

A.15.1.1

INDICE

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[1], 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.

3. Roles y Responsabilidades:

3.1. Departamento de Administración:

3.1.1. Dar cumplimiento a lo establecido en esta Política.

3.1.2. Dar cumplimiento a lo establecido en el manual de compras.

3.1.3. Incluir en los contratos con terceros las respectivas cláusulas de confidencialidad según sea el caso.

3.2. Proveedores:

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.

3.3. Personal externo que presta servicios a SUPEREDUC:

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.

3.4. Usuarios internos:

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

[1] *Se entiende por usuarios a los funcionarios/as en calidad jurídica planta, contrata, reemplazos y suplencia, tanto para el personal a honorarios y terceros (proveedores, compra de servicios, etc.) que trabajen para SUPEREDUC.*

en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la SUPEREDUC.

3.5. Encargado/a de Seguridad de la Información:

Gestionar los incidentes de seguridad de la información relacionados a los incumplimientos de la presente política.

4. Definiciones:

a) **Activos de Información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información. Para el presente documento considera especialmente: bienes con cargo, los accesos habilitados a sistemas y recursos informáticos y la información de valor para la Institución que generen las personas como resultado de la evaluación que realiza el funcionario/a y su jefatura directa.

b) **Incidente de seguridad:** Cualquier evento o situación que comprometa de manera IMPORTANTE la **disponibilidad**, **integridad** y **confidencialidad** de la información, junto con la plataforma tecnológica, procesos y aplicativos que permitan acceder a esta en forma oportuna. En general es una violación de una política, estándar o procedimiento de seguridad que no permita dar un servicio computacional.

c) **Integridad:** Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas.

d) **Disponibilidad:** Acceso y utilización de los servicios sólo y en el momento de ser solicitado por una persona autorizada.

e) **Confidencialidad:** Información disponible exclusivamente a personas autorizadas.

f) **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).

g) **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 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. Documentos relacionados:

a) Ley 19.628 sobre Protección de datos de carácter personal.

b) Ley 19.886 de compras públicas.

c) Política general de seguridad de la información.

d) Política de uso de contraseñas.
e) Política de pantallas y escritorios limpios.
f) Política de uso de computadores.
g) Política de uso de medios removibles.
h) Manual de procedimientos de compras.
i) Instructivo de acuerdos de confidencialidad en contratos con terceros.

6. Política:

6.1. Personal externo:

Todo personal externo que desarrolle labores para SUPEREDUC deberá tomar conocimiento de la Política General de Seguridad de la Información, disponible en el sitio web www.supereduc.cl y en la Intranet institucional, observando sus directrices y colaborando 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 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, toda información, además de las personas, tecnología y equipamiento que la soportan.

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 responsable de ella.

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 Ver 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.

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

6.3.8. 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:

6.3.9. 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.

6.3.10. No se guardarán datos de carácter personal en las unidades locales de disco de los puestos PC de usuario.

6.3.11. 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 *ver Política de uso de medios removibles y dispositivos móviles.*

6.3.12. 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 que no cuenten con licencia.

6.4.3. Asimismo, queda prohibido el uso, reproducción, cesión, 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:

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

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

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

6.5.2. 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.

6.5.3. Transferencia de archivos a terceras partes no autorizadas de material de SUPEREDUC o material que es de alguna u otra manera confidencial.

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

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

6.5.6. Participación en actividades de Internet como grupos de noticias, juegos, redes sociales u otras que no estén directamente relacionadas con el servicio.

6.5.7. Quienes trabajen en conjunto con SUPEREDUC no deben divulgar información sobre los procesos internos de este.

6.5.8. 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.

6.5.9. 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.

6.5.10. 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:

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

6.6.2. 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.

6.6.3. 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 cumplimentar las obligaciones y propósito de la operativa para la que fueron proporcionados. SUPEREDUC se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

6.6.4. 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 SUPEREDUC dichos equipos para que SUPEREDUC les instale el software homologado y las configure apropiadamente.

6.6.5. 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 de Seguridad de SUPEREDUC y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.

6.6.6. Se deberán restituir a SUPEREDUC todos los activos físicos y destruir o restituir a SUPEREDUC todos los activos de información, sin retraso injustificado, antes de la finalización del contrato. Todos los equipos personales a los que SUPEREDUC les haya instalado software se llevaran a SUPEREDUC para que se formatee el disco duro a la finalización del servicio, ver Política seguridad en la reutilización o descarte de equipos.

Se prohíbe expresamente:

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

6.6.8. 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.

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

6.6.10. 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.

6.6.11. Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que SUPEREDUC les haya asignado.

6.6.12. Intentar acceder sin autorización explícita a áreas restringidas de los Sistemas de información de SUPEREDUC.

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

6.6.14. 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.

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

6.6.16. 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:

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:

6.7.1. Cada persona con acceso a información de SUPEREDUC es responsable de la actividad desarrollada por su identificador de usuario *ver 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.

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

6.7.3. 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 *ver Política de uso de contraseñas:*

6.7.4. Seleccionar contraseñas de calidad *ver Política de uso de contraseñas.*

6.7.5. Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas *ver Política de uso de contraseñas.*

6.7.6. Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar viejas contraseñas *ver Política de uso de contraseñas.*

6.7.7. Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión ("login") *ver Política de uso de contraseñas.*

6.7.8. Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro *ver Política de uso de contraseñas.*

6.7.9. Notificar cualquier incidente de seguridad relacionado con sus contraseñas como perdida, robo o indicio de perdida de confidencialidad *ver Procedimiento de reporte de eventos y debilidades 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 *ver Política de pantallas y escritorios limpios.*

Cualquier persona con acceso a información de responsabilidad del SUPEREDUC deberá respetar al menos las siguientes políticas de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles *ver Política 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 *ver Política de pantallas y escritorios limpios*.

6.7.10. 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 *ver Política de pantallas y escritorios limpios*.

6.7.11. No dejar desatendidos los equipos asignados a funciones criticas de SUPEREDUC, y bloquear su acceso cuando sea necesario *ver Política de pantallas y escritorios limpios*.

6.7.12. 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.

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

6.7.14. 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.

6.7.15. 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.

6.7.16. 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.

6.7.17. 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.

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

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

6.7.19. 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.

6.7.20. Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.

6.7.21. Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o la información accedida.

6.7.22. Conocer, aceptar y cumplir las presentes Políticas 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 *ver 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 *ver Política de uso de computadores.*

6.8.3. Los equipos de usuario se mantienen de acuerdo a las especificaciones del fabricante *ver Política de uso de computadores.*

6.8.4. Todos los equipos de usuario están adecuadamente protegidos frente a malware *ver 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 *ver 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 *ver 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. Publicación y comunicación de esta política

La comunicación de esta política se efectuará de manera que los contenidos de la documentación sean accesibles y comprensibles para todos los usuarios, pudiendo

utilizarse los canales de difusión establecidos por la SUPEREDUC (www.supereduc.cl, intranet, email, circulares, etc).

8. Aceptación de la política

Todos los usuarios de la SUPEREDUC, sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar ésta política y procedimientos relacionados.

Para el caso de terceros y por solo hecho de participar en algún proceso de adquisición del servicio, el oferente debe dar cumplimiento a la política y procedimientos vigentes de seguridad de la información de la SUPEREDUC, publicados en el sitio web www.supereduc.cl y sus correspondientes modificaciones, la cuales se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

9. Revisión de la política

La presente política será evaluada y revisada al menos una vez al año, o cuando SUPEREDUC lo requiera, para asegurar su continuidad e idoneidad, considerando cambios externos o internos que puedan afectarla.

10. Sanciones aplicables

El incumplimiento o violación a esta política, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios/as de la SUPEREDUC, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

11. Control de versiones:

Control de versiones		
Versión	**Resumen de cambios**	**Fecha**
1.0	- Versión inicial	Octubre 2017

12. Responsabilidades de elaboración y aprobación del documento:

Elaborado Por	Revisado por	Aprobado por
Encargado de Seguridad de la Información	Comité Operativo Seguridad de la Información	Comité Directivo Seguridad de la Información

13. ANEXO N° 1

FORMATO TIPO: ACUERDO DE RESERVA Y CONFIDENCIALIDAD

Nombre del Profesional que suscribe el acuerdo

En Santiago, a dd de mmmm de aaaa, entre Razón Social del Contratista, en adelante el "Contratista", RUT XX.XXX.XXX-X, representada por don XXXX RUT XX.XX.XX-X, ambos domiciliados en domicilio del contratista, comuna de XXXX, y LA SUPERINTENDENCIA DE EDUCACIÓN, en adelante "la Superintendencia" o "SUPEREDUC", RUT 61.980.220-9, representado por el Superintendente de Educación, don/doña XXXX, ambos domiciliados para estos efectos en calle Morandé 115, Piso 10, comuna de Santiago, se ha suscrito el siguiente Acuerdo de Reserva y Confidencialidad, que se expresa en las cláusulas siguientes:

1. Antecedentes Generales.

Como resultado del proceso licitatorio ID XXXX, efectuado por la Dirección de Compras y Contratación Pública, el Contratista resultó adjudicado en el Convenio Marco de Perfiles para el Desarrollo y Mantención de Sistemas Informáticos.

A través del presente acuerdo la Superintendencia de Educación busca resguardar la reserva y confidencialidad de la información que durante la ejecución del "Nombre del Proyecto o Servicio Contratado" el Contratista Razón Social del Contratista pudiese tener acceso.

2. Considerandos

Teniendo presente que:

a) el CONSULTOR le presta o prestará servicios a la SUPERINTENDENCIA y que, en virtud de ello, éste último revelará al CONSULTOR o éste conocerá, determinados antecedentes o información de la SUPERINTENDENCIA.

b) el CONSULTOR desea y está obligado a mantener bajo una absoluta confidencialidad dichas informaciones y antecedentes

c) que estos antecedentes pueden ser conocidos a través del desarrollo de sistemas, operación de los mismos, resultados, datos e informes obtenidos producto del desarrollo de la solución y/o la prestación de servicios

d) se desea evitar absoluta, estricta, permanente e indefinidamente el uso y la divulgación por cualquier medio dicha información por parte del CONSULTOR y de quienes de ella dependan, incluso el emitir opiniones o difundir juicios sin que signifique necesariamente divulgar información, conforme a lo estipulado en este Acuerdo.

3. Información Confidencial

Para efectos del presente Acuerdo, se entenderá por "**Información Confidencial**" toda información, ya sea oral, escrita o electrónica, que emane directa o indirectamente de y la SUPERINTENDENCIA al CONSULTOR, 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. También será considerada como "Información Confidencial" la existencia y los términos de este Acuerdo y la información o la correspondencia relacionada con el mismo incluyendo la identificación por el nombre o descripción de las partes y no podrá ser divulgada sin el consentimiento de la SUPERINTENDENCIA. Desde ya, se considera confidencial toda la información referida a los sistemas.

Para efectos de este acuerdo **no** se considerará "Información Confidencial" aquella que:

a) Sea de dominio público al momento de suscripción del presente instrumento;

b) Sea obtenida legalmente a través de otra fuente distinta a la SUPERINTENDENCIA, sin obligación de mantenerla confidencial;

c) Sea conocida previamente por el CONSULTOR sin obligación de mantenerla confidencial y ello pueda ser comprobado por instrumentos escritos;

d) Sea expresamente comunicada por escrito y liberada de las obligaciones de confidencialidad impuestas por este contrato, por la SUPERINTENDENCIA.

e) Requiera ser divulgada por razones judiciales, una vez que es debidamente notificado el CONSULTOR, o de conformidad a la normativa legal vigente, o a solicitud de algún órgano contralor que tenga autoridad legal suficiente; siempre y cuando en forma previa el CONSULTOR, haya dado aviso por escrito a la SUPERINTENDENCIA, notificándole dicho requerimiento y éste lo haya autorizado formalmente y por escrito para entregar la información solicitada;

- ✓ Sea desarrollada independientemente por el CONSULTOR, y no diga relación alguna con las relaciones que tiene para con la SUPERINTENDENCIA, y ello pueda ser comprobado con instrumentos escritos.
- ✓ El CONSULTOR afirme que no es Información Confidencial en virtud de las letras a) a la e), antes mencionados, teniendo la obligación de probarlo. Asimismo, la SUPERINTENDENCIA deberá notificar inmediatamente y por escrito al CONSULTOR sobre la existencia de información que afirme no esté cubierta por este Contrato.

4. Acuerdos

En consideración a la calidad de "Información Confidencial" las partes acuerdan:

La SUPERINTENDENCIA, en caso de ser necesario entregará al CONSULTOR información confidencial, la cual éste utilizará sólo con ocasión de los encargos que la SUPERINTENDENCIA le solicite, única y exclusivamente en relación con y para las actividades relacionadas con el diseño de soluciones y/o la prestación de los servicios, y no para otro propósito, sin el consentimiento previo y por escrito de la SUPERINTENDENCIA.

Nombre completo y RUT del profesional, asume la obligación de no revelar ni permitir a nadie revelar la "Información Confidencial" así como a restringir el acceso a ella sólo a sus representantes legales, agentes, empleados, dependientes y/o subcontratistas, que necesariamente deban conocer dicha información, haciéndoles extensivo el deber de reserva y confidencialidad y de velar por el cumplimiento de las obligaciones que asumen personalmente y las que asume el CONSULTOR, para lo cual se suscribe el presente acuerdo que forma parte integrante del Acurdo Complementario entre la SUPERINTENDENCIA y el CONSULTOR en virtud de la ejecución del "Nombre del Proyecto".

5. Responsabilidades

El CONSULTOR responderá a este respecto de la culpa levísima, por sí y por los que de él dependan, por lo que deberá adoptar todas las medidas, dispositivos y procedimientos necesarios para proteger la "Información Confidencial"; y tomar rigurosas precauciones para mantener la confidencialidad de toda la información a la cual pueda tener acceso tanto durante la vigencia de este Acuerdo, como en el futuro, entendiéndose que de modo alguno podrá divulgarla, salvo autorización expresa y por escrito otorgada por la SUPERINTENDENCIA.

6. Prohibiciones

Queda prohibido al CONSULTOR y a sus dependientes, copiar, informar directa o indirectamente, publicar, distribuir, divulgar, por sí o a través de terceros, ni difundir, ni por cualquier procedimiento ceder la "Información Confidencial" o cualquier parte de esta información, a un tercero, ni usar la "Información Confidencial" o alguna parte de ella, salvo autorización previa y por escrito de la SUPERINTENDENCIA. La entrega de cualquier tipo de información al CONSULTOR 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).

Toda la Información permanecerá como propiedad de la SUPERINTENDENCIA y deberá ser devuelta inmediatamente después de la solicitud por escrito al CONSULTOR, o destruida a petición de la SUPERINTENDENCIA. Asimismo, deberá garantizar por escrito a la SUPERINTENDENCIA que dicha información, y todas las copias hechas por cualquier medio que contengan esta "Información Confidencial", han sido destruidas o devueltas.

7. Sanciones

Las partes reconocen que cualquier divulgación que no esté autorizada por la SUPERINTENDECIA, o uso de la "Información Confidencial" no autorizado, podría provocar numerosos y graves perjuicios y/o daños a la SUPERINTENDENCIA. En caso de violación o posible violación de este acuerdo, la SUPERINTENDENCIA tendrá derecho a solicitar, entre otras, medidas precautorias o cualquier otra medida judicial que pueda producir una orden de restricción temporal, impidiendo al CONSULTOR usar o divulgar en forma alguna la "Información Confidencial" u otra medida equivalente que sea necesaria para proteger los intereses de la SUPERINTENDENCIA. El CONSULTOR será responsable de indemnizar, directa, integra y cumplidamente a la SUPERINTENDENCIA de cualquier daño y/o perjuicio, directo y/o indirecto, que resulte de la violación de este acuerdo, incluyendo los honorarios de abogados y todos los costos relacionados con la ejecución forzada de este instrumento. La ausencia del ejercicio de las acciones correspondientes a la SUPERINTENDENCIA, fruto del incumplimiento de este Acuerdo, no podrá entenderse como una renuncia a las mismas, excepto si tal renuncia se notifica por escrito.

La SUPERINTENDENCIA notificará de la violación o posible violación de este acuerdo al CONSULTOR mediante carta certificada enviada al domicilio indicado en la comparecencia. El CONSULTOR adoptará de inmediato las medidas tendientes a evitar o atenuar los efectos dañinos de la violación o posible violación de este acuerdo, quedando responsable de las omisiones en las que incurra, en los términos y alcances establecidos en la cláusula cuarta.

8. Vigencia

Este acuerdo tendrá una vigencia indefinida a partir de la fecha de suscripción del presente instrumento. Por lo anterior, la obligación de reserva y confidencialidad respecto de todos y cada uno de los temas, asuntos y/o negocios abordados conforme a las disposiciones de este Acuerdo se mantendrá plenamente vigente en tanto la SUPERINTENDENCIA no libere a al CONSULTOR de esta obligación mediante comunicación escrita en tal sentido.

En el evento que el CONSULTOR dejare de existir por cualquier causa, las obligaciones establecidas en el presente acuerdo pasarán a sus sucesores legales o sus representantes legales.

9. Domicilio y Personerías

Para todos los efectos derivados del presente instrumento las partes fijan su domicilio en la ciudad y comuna de Santiago y se someten desde ya a la jurisdicción y competencia de sus Tribunales Ordinarios de Justicia.

El nombramiento de don/doña XXXXXXX consta en Decreto N° XXX, de fecha dd de mm de aaaa, del Ministerio de Educación.

La representación legal de Razón Social del Contratista, RUT XX.XXX.XXX-X, a partir de mes del año 20XX en adelante, corresponde a don XXXXXXXX, cédula de identidad XX.XXX.XXX-X, ambos con domicilio en domicilio del contratista, comuna de XXXX, ciudad de XXXX, según consta en el Registro Electrónico de Empresas y Sociedades de fecha dd de mmmm de aaaa y que a la fecha se encuentra vigente.

Nombre del Profesional RUT: XX.XXX.XXX-X Cargo o Función	**Nombre Representante Legal** RUT: XX.XXX.XXX-X **Razón Social Empresa** RUT: XX.XXX.XXX-X