Gobierno de Chile

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON PROVEEDORES, DE LA SUBSECRETARÍA DE EDUCACIÓN.

DGSV/ RVL/BPE

Solicitud N° 1266

MINISTERIO DE EDUCACION
07 MAR 2022
DOCUMENTO TOTALMENTE TRAMITADO

SANTIAGO, 09 de febrero de 2022

RESOLUCIÓN EXENTA N° 1148

VISTO:

Lo dispuesto en la Ley N° 18.956, que Reestructura el Ministerio de Educación; en la Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; en el D.F.L N° 29 de 2004, del Ministerio de Hacienda, que fija el texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en el D.F.L 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; en el Decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en la Ley N° 19.628, sobre Protección de la Vida Privada; en la Ley N° 20.285, sobre Acceso a la Información Pública; en el Decreto N° 779 de 2000 del Ministerio de Justicia, que aprobó el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos; en la Resolución Exenta N° 304 del 07 de diciembre de 2020, Consejo para la Transparencia, que aprueba Recomendaciones sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado; en la Resolución Exenta N°1.540, de 2010, del Servicio de Registro Civil e Identificación relativa al Registro de Datos Personales; en la Resolución Exenta N° 296 de 19 de enero de 2021 que Aprueba la Nueva Política de Seguridad de la Información del Ministerio de Educación y Define las Labores del Órgano Encargado de Velar por su Cumplimiento; en el Decreto Exento N° 1120 de 2018 que Aprueba la Política de Seguridad en la Relación con Proveedores para el Ministerio de Educación; en el Memorándum N° 41 de 2021 del Encargado de Seguridad de Información ; y en la Resolución N° 7, de 2019, de Contraloría General de la República.

CONSIDERANDO:

Que, en conformidad a lo dispuesto en la Ley N°18.956 de 1990, que Reestructura el Ministerio de Educación, esta Cartera es la encargada, entre otras funciones, de fomentar el desarrollo de la educación en todos sus niveles.

Para apoyar su cumplimiento, el Ministerio de Educación, ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y produce el almacenaje de datos, mediante diferentes dispositivos, que permiten interactuar tanto con los funcionarios en todo el país, como con la comunidad escolar y la ciudadanía en general.

En este orden de ideas, mediante la Resolución Exenta N° 296 del 19 de enero de 2021, aprobó "la Nueva Política de Seguridad de la Información" definiendo las labores del órgano encargado de velar por su cumplimiento y estableció la función de Encargado de Seguridad de la Información.

Que, mediante Decreto Exento N° 1120, de 2018, se aprobó la Política de Seguridad en la Relación con Proveedores, para el Ministerio de Educación, y señala que esta será revisada cada tres años, sin perjuicio de que sea evaluada en cualquier momento.

Que, por lo anterior, se hace necesario actualizar la "Política de Seguridad de la Información en la Relación con Proveedores" que tiene como objetivo la protección de la integridad, confidencialidad y disponibilidad de los datos, en la contratación de servicios externos y que de acuerdo con las funciones encomendadas tendrán acceso a los activos de información del Mineduc.

Que, en dicho sentido, este procedimiento es elaborado por el Encargado de Seguridad de la Información, según lo señalado en el Memorándum N° 41, de 2021.

Que, conforme lo anterior, atendida a la normativa vigente y sus disposiciones en esta materia, se hace necesario sancionarlo mediante el presente acto administrativo.

RESUELVO:

1-Apruébase actualización del "Política de Seguridad de la Información en la Relación con Proveedores", de la Subsecretaría de Educación, cuyo texto, y sus anexos, se adjuntan al presente acto y se entienden formar parte integrante del mismo.

2- Déjase constancia, que la "Política de Seguridad en la Relación con Proveedores" aprobada mediante Decreto Exento N° 1120 de 2018 del Ministerio de Educación, será reemplazada por la que se adjunta, en atención a que ha cesado la vigencia de la anterior.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

REPUBLICA DE CHILE
MINISTERIO DE EDUCACIÓN
SUBSECRETARIO

FELIPE SEREY GUERRA
SUBSECRETARIO DE EDUCACIÓN (S)

Distribución:
- Of. Partes
- Gabinete Sr. Ministro
- Gabinete Sr. Subsecretario
- División Jurídica
- División de Planificación y Presupuesto.
- Encargado de Seguridad de la Información.
- Comité de Actos y Contratos- División Jurídica
- Exp. N° 40.321-2022

Gobierno de Chile

Política de Seguridad de la Información en la Relación con Proveedores

Ministerio de Educación

Elaborado por:	Revisado Por:	Aprobado por:
NOMBRE: Juan Antonio Serrano CARGO: Encargado de Seguridad	NOMBRE: Wanda Viera CARGO: Coordinador Nacional de Tecnología	NOMBRE: León Paul CARGO: Presidente Comité de Seguridad de la Información

1.- DECLARACIÓN INSTITUCIONAL.

Esta Secretaría de Estado, en conformidad a lo dispuesto en la Ley N°18.956, que Reestructura el Ministerio de Educación, es la encargada, entre otras funciones, de fomentar el desarrollo de la educación en todos sus niveles

Para apoyar su cumplimiento, el Ministerio de Educación (en adelante e indistintamente Mineduc), ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y se produce el almacenaje de datos, mediante diferentes Activos de Información, que permiten interactuar tanto con los funcionarios en todo el país, como con la comunidad escolar y la ciudadanía en general.

Así, la información que se encuentra en poder de esta Subsecretaría de Educación es un bien estratégico para sus funciones, por lo que se requiere que sea protegida tanto en su obtención, procesamiento, transmisión y almacenamiento. Por lo tanto, el personal que integra la organización será responsable de velar por su confidencialidad, integridad y disponibilidad según lo que su cargo y función le corresponda administrar y gestionar, de conformidad al marco legal actualmente vigente.

En este orden de ideas y, con el fin de apoyar la organización de la seguridad de la información, esta Cartera de Estado modificó mediante la Política de Seguridad de la Información, aprobada por Resolución Exenta N.° 3.862, del 18 de noviembre 2016, de Educación, el Comité de Seguridad de la Información. Por su parte, por la Resolución Exenta N° 4.503, de 11 de julio de 2014, de esta Subsecretaría de Educación, estableció la función de Encargado de Seguridad de la Información.

Luego, este documento define el objetivo y alcance de la Política de Seguridad en la relación con Proveedores de la Subsecretaría de Educación.

2.- OBJETIVO

La presente política tiene como objetivo la protección de la integridad, confidencialidad y disponibilidad de los datos, en la contratación de servicios

externos y que de acuerdo con las funciones encomendadas tendrán acceso a los activos de información del Mineduc.

3.- ALCANCE

La Política de Seguridad en la Relación con Proveedores, considerada como parte del Dominio Relaciones con el proveedor según la Norma NCh ISO 27001:2013, aplica a todos los funcionarios de la Subsecretaria de Educación, ya sean funcionarios de planta, contrata, honorarios y externos que presten servicios a esta Subsecretaria.

Esta política aplica a todas las actividades desarrolladas por personal externo que prestan servicios a esta Subsecretaría o colaboran con ella y que pertenecen a empresas u otros organismos proveedoras de servicios, vinculadas a través de contrato de provisión de servicios requeridos por el Ministerio de Educación gestionados por la División Jurídica.

De igual forma, esta Política como las demás relativas a la seguridad de esta Subsecretaría, es aplicable a todo activo de información que la organización posea actualmente o en el futuro, cubriendo prioritariamente aquéllos que están asociados a procesos de provisión de los productos estratégicos de la institución (Formulario A1 de definiciones estratégicas) o datos personales de la Comunidad Escolar.

4.- DOCUMENTOS RELACIONADOS

- Ley 19.886 de compras públicas.
- Política general de seguridad de la información.

5.- POLÍTICA

5.1 ROLES Y RESPONSABILIDADES

- **Comité de Seguridad de la Información:** Es el encargado de aprobar y sancionar la Política de Seguridad de Seguridad con Proveedores.
- **Encargado(a) de Seguridad de la Información**: Es la persona que coordina mecanismos de control para las medidas desarrolladas en la presente Política.
- **Encargados(as) del Departamento de Compras, División Jurídica y Encargados Jurídicos Regionales:** Dar cumplimiento a lo establecido en esta

política e incluir en los contratos con terceros las respectivas cláusulas de confidencialidad y tratamiento de datos personales según sea el caso.

- **Proveedores y personal externo**: Dar cumplimento a las normas de seguridad descritas en esta política y todas las políticas de seguridad con las que cuenta el Servicio.
- **Funcionarios**: Todos los funcionarios deberán velar que personal externo y proveedores den cumplimiento a las reglas sobre el acceso a la información y a los distintos sistemas, en especial aquellos funcionarios que son requirentes de Servicios de Proveedores.
- **Coordinador(a) Nacional de Tecnología:** Revisar contratos que involucren activos TI que soportan procesos de provisión de productos estratégicos, velando que los lineamientos técnicos de seguridad de la información estén considerados en ellos y que se encuentran indicados en 5.3 del presente documento. Casos especiales de interés son los concernientes al tratamiento de datos personales, monitoreo, ciclo de vida de aplicativos, soporte, administración, datos almacenados y aquellos relacionados con la infraestructura en cualquiera de las etapas de su ciclo de vida.
- **Encargado de cada Área:** Gestionar con la asesoría de la División Jurídica y Encargados Jurídicos Regionales, la inscripción de los bancos de datos personales en el Registro de los Bancos de Datos Personales que lleva el Servicio de Registro Civil e Identificación, de acuerdo con lo señalado en el decreto supremo N° 779 del 2000. Esta actividad es previa al inicio de cualquier tipo de tratamiento de datos.

5.2 PERSONAL EXTERNO.

Toda persona externa que desarrolle labores para el Ministerio de Educación deberá tomar conocimiento de la Política general de Seguridad de la Información y de la o las políticas específicas de seguridad que sean atingentes a las tareas que le han sido encomendadas como es esta misma, las que se encuentran disponibles en la intranet institucional, observando sus directrices y colaborando en su aplicación y cumplimento dentro de su ámbito de acción.

Para estos efectos, el trabajo o proyecto realizado por personal externo, debe ser compatible con los estándares de seguridad establecidos por esta Cartera de Estado.

5.3 INSCRIPCION DE LOS BANCOS DE DATOS PERSONALES

Antes de iniciar cualquier tipo de tratamiento de datos personales y como una etapa previa a la prestación de servicios por parte de organismos externos, se debe realizar la inscripción de las bases de datos relacionadas con el servicio contratado, en el Registro de Banco de Datos Personales a cargo de organismos públicos del Registro Civil.

5.4 PRESTACIÓN DE SERVICIOS EN EL MINISTERIO DE EDUCACIÓN.

Los proveedores que presten servicios sólo podrán desarrollar aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios. De este modo, se entenderá que todas las actividades desarrolladas por personal perteneciente a empresas proveedoras u otras instituciones se encuadran en los contratos de provisión de servicios que vinculan al MINEDUC con los proveedores.

En caso de autorizarse a un tercero (Proveedor u organismo encargado) el acceso a cierta información personal, esta debe hacerse a través de un mandato, que debe contar con las especificaciones establecidas en la Resolución N° 304, de 07 de diciembre de 2020, Consejo para la Transparencia, debiendo otorgarse además por escrito, dejando especial constancia de las condiciones de la utilización de los datos, estableciendo además que dicho mandatario estará obligado a respetar esas estipulaciones en el cumplimiento de su encargo. En estos casos no se entenderá que existe transmisión, comunicación o cesión de datos entre esta Subsecretaría y el encargado.

Las especificaciones mínimas del mandato a otorgar son las siguientes:

a) Que el tratamiento se efectúa a cuenta y riesgo del organismo responsable del tratamiento,

b) Los tipos de datos personales y las condiciones de utilización de los datos,

c) Las medidas de seguridad que se deban adoptar,

d) Las exigencias de confidencialidad de las personas que trabajen en el tratamiento y, en general, de la necesidad de dar cumplimiento a las obligaciones establecidas en la ley N°19.628 y de observar las presentes recomendaciones,

e) El plazo que el encargado conservará los datos y las condiciones para su devolución o eliminación segura e irrevocable. Los órganos públicos deberán adoptar las medidas técnicas y contractuales necesarias para

impedir cualquier procesamiento de datos personales por parte del encargado, una vez terminado el contrato suscrito.

Se deberá incorporar desde el diseño de las bases administrativas y técnicas de los convenios que involucren -o puedan involucrar operaciones de tratamiento de datos personales, las menciones señaladas en los literales anteriores y deberán adoptar las medidas que sean necesarias para el cumplimiento integral de las disposiciones contenidas en el artículo 8° de la ley N°19.628.

La empresa proveedora proporcionará al MINEDUC 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.

De acuerdo con lo establecido en las cláusulas asociadas al contrato de provisión de servicios y en conformidad de con la Ley N° 20.880 sobre la Probidad en la función pública y prevención de los conflictos de intereses, tanto el proveedor como todo el personal externo que desarrolle labores para el MINEDUC deberá cumplir con las directrices definidas en el presente documento y, las políticas de seguridad de la información pertinentes al contrato específico, incluidos los compromisos de confidencialidad, requerimientos de protección de datos personales, los derechos de propiedad intelectual, las condiciones de soporte y mantenimiento si corresponde y las condiciones relativas al cese de sus actividades. En caso de incumplimiento de cualquiera de estas obligaciones, el Servicio se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como las sanciones que se consideren pertinentes en relación con el proveedor o persona contratada y la aplicación de multas según corresponda.

El proveedor deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, así como también en materia de seguridad de la información, para lo cual deberá asegurarse que todo el personal asociado al servicio conoce y se compromete a cumplir las Políticas de Seguridad de la Información del MINEDUC.

Cualquier tipo de intercambio de información que se produzca entre el MINEDUC y los proveedores 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 para otros fines diferentes a los asociados a dichos documentos.

En el caso de que ocurra un incidente que afecte a activos de información del Ministerio, el proveedor deberá notificarlo y colaborar en las acciones de remediación.

El proveedor deberá tener implementados mecanismos o estrategias que permitan una adecuada protección de los activos relacionados al servicio, así como detección de anomalías y eventos, respuesta, recuperación y resiliencia para la continuidad del servicio sobre todo para el caso de productos considerados estratégicos del Ministerio o que involucren datos de la Comunidad Escolar.

Condiciones de resguardo en los casos de disolución o cese de actividades por parte del proveedor o de la eventual cesación de los servicios de soporte y mantenimiento, en especial si el servicio se presta a través de infraestructura en la nube.

En los contratos se deben dejar reflejados los riesgos que representa la participación de proveedores y terceros como es el caso de afectación a la confidencialidad, integridad y disponibilidad de datos ministeriales o de la Comunidad Escolar, así como el detalle de las distintas medidas de seguridad que se implementarán en relación con el uso y trasmisión de los datos.

5.5 MEDIDAS DE SEGURIDAD

Se deben adoptar las medidas mínimas de seguridad descritas más adelante, las que deberán quedar explícitas en los contratos:

- Garantizar en todo momento la seguridad de la información, mediante sistemas informáticos actualizados y protegidos.
- Incorporar procedimientos para la prevención de filtraciones y accesos indebidos; y la definición de perfiles de acceso a los bancos de datos.
- Informar a los titulares de datos sensibles, de las eventuales brechas de seguridad que pudieran ocurrir, de las posibles consecuencias de estas vulneraciones y de las medidas de solución o resguardo adoptadas.
- En aquellos casos en que los datos recolectados sean comunicados o transmitidos a terceras personas, naturales o jurídicas, se recomienda la adopción de medidas de encriptación, a efectos de asegurar la integridad y confidencialidad de los datos entre remitente y destinatario.

El personal externo que tenga acceso a información del MINEDUC deberá velar por la confidencialidad de los datos.

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.

El proveedor deberá minimizar el número de informes en formato papel que contengan información confidencial y estos documentos deben mantenerse en un lugar seguro y fuera del alcance de terceros.

El representante legal así como el personal externo deberá firmar un acuerdo de no divulgación en el caso que deba acceder, por su labor, a información confidencial del Servicio.

5.6 PROPIEDAD INTELECTUAL

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

Queda estrictamente prohibido el uso de programas informáticos que no cuenten con licencia.

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 del MINEDUC.

5.7 USO APROPIADO DE LOS RECURSOS

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

Los recursos que el MINEDUC 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. El Ministerio se reserva el derecho de auditar los procesos y los controles del proveedor relacionados al acuerdo o contrato.

Se deberán restituir al MINEDUC todos los activos físicos y los activos de información antes de la finalización del contrato.

6. VIGENCIA

Esta norma entrará en vigor cuando el documento esté totalmente tramitado.

Las revisiones de la presente Política se realizarán cada tres años, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad del Servicio. Todo el personal de la Subsecretaría de Educación deberá tomar

conocimiento por escrito de la presente política, la cual se encontrará en formato electrónico en la Intranet para futuras consultas.

7. LEGISLACIÓN VIGENTE

- Ley N° 20.880, sobre Probidad en la función pública y prevención de los conflictos de intereses.
- Ley N° 17.336, de Propiedad Intelectual, y sus actualizaciones
- Ley N° 19.223, que Tipifica Figuras penales relativas a la Informática.
- D.F.L. N° 29 de 2004, que fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo.
- Ley N° 19.628, sobre Protección de la Vida Privada.
- Ley N° 19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.
- Ley N° 20.285, sobre Acceso a la Información Pública.
- Decreto Supremo N° 83 del 2005 Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Decreto Supremo N° 93 del 2006 Ministerio Secretaría General de la Presidencia, que aprueba Norma Técnica para la Adopción de Medidas Destinadas a Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos Masivos no Solicitados Recibidos en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus funcionarios.
- Decreto supremo N° 779 de 2000 del Ministerio de Justicia, que aprobó el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos.
- Norma Chilena NCh-ISO27001:2013 sobre "Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos".
- Rex N° 304 del 07 de diciembre de 2020, Consejo para la transparencia que aprueba Recomendaciones sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado.
- Rex (E) N°1.540, de 2010, del Servicio de Registro Civil e Identificación relativa al Registro de Datos Personales.

8. ACCIONES DISCIPLINARIAS

La infracción a las obligaciones establecidas en este documento eventualmente podría constituir una violación al principio de probidad administrativa, en cuyo caso será sancionada en conformidad a lo dispuesto en el D.F.L. N° 29, de 2004, del Ministerio de Hacienda, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo. Lo anterior, sin perjuicio de la responsabilidad civil o penal que pudiera concurrir.

Por su parte y, respecto del personal a Honorarios o de carácter externo a Mineduc, la infracción a las obligaciones materia del presente instructivo podría, eventualmente, constituir una infracción a su respectivo contrato, acarreando las consecuencias jurídicas del caso.

9. GLOSARIO DE TÉRMINOS

Para los propósitos de esta Política, las siguientes palabras se entenderán en el sentido que a continuación se indica:

- Confidencialidad: garantía de que accedan a la información sólo aquellas personas autorizadas a hacerlo.
- Disponibilidad: derecho de los usuarios autorizados a tener a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- Integridad: Mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.