Gobierno de Chile

MINEDUC JEFE DIVISIÓN JURÍDICA L/BPE

APRUEBA POLÍTICA DE SEGURIDAD DE INTERCAMBIO DE INFORMACIÓN CON TERCEROS, DE LA SUBSECRETARÍA DE EDUCACIÓN.

Solicitud N° 1295

SANTIAGO, 15 FEB 2022

MINISTERIO DE EDUCACION
07 MAR 2022
DOCUMENTO TOTALMENTE TRAMITADO

RESOLUCIÓN EXENTA N° 1171

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 la 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° 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° 1126 de 2018 que Aprueba la Política de Intercambio de Información con Terceros Para el Ministerio de Educación; en el Memorándum N° 40 de 16 de noviembre 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.

Que, mediante la Resolución Exenta N° 296 del 19 de enero de 2021, se 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, en la Política de Seguridad de Intercambio con Terceros para el Ministerio de Educación, aprobada mediante Decreto Exento N° 1126, de 2018, se 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 Intercambio de Información con Terceros que tiene como objetivo, la protección de la integridad, confidencialidad y disponibilidad de los datos, en el intercambio de información entre el Ministerio de Educación y terceras partes, teniendo en cuenta la adecuada protección de los datos según normativa vigente.

Que, en dicho sentido, este procedimiento es elaborado por el Encargado de Seguridad de la Información, según lo señalado en el Memorándum N° 40, de 2021.

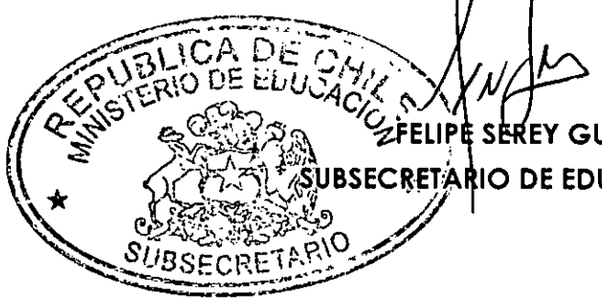
Que, conforme lo anterior, atendida a la normativa vigente y sus disposiciones en esta materia, se hace necesario sancionarla mediante el presente acto administrativo.

RESUELVO:

1.- **Apruébase** la actualización de la "Política de Seguridad de Intercambio de Información con Terceros" de la Subsecretaría de Educación, cuyo texto y sus anexos, se adjuntan al presente acto y se entienden forman parte integrante del mismo.

2.- **Déjase constancia**, que la "Política de Seguridad de Intercambio de Información con Terceros" aprobada mediante Decreto Exento N° 1126 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



FELIPE SEREY GUERRA
SUBSECRETARIO DE EDUCACIÓN (S)

Distribución:
- Of. Partes
- Gabinete Sr. Ministro
- Gabinete Sr. Subsecretario
- División Jurídica
- División de Planificación y Presupuesto.
- Comité de Convenios- División Jurídica
- Exp. N° 40.314-2021

Política de Seguridad de Intercambio de Información con Terceros

Ministerio de Educación

Elaborado por: NOMBRE: Juan Antonio Serrano CARGO: Encargado de Seguridad de la Información	Revisado Por: NOMBRE: Wanda Viera Andrade CARGO: Coordinador Nacional de Tecnología	Aprobado por: NOMBRE: León Paul Castro 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 almacenamiento 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 este Ministerio 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 aprobó la nueva Política de Seguridad de la Información del Ministerio de Educación, a través de Resolución Exenta N° 296, del 19 de enero de 2021. Por su parte, por la Resolución Exenta N° 4.503, de 11 de julio de 2014, de la 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 de Intercambio de Información con Terceros del Ministerio de Educación.

2.- OBJETIVO

La presente política tiene como objetivo la protección de la integridad, confidencialidad y disponibilidad de los datos, en el intercambio de información entre el Ministerio de Educación y terceras partes, teniendo en cuenta la adecuada protección de los datos según normativa vigente.

3.- ALCANCE

La Política de Seguridad de Intercambio de Información con Terceros, considerada como parte del Dominio Seguridad en la Comunicaciones según la Norma NCh ISO 27001:2013, aplica a todos los usuarios internos (funcionarios(as) y prestadores de servicios a honorarios) del Ministerio de Educación y usuarios externos que presten servicios a esta Secretaría de Estado.

Esta política aplica sobre la información digital contenida en las bases de datos del Ministerio de Educación, que requiera ser entregada a terceros.

De igual forma, esta Política como las demás relativas a la seguridad de este Ministerio, 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 aquellos que involucren el manejo de datos personales de clientes, usuarios y beneficiarios del Ministerio o de la comunidad escolar en general.

4.- DOCUMENTOS RELACIONADOS

- Política de Seguridad de la Información y define las labores del órgano encargado de velar por su cumplimiento.
- Política de Seguridad en relación con proveedores.
- Política de Privacidad y Protección de datos personales.
- Política de seguridad de correo electrónico.

5.- POLÍTICA

5.1 ROLES Y RESPONSABILIDADES

- **Comité de Seguridad de la Información:** Es el órgano encargado de proponer la aprobación, promoción y control de cumplimiento de la Política de Seguridad de Intercambio de Información con Terceros.
- **Coordinador(a) Nacional de Tecnología:** Es el encargado de firmar electrónicamente la información a ser transferida o quien él designe.
- **Encargado(a) de Seguridad de la Información:** Es el responsable de mantener actualizada la presente política, controlar su implementación y velar por su correcta aplicación.
- **Contraparte técnica de la entidad que requiere información:** Responsable de colaborar en la preparación del convenio según se le requiera, así como también velar por su cumplimiento en el ámbito de sus funciones.

- **Encargado(a) de Gestión de datos**: Es el responsable de obtener o generar la información requerida por terceros, desde las bases de datos institucionales.
- **División Jurídica y Encargados Jurídicos Regionales:** Dar cumplimiento a lo establecido en esta política, e incluir en los convenios de intercambio de información las respectivas cláusulas de confidencialidad y tratamiento de datos personales según sea el caso.
- **Coordinador(a) Nacional de Tecnología:** Es el encargado de firmar electrónicamente la información a ser transferida o quien él designe. Debe velar por la aplicación de las medidas de seguridad y normas técnicas señaladas en los convenios.
- **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 CONDICIONES PARA CURSAR UN REQUERIMIENTO DE INFORMACIÓN Y CONVENIO.

La solicitud de intercambio de información puede originarse por requerimiento de un organismo externo que necesite el dato o información, por disposiciones legales o cumplimiento de su misión.

Para el caso del tratamiento de datos personales el requirente deberá contar con habilitación legal expresa en las normas que regulan su funcionamiento, establezcan sus competencias o determinen sus funciones especiales. En aquellos casos donde no exista tal regla expresa, el tratamiento de datos personales sensibles podría basar su habilitación legal en la regla general del artículo 20 de la ley N°19.628, si y solo si el tratamiento de esta categoría especial de datos resulta imprescindible para el debido cumplimiento de su función pública. En todo caso el receptor sólo podrá utilizar los datos personales para los fines que motivaron la transmisión.

El procedimiento para cursar un requerimiento considera las siguientes etapas:

- Inscripción de las Bases de Datos en el registro de Banco de Datos Personales a cargo de organismos públicos, actividad que es preliminar a toda otra acción relacionada.
- Requerimiento expreso.

- Admisibilidad de éste.
- Suscripción del convenio respectivo.

En el caso de que un tercero, ya sea proveedor u organismo encargado, requiera acceder a cierta información personal, esta debe hacerse siguiendo los lineamientos contenidos en las Políticas de Seguridad de la Información vigentes.

Dicho convenio debe ser aprobado por las autoridades correspondientes de cada servicio y debe incluir cláusulas de responsabilidad, deberes y derechos. Se debe velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Asimismo, se deben especificar las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de esta.

Además, debe establecer de manera explícita las contrapartes técnicas de ambas instituciones, que deben coordinarse para la adecuada operación del Convenio.

En el caso que el requerimiento origine una respuesta por una única vez, la respuesta debe ser proporcionada a través de un Oficio.

5.3 INSCRIPCION DE LOS BANCOS DE DATOS PERSONALES

Antes de iniciar cualquier tipo de tratamiento de datos y como una etapa previa al intercambio de bases de datos con otros organismos, 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 REQUERIMIENTO EXPRESO

Las solicitudes de acceso a información contenida en los bancos de datos de la Subsecretaría de Educación deben tener las siguientes características:

- La individualización del requirente, el que puede ser un organismo público o privado, con indicación expresa de la habilitación legal para el tratamiento que invoque. En el caso de los organismos públicos, deberán identificar la función legal específica que se está ejecutando y que requiere de la comunicación o transferencia de datos personales.
- El motivo y el propósito del requerimiento, con indicación expresa del tratamiento de datos que se busque efectuar y la finalidad del mismo.
- El tipo de datos que se desea transmitir, con indicación expresa de la pertinencia o necesidad de los datos solicitados en relación con las finalidades informadas.

5.5 ADMISIBILIDAD DEL REQUERIMIENTO

La admisibilidad del requerimiento será evaluada por el Mineduc, verificando que la comunicación guarde relación con sus tareas o finalidades, es decir, que se encuentra dentro del ámbito de sus competencias, y estableciendo los requisitos necesarios para el resguardo de los derechos de protección de datos en el convenio respectivo.

5.6 SUSCRIPCIÓN DEL CONVENIO RESPECTIVO.

En relación con la implementación de un Convenio de comunicación o transmisión, se dejará constancia en él de aspectos tales como la transmisión, la fecha, el motivo y propósito de la misma, los requisitos específicos para la protección de los datos personales transmitidos, y la obligación del solicitante de utilizar los datos personales sólo para los fines que motivaron la transmisión. El Convenio se entenderá aprobado una vez que se encuentre totalmente tramitado él o los correspondientes actos administrativos de aprobación, según se trate de uno o más órganos públicos. Aspectos mínimos que el convenio debe contener son:

- Identificación del órgano público que transmite los datos y del destinatario de estos.
- Identificación del banco de datos, según la denominación dada en la inscripción efectuada en el Registro de Bancos de Datos Personales a cargo de Organismos Públicos.
- Las medidas de seguridad que deberán adoptar tanto el que transmite los datos como el destinatario de estos durante todo el procedimiento de transmisión y posterior tratamiento de los datos por este último.
- La indicación de que el receptor de los datos tendrá la calidad de responsable del tratamiento, estando sometido a las mismas obligaciones, multas y responsabilidad de indemnizar en caso de tratamiento indebido de los datos, que el órgano público que efectuó la transmisión.
- El procedimiento para efectuar el aviso a que se refiere el artículo 12, inciso final, de la ley N°19.628, en caso de que se ejerza ante cualquiera de los responsables de la base de datos comunicada los derechos de modificación, cancelación o bloqueo, adoptando las medidas de trazabilidad que correspondan.
- El plazo que el destinatario conservará los datos transmitidos, y
- Los cursos de acción que deberá seguir el destinatario una vez que haya efectuado el tratamiento que motivó la transmisión, ya sea que se acuerde

la destrucción o devolución del banco de datos al transmisor y de cualquier otro soporte donde consten los datos objeto de la comunicación.

En caso de autorizarse en el convenio indicado a alguna de las partes, el acceso a cierta información personal a un tercero (Proveedor u organismo encargado), se debe indicar expresamente en este, que se debe realizar 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.

Se establece además que no serán aplicables las directrices de este numeral a los convenios o contratos celebrados entre órganos o servicios públicos y particulares cuando este último tenga la calidad de encargado del tratamiento, esto es, cuando actúa bajo las instrucciones del organismo responsable del tratamiento, caso en el cual, deberá estarse a las exigencias contempladas en el mandato, considerando lineamiento de la Política de Seguridad en relación con Proveedores y la Política de Privacidad y Protección de los Datos Personales.

Así mismo, tampoco serán aplicables las directrices de este numeral, a las comunicaciones o transferencias de datos personales que se realicen de conformidad a lo dispuesto en el artículo 24 bis de la ley N°19.880, sobre remisión electrónica de documentos o información entre organismos públicos para la sustanciación de un procedimiento administrativo electrónico.

5.7 MEDIDAS DE SEGURIDAD EN LA ENTREGA DE INFORMACIÓN Y NORMAS TÉCNICAS

Todo intercambio de información electrónica reservada o confidencial de la Institución con terceras partes, debe cumplir con las siguientes medidas de seguridad y las normas técnicas que para estos efectos se encuentren vigentes, especialmente aquellas contenidas en el Decreto Supremo N°14/2014 del Ministerio de Economía.

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

- 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.

Además:

- La información que se transfiera por vía de mensajería electrónica será efectuada a través de la plataforma de correo electrónico institucional, regulada por la "Política de Seguridad de Correo Electrónico".
- No está permitido el envío de bases de datos personales por medio de correo electrónico. En caso de que sea estrictamente necesario enviarlo a través de este medio, se deberá utilizar un método de cifrado que resguarde la confidencialidad de los datos y firma electrónica avanzada para asegurar la integridad de estos.
- En caso de utilización de otros medios electrónicos (ssh, sftp, vpn y otros) la transferencia deberá ser efectuada utilizando canales seguros, precisando su origen y destino, donde la criptografía empleada se sustente en algoritmos robustos y fuertes.
- En general, cada vez que sea necesario entregar datos personales o sensibles, estos deben ir siempre cifrados, independientemente del soporte a través del cual se entregue.
- La Coordinación Nacional de Tecnologías entregará las orientaciones necesarias a través de los procedimientos o guías técnicas correspondientes.

5.8 SITUACIONES PARTICULARES.

Existen otras situaciones que obligan al Ministerio a hacer entrega de información a terceros, tales como:

- Solicitudes de información por Ley de Transparencia
- Requerimientos del Poder Judicial

En dichos casos se procederá según los procedimientos que establezca la División Jurídica junto con las áreas específicas del Ministerio que participan de la gestión del requerimiento.

Otra situación especial es respecto a información sobre la cual el Ministerio no es propietario pero que es obtenida a través de un convenio de intercambio de información vigente con otro organismo y que es demanda por un tercero. En este

caso, solo es posible entregarla al tercero si el organismo propietario de la información lo autoriza expresamente.

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 del Ministerio 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° 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° 14 del 2014 Ministerio de Economía, Fomento y Reconstrucción que Modifica Decreto N° 181, de 2002, que aprueba reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica,
- 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° 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: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- Disponibilidad: propiedad de que la información sea accesible y utilizable toda vez que lo requiera una entidad autorizada.

- Integridad: propiedad relativa a la exactitud y totalidad de la información.