MINISTERIO DE EDUCACIÓN
13 FEB 2026
DOCUMENTO TOTALMENTE TRAMITADO

Gobierno de Chile

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON PROVEEDORES, DEL MINISTERIO DE EDUCACIÓN

Solicitud N° 1252

SANTIAGO, 13 FEB 2026

RESOLUCIÓN EXENTA N° 677

VISTO:

Lo dispuesto 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 del Estado; en el D.F.L. N° 29 de 2004, que Fija el texto Refundido, Coordinado y Sistematizado de la Ley N.° 18.834, sobre Estatuto Administrativo; en la Ley N° 18.956, que Reestructura el Ministerio de Educación; en la Ley N° 19.628, sobre Protección de la Vida Privada; 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 la Ley N° 20.285, sobre Acceso a la Información Pública; en la Ley N° 21.180, sobre Transformación Digital del Estado; en la Ley N° 21.459, que establece Normas sobre Delitos Informáticos, deroga la Ley N.° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest; en la Ley 21.663 Marco sobre Ciberseguridad; en el 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; 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 el Decreto N° 7, de 2023, del Ministerio Secretaría General de la Presidencia, que Establece Norma técnica de Seguridad de la Información y Ciberseguridad conforme la Ley N° 21.180; en la Resolución Exenta N° 304, de 2020, del 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° 1.148, de 2022, del Ministerio de Educación, que Aprueba la Política de Seguridad de la Información en la Relación con los Proveedores; en la Resolución Exenta N° 2.693, de 2023, del Ministerio de Educación, que Aprueba Política de Seguridad de la Información del Ministerio de Educación y Define las Labores del Órgano Encargado de Velar por su

Cumplimiento; en la Resolución Exenta N° 4.877, de 2024, del Ministerio de Educación, que Designa a Responsable Institucional de Seguridad de la Información y Ciberseguridad y a Responsable Institucional de Activos de la Información; en el Memorándum N° 17 de 2023, del Encargado de Seguridad de la Información; y, en la Resolución N° 36, de 2024, de la Contraloría General de la República.

CONSIDERANDO:

Que, esta Secretaría de Estado, en conformidad a lo dispuesto en el artículo 1, de la Ley N° 18.956, que Reestructura el Ministerio de Educación (Mineduc), tiene a su cargo entre otras funciones, el fomentar el desarrollo de la educación en todos sus niveles.

Que, el referido cuerpo legal en su artículo 5 establece que la Subsecretaría de Educación es el órgano de colaboración directa del (de la) Ministro(a), y le corresponderá, en general, la administración interna del Ministerio y la coordinación de los órganos y servicios públicos del sector, y el cumplimiento de las demás funciones que en materias de su competencia le encomiende la ley y el (la) Ministro(a). Por su parte, el inciso primero del artículo 6 indica que el (la) Subsecretario(a) es el (la) colaborador(a) inmediato(a) del (de la) Ministro(a) y el (la) Jefe(a) Administrativo del Ministerio, teniendo a su cargo la coordinación de las Subsecretarías que componen el Ministerio.

Que, con la finalidad de cumplir esas funciones, la Subsecretaría de Educación ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes activos, que permiten interactuar con la comunidad escolar, ciudadanía en general y los integrantes de esta repartición en todo el país, para dar cumplimiento a las funciones que el mandato legal exige, considerando que la información resguardada puede ser propia de los sistemas de esta Cartera de Estado, de los servicios o sus procesos, así como también de los usuarios internos o externos.

Que, por su parte, estos datos son un bien estratégico para sus funciones, por lo que se requiere que sean protegidos tanto en su obtención, procesamiento, transmisión y almacenamiento, deber que incluye al personal que integra la organización, el que será responsable de velar por su confidencialidad, integridad y disponibilidad según lo que su cargo y función le corresponda.

Que, asimismo, esta Cartera de Estado debe velar por la regulación respecto del desarrollo de aplicativos, así como también a cualesquiera de las relaciones con terceros que implique el acceso a los datos, utilización de recursos, o instalación, configuración o actualización de aplicativos de software.

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

RESUELVO:

I. **APRUÉBASE** la Política de Seguridad de la Información en la Relación con Proveedores, del Ministerio de Educación, cuyo texto es el siguiente:

1.- DECLARACIÓN INSTITUCIONAL

El Ministerio de Educación (MINEDUC), en conformidad a lo dispuesto en la Ley N° 18.956, que lo reestructura, es la Secretaría de Estado encargada, entre otras funciones, de fomentar el desarrollo de la educación en todos sus niveles. Por su parte, la Subsecretaría de Educación es el órgano de colaboración directa del (de la) Ministro(a), y le corresponderá, en general, la administración interna del Ministerio, correspondiéndole así al (a la) Subsecretario(a) ser el (la) Jefe(a) Administrativo de la Cartera de Estado en comento.

Para apoyar el cumplimiento de sus deberes, ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes activos, los que permiten el trabajo conjunto de los funcionarios en todo el país, su interacción con la comunidad escolar y con la ciudadanía en general, en aras del cumplimiento de las funciones que le han sido encomendadas y le competen.

Así, los datos que se encuentran en poder de esta repartición pública es un bien estratégico para sus funciones, por lo que se requiere que sea protegida tanto en su obtención, como en sus procesamientos, transmisión y almacenamiento. Por lo tanto, el personal que integra la organización será responsable de velar por su confidencialidad, integridad y disponibilidad de acuerdo con lo que según 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 la Resolución Exenta N° 2.693, de 2023, del Ministerio de Educación, que Aprueba Política de Seguridad de la Información del Ministerio de Educación y Define las Labores del Órgano Encargado de Velar por su Cumplimiento.

En ese contexto, y acorde al lineamiento que deriva de la Política de Seguridad de la Información antes referida, se establece por este acto administrativo la Política de Seguridad de la Información en la Relación con Proveedores.

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, en consideración al Anexo A, Tabla A.1. sección A.15 "Relaciones con el proveedor" de la Norma NCh ISO 27001:2013, aplica a todos(as) los(as) funcionarios(as) del Ministerio de Educación, ya sean funcionarios(as) de planta, contrata, honorarios y externos que presten servicios a este Ministerio.

Esta Política aplica a todas las actividades desarrolladas por personal externo que prestan servicios a este Ministerio 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 y gestionados por la División Jurídica.

Asimismo, como las demás políticas 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 datos personales de la Comunidad Escolar.

4.- DOCUMENTOS RELACIONADOS

a) Ley N° 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.
b) Política de Seguridad de la Información y Organización de la Seguridad.
c) Política de Clasificación y Manejo de la Información.
d) Política de Control de Acceso Lógico.
e) Política de Seguridad en Adquisición, Desarrollo y Mantenimiento de Sistemas.

5.- POLÍTICA

5.1. ROLES Y RESPONSABILIDADES

5.1.1. Encargado(a) de Seguridad de la Información

Es la persona responsable de mantener actualizada la presente política, controlar su implementación y velar por su correcta aplicación.

5.1.2. Coordinador(a) Nacional de Tecnología

Es la persona responsable de implementar o exigir la implementación, según sea el caso, de la presente política en todos los procesos tecnológicos que estén bajo su responsabilidad. Casos especiales de interés son los concernientes al tratamiento de datos personales, monitoreo, ciclo de vida de aplicativos, soporte, administración, datos almacenados, gestión de incidentes y aquellos que incorporen componentes tecnológicos en el servicio, en cualquiera de las etapas de su ejecución.

5.1.3. Encargados(as) del Departamento de Compras, División Jurídica y Encargados(as) Jurídicos Regionales:

Son las personas responsables de solicitar el cumplimiento de lo establecido en esta Política, en particular en lo relativo a la posibilidad de incluir en los contratos con terceros las respectivas cláusulas de confidencialidad y tratamiento de datos personales. En el caso de los proveedores de servicios de tecnología, deben cumplir con compartir la exigencia de la información sobre las amenazas y vulnerabilidades que puedan afectar a las redes, plataformas y sistemas informáticos, de los órganos de la administración del Estado, las medidas de mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados según normativa vigente, lo que podrá ser incorporado en los contratos. Además, en el caso de los prestadores de servicios relacionados con infraestructura central o información crítica que presten servicios fuera del territorio nacional, se debe considerar para la evaluación o contratación la condición de suscripción del país al Convenio de Budapest.

5.1.4. Funcionarios(as) y personal externo que preste servicios

Toda persona que se relacione con esta Cartera de Estado, sean estos funcionarios(as) de planta, contrata, honorarios y/o externos que presten servicios, quienes deben dar cumplimiento a lo estipulado en esta Política.

5.1.5. Encargado(a) de cada área

Es la persona responsable de gestionar, con la asesoría de la División Jurídica y los(as) Encargados(as) 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, de 2000. Esta actividad es previa al inicio de cualquier tipo de tratamiento de datos.

5.2 LINEAMIENTOS

5.2.1 PERSONAL EXTERNO

Toda persona externa que desarrolle labores para el Ministerio de Educación deberá tomar conocimiento de la Política de Seguridad de la Información y Organización de la Seguridad y de la o las políticas específicas de seguridad que sean atingentes a las tareas que le han sido encomendadas, 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.
Toda área ministerial que contrate servicios tecnológicos externos debe tener un listado de proveedores vigentes.

5.2.2. INSCRIPCIÓN 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, en el caso de que una o varias bases de datos relacionadas con la prestación del servicio contratado, no se encuentre(n) inscrita(s) en el Registro del Banco de Datos Personales a cargo de organismos públicos del Servicio de Registro Civil e Identificación, se debe realizar la inscripción de esta(s) base(s) de datos.

5.2.3. 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 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, del 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 este Ministerio 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, observando las presentes recomendaciones.
e) El plazo que el (la) encargado(a) 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, adoptando 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 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 con lo dispuesto en el artículo 2 bis de la Ley 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios, 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.
El proveedor deberá comprometer condiciones de resguardo para 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. Asimismo, deberá informar el detalle de las diferentes medidas para controlar 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. Estas consideraciones podrán ser incluidas en el contrato.

5.2.4. MEDIDAS DE SEGURIDAD

Se deben adoptar las medidas mínimas de seguridad descritas más adelante, las que deberán ser informadas formalmente por los proveedores y podrán quedar explícitas en los contratos:

a) Garantizar en todo momento la seguridad de la información, mediante sistemas tecnológicos actualizados y protegidos.
b) Incorporar procedimientos para la prevención de filtraciones y accesos indebidos; y la definición de perfiles de acceso a los bancos de datos.
c) 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.

d) En aquellos casos en que los datos recolectados sean comunicados o transmitidos a terceras personas, naturales o jurídicas, se deben utilizar contenedores ministeriales o bien medidas de encriptación, a efectos de asegurar la integridad y confidencialidad de los datos entre remitente y destinatario.

e) Los productos o servicios resultantes deberán ser revisados con el procedimiento vigente antes de entrar en operación.

f) En el caso de que se adquieran sistemas o productos tecnológicos, ya sea de hardware o de software, se debe considerar también la adquisición de mecanismos de actualización en el tiempo para estos productos, tal como parches o cambios de versión.

g) Deben estar claramente definidas las exigencias de los niveles de servicios requeridos.

h) 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.

i) 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 personales.

j) Los proveedores de servicios de tecnologías deberán compartir en forma obligatoria información sobre las amenazas y vulnerabilidades que puedan afectar a las redes, plataformas y sistemas de los órganos de la administración del Estado, al igual que las medidas de mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados.

k) 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.

l) 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.

m) El representante legal, así como el personal externo, deberá firmar un acuerdo de confidencialidad en el caso que deba acceder, por su labor, a información crítica del Servicio. Asimismo, el personal externo que tenga acceso a información del MINEDUC deberá velar por la confidencialidad de los datos.

n) Los accesos y datos proporcionados deben ser restituidos y no pueden ser utilizados de ninguna forma posteriormente al término del servicio contratado.

5.2.5. 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.

5.2.6. 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, etcétera), 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 del Ministerio de Educación deberá tomar conocimiento por escrito de la presente Política, la cual se encontrará disponible en formato electrónico en la Intranet de la institución para futuras consultas.

7. LEGISLACIÓN VIGENTE

a) Ley N.° 17.336, de Propiedad Intelectual, y sus actualizaciones.
b) Ley N° 19.628, sobre Protección de la Vida Privada.
c) Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma.

d) Ley N° 20.285, sobre Acceso a la Información Pública.
e) Ley N° 20.880, sobre Probidad en la función pública y prevención de los conflictos de intereses.
f) Ley N° 21.180, sobre Transformación Digital del Estado.
g) Ley N° 21.459, que establece Normas sobre Delitos Informáticos, deroga la Ley N.° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
h) Ley 21.663 Marco sobre Ciberseguridad.
i) D.F.L. N° 29 de 2004, que fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo.
j) 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.
k) Decreto N° 273 de 2022, del Ministerio del Interior y Seguridad Pública, que establece obligación de reportar incidentes de ciberseguridad.
l) Decreto Supremo 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.
m) Decreto Supremo N° 93 de 2006, del 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.
n) Decreto N° 7, de 2023 Ministerio Secretaría General de la Presidencia, que establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme la Ley N° 21.180.
o) Norma Chilena NCh-ISO27001:2013 sobre "Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos".
p) Resolución Exenta N° 304 de 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.
q) Resolución Exenta 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, respecto de los dependientes que detentan la calidad de funcionarios públicos, ya sea Titulares o a Contrata, 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 podrá constituir causal suficiente para producir el término inmediato y anticipado del respectivo contrato que los vincule con el Ministerio, de acuerdo a lo que dicho contrato establezca, sin perjuicio de otras responsabilidades civiles o penales que la infracción pudiere irrogarles.

9. GLOSARIO DE TÉRMINOS

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

a) Activo: Cualquier elemento que tenga valor para la organización. Para el ámbito de seguridad de la información, se puede clasificar en:

   a.1) Activos de Información: Se entenderá por Activo de Información todo elemento en que se registre, en que se almacene y/o procese datos e información, sea a través de medios tecnológicos o no, tales como: bases de datos y archivos, contratos y acuerdos, documentación de sistema, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, plan de continuidad de negocio, información de auditorías, información archivada, activos de software, activos físicos y servicios.

   a.2) Activos de Software: Constituidos por las aplicaciones de software, sistemas, herramientas de desarrollo y utilidades.

   a.3) Activos Físicos: Constituidos por el equipamiento computacional, equipamiento de comunicaciones, medios móviles y otros equipamientos.

b) Confidencialidad: Garantía de que accedan a la información sólo aquellas personas autorizadas a hacerlo.

c) Disponibilidad: Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

d) Integridad: Mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.

e) Nivel de servicio: En un acuerdo o contrato, el nivel de servicio expresa en forma objetiva la(s) necesidad(es) del cliente o contratante, por ejemplo: el periodo de tiempo que debe transcurrir para que el soporte de la empresa responda y solucione un incidente según su tipificación, o el porcentaje aceptable de fallas en un periodo de tiempo. El nivel de servicio que se solicita en un contrato está condicionado por el costo para alcanzarlo.

f) Parche: Cambio que se aplica a un programa para corregir errores, aplicar actualizaciones, eliminar secciones o corregir vulnerabilidades.

II. **DÉJASE** sin efecto la Resolución Exenta N° 1.148 de 2022, del Ministerio de Educación, que Aprobó la "Política de Seguridad de la Información en la Relación con los Proveedores", a contar de la fecha del presente acto administrativo.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

ALEJANDRA ARRATIA MARTÍNEZ
SUBSECRETARIA DE EDUCACIÓN

Distribución:
- Gabinete Sr. Ministro
- Gabinete Sra. Subsecretaria de Educación
- Encargado de Seguridad de la Información
- División Jurídica
- Oficina de Partes y Archivos.
- Archivo.

Expediente N.° 32.823-2023