MINISTERIO DE EDUCACION
10 JUN 2024
DOCUMENTO TOTALMENTE TRAMITADO

13

Ministerio de Educación
Gobierno de Chile

JVG/VAM/KGR/PTM

APRUEBA POLÍTICA DE SEGURIDAD EN EL DESARROLLO Y MANTENCIÓN DE SISTEMAS PARA EL MINISTERIO DE EDUCACIÓN

Solicitud N° 4486

SANTIAGO, - 3 JUN 2024

RESOLUCIÓN EXENTA N° 4678

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 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, que fija el texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; 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° 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° 5.773, de 2021, del Ministerio de Educación, que Aprueba Política de Seguridad en el Desarrollo y Mantención de Sistemas para el Ministerio de Educación; y, en las Resoluciones N°s 6 y 7, de 2019, 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 Ministro, 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 encomienda 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 en el Desarrollo y Mantención de Sistemas para el Ministerio de Educación:

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 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 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 en el Desarrollo y Mantención de Sistemas.

2. OBJETIVO

La presente política tiene por objetivo definir un marco estándar para garantizar la protección de la información del Ministerio de Educación, orientado a las actividades de adquisición, desarrollo, mantenimiento y configuración tanto de aplicativos como de software.

3. ALCANCE

La presente Política de Seguridad en el Desarrollo y Mantención de Sistemas, aplica a la totalidad de los (las) usuarios(as) que se relacionan con la Subsecretaría de Educación y que tengan acceso a los Activos de Información de esta Cartera de Estado, sean funcionarios(as) de planta, contrata, honorarios y externos que presten servicios a esta entidad, incluyendo personal de empresas proveedoras que presten servicios en el Ministerio de Educación, y que intervengan en alguna

etapa del ciclo de 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.

Cabe señalar que esta política aplica a unidades, recursos humanos, proveedores de servicios de MINEDUC, localidades e infraestructura de la institución y elementos tecnológicos relacionados con procesos de esta Cartera de Estado.

Esta Política, como las demás relativas a la seguridad de esta entidad, 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, según lo determinen los lineamientos ministeriales al efecto.

4. POLÍTICA

4.1 Roles y responsabilidades

4.1.1 Coordinador(a) Nacional de Tecnología:

Es la persona encargada de gestionar los recursos necesarios para la implementación de esta Política y fijar estándares técnicos relativos al desarrollo de aplicativos, así como de la adquisición, configuración y mantenimiento de aplicativos o software, y resguardo de los datos ministeriales, en especial la información sensible.

4.1.2 Encargado(a) de Seguridad de la Información:

Es la persona responsable de señalar los lineamientos de seguridad de la Información y velar por la correcta aplicación de la presente Política.

4.1.3 Persona dueña de los datos:

Será la responsable de definir el nivel de criticidad del aplicativo, software o servicio en la nube a desarrollar, mantener, adquirir o utilizar.

4.1.4 Encargado(a) del Área de Desarrollo, Área de Gestión de Proyectos y Área de Mantención Evolutiva:

Es la persona responsable de definir las normas, procedimientos y controles que permitan asegurar que, en los procesos de construcción, adquisición o mantención de sistemas de información, según corresponda a cada área, se apliquen los controles necesarios para la seguridad de la información, tales como:

a) Metodología(s) de desarrollo o mantención.

b) Ejecución de pruebas de aseguramiento de calidad.

c) Documentación.

e) Sistema de gestión de código.

f) Consideración de requerimientos de seguridad en el ciclo de desarrollo o mantención.

4.1.5 Encargado(a) del Área de Operaciones:

Es la persona que debe mantener la continuidad operacional y la seguridad en las plataformas tecnológicas que soportan los sistemas, software y datos del Ministerio de acuerdo con los lineamientos contenidos en esta política.

4.1.6 Jefes(as) de Proyecto de las diferentes Áreas de la Coordinación y Contrapartes de Áreas Usuarias:

Serán responsables de gestionar proyectos de adquisición, instalación, actualización de aplicativos, software o servicios en la nube a su cargo. Deben aplicar los lineamientos de esta Política, estándares y procedimientos definidos.

4.2 Disposiciones generales

Las normas de seguridad relativas a la materia de esta política deben estar incorporadas en los siguientes procesos y actividades desarrolladas en esta Cartera de Estado:

4.2.1 Las actividades propias del Ciclo de Desarrollo de Sistemas deberán resguardar los activos de información sensibles y que estén asociados a cada proyecto, tales como bases de datos personales, información estratégica, acuerdos de confidencialidad, documentación, información de control de proyectos, así como también los productos del mencionado Ciclo de Desarrollo, esto es los propios aplicativos y su documentación. Para dichos efectos se deberá:

(i) Normar y estandarizar el ciclo de desarrollo de sistemas en cada una de sus fases, según la(las) metodología(s) de desarrollo y mantención que defina la Coordinación Nacional de Tecnología (CNT).

(ii) Cada Jefe(a) de Proyecto de la CNT o del área usuaria responsable, debe supervisar y monitorear que el desarrollo, mantenimiento, configuración e instalación de aplicativos y/o software desarrollados o mantenidos interna o externamente cumpla con las políticas, estándares y procedimientos definidos.

(iii) Implementar y mantener los ambientes separados de desarrollo, pruebas y producción. Cada uno debe contar con mecanismos de acceso controlado, así mismo el ambiente de desarrollo debe estar restringido al equipo de Desarrollo, de Mantención Evolutiva o personal externo autorizado.

(iv) Por motivos de protección de los datos, en el ambiente de pruebas se deben utilizar datos anonimizados.

(v) El acceso a las bases de datos de construcción, pruebas y producción debe contar con controles según roles autorizados, evitando el acceso a estas bases de datos por parte de los usuarios. En ningún caso en las etapas de construcción y/o pruebas se debe dar acceso a los datos de producción.

(vi) Todo aplicativo o software desarrollado, modificado, instalado o configurado por externos debe cumplir con lo establecido en esta política. Esto incluye sistemas en "la nube" o Cloud, cuyo desarrollo debe considerar, adicionalmente, las directrices y buenas prácticas específicas que existan para estos efectos en los órganos de la Administración del Estado.

(vii) Todo cambio en los sistemas, como parte del Ciclo de Desarrollo, debe ser controlado por el área correspondiente, mediante el uso de procedimientos formales de control de cambios.

(viii)Toda modificación de software de base o de sistema, como sistemas operativos, controladores, bibliotecas, por parches o módulos adicionales, debe ser analizada y probada previamente en ambientes separados del ambiente de producción.

(ix) Se deben efectuar revisiones de los requisitos de seguridad durante el ciclo de vida del desarrollo.

4.2.2 En el caso de adquisición, actualización o instalación de software, se debe considerar que, por motivos de seguridad, estos activos deben tener actualizaciones en forma periódica en la modalidad de parches u otra que sea conveniente al Ministerio.

4.2.3 En los casos en que personal ajeno a la CNT instale soluciones de software o esté incorporado en equipos de desarrollo o mantención de aplicativos en los cuales se manipulen datos de Mineduc, las contrapartes del área usuaria deberán velar que se apliquen los lineamientos indicados en esta política, guías y procedimientos correspondientes; así como en las Políticas de Seguridad de Proveedores, Respaldo de Información, Intercambio de Información y Control de Acceso. Estos solo podrán operar si cuentan con la debida autorización de la Coordinación Nacional de Tecnología y la jefatura directa del usuario.

Adicionalmente, será responsabilidad de cada Jefe(a) de Proyecto o contraparte de área usuaria según corresponda, el asegurar que se cumpla con las políticas de seguridad, en lo que se refiere a resguardo del código fuente, acceso restringido, respaldo de datos y firma de Non Disclosure Agreement (NDA) tanto del representante legal como del especialista externo. Además, deberán contar con la autorización de CNT para efectuar cualquier tipo de modificación,

actualización, instalación, paso a producción u otra actividad dentro del ciclo de vida del software.

4.3 Lineamientos específicos para el Ciclo de desarrollo o para actividades de mantención.

4.3.1 Levantamiento, Análisis y evaluación de la solución

Durante el levantamiento, análisis y evaluación de la solución se deben considerar los aspectos de seguridad en cuanto al nivel de criticidad del sistema y el nivel de protección de seguridad que requerirán los datos y las aplicaciones que lo compongan.

4.3.2 Especificación de requerimientos

En la especificación y análisis de los requerimientos se deben comenzar a identificar los tipos de los controles de seguridad que se deben utilizar, actividad en la cual es muy recomendable que participen las áreas de negocio que serán (o son) usuarias del sistema en construcción o mantención.

4.3.3 Diseño

La persona encargada del Área de Desarrollo o de Mantención Evolutiva revisará los aspectos relacionados con el diseño de arquitectura de la solución, velando por su seguridad, rendimiento, escalabilidad, disponibilidad y auditoría del sistema a desarrollar.

Todos los sistemas clasificados como estratégicos deben incluir la generación de registros de auditoría considerando como mínimo la identidad del usuario que lee o escribe, y la fecha y hora del evento o lo que se indique en la Política de Seguridad de Logs del Servicio. Estos registros deben ser protegidos contra la manipulación no autorizada.

4.3.4 Codificación

Se deben utilizar librerías y frameworks de autores confiables, con mantención y desarrollo activo que cumplan requisitos de licencia, y que sean de origen seguro o validadas por la industria. Estas deben estar autorizadas por el (la) Coordinador(a) Nacional de Tecnología antes de empezar cualquier desarrollo.

Toda modificación de código fuente debe registrarse en el sistema de versionamiento que se esté utilizando.

Finalmente, debe revisarse la calidad del código durante la construcción para evitar posibles bugs de seguridad.

4.3.5 Pruebas

Dentro del Ciclo de Desarrollo deben realizarse pruebas o revisiones de seguridad y pruebas de funcionalidad. Estas pruebas deben realizarse antes de ejecutar la instalación en los servidores de producción. En el caso que las revisiones de seguridad detecten vulnerabilidades, estas deben ser corregidas antes de su paso a producción.

No se utilizarán datos personales o sensibles en ambientes de desarrollo y/o pruebas.

4.4 Datos personales y sensibles

En el caso que no se pueda evitar utilizar datos personales o sensibles en el proceso de desarrollo, instalación, configuración u otra actividad dentro del alcance de esta política, éstos deben ser protegidos tanto en el almacenamiento como en la transmisión mediante encriptación, para prevenir la modificación o acceso no autorizado.

Las personas que ejerzan como programadores(as), analistas y, en general, el personal ajeno a esta Cartera de Estado, no deben tener acceso a datos personales o sensibles que se encuentren en Producción.

4.5 Seguridad en la plataforma operativa

El Ministerio de Educación debe mantener la seguridad en la plataforma operativa que soporta los sistemas, sean éstas de producción, mantenimiento, prueba y/o desarrollo, en particular se deben custodiar y proteger los programas fuentes, los programas ejecutables, el software y los datos, de tal manera que no sean intervenidos o alterados sin contar con las aprobaciones y accesos autorizados

Cuando sea necesario realizar cambios, actualizaciones o reconfiguraciones en servidores de aplicaciones, de bases de datos, en dispositivos de seguridad o cualquier otro equipo asociado a la operación de los aplicativos o software, se debe evaluar y planificar las actividades antes de ejecutar las tareas correspondientes, con el fin de mitigar riesgos e impactos negativos en las operaciones o en la seguridad de la información de la organización, específicamente en su continuidad, integridad o disponibilidad.

Dentro de la planificación, se deben considerar respaldos, pruebas y revisiones de los sistemas o software instalados con el fin de asegurar su adecuada operación, así como el roll-back o reversa ante la ocurrencia de algún problema.

4.6 Documentación

La documentación del Sistema debe mantenerse actualizada cada vez que se realicen cambios en su funcionalidad y se debe contar con un procedimiento de control de versiones.

El acceso a la documentación de sistemas, bibliotecas de código fuente y programas ejecutables debe estar restringida solo al personal autorizado. La excepción son los manuales de usuario, manuales de capacitación u otros documentos destinados a los usuarios de los sistemas.

4.7 Controles de seguridad

En el desarrollo o mantención de aplicativos, o en la adquisición, configuración e instalación de software se deben considerar los siguientes tipos de controles básicos de seguridad según normativa interna vigente:

a. Arquitectura, diseño y modelado de amenazas

b. Requisitos de verificación de autenticación

c. Requisitos de verificación de gestión de sesiones

d. Requisitos de verificación del control de acceso

e. Requisitos de verificación para manejo de entrada de datos maliciosos

f. Codificación / escape de salidas de datos

g. Requisitos de verificación de gestión y registro de errores

h. Requisitos de verificación de protección de datos

i. Requisitos de verificación de seguridad de las comunicaciones

j. Requisitos de verificación de configuración de seguridad HTTP

k. Requisitos de seguridad para controlar software malicioso

l. Requisitos de verificación de archivos y recursos

m. Requisitos de configuración

El Área de Seguridad de la Información entregará orientaciones para la adecuada implementación de un conjunto mínimo de controles de seguridad.

Los equipos técnicos facilitarán las actividades de revisiones de seguridad de los aplicativos por parte de terceros autorizadas, sean estas manuales o automatizadas, y gestionarán, según los recursos disponibles, la aplicación de las recomendaciones resultantes de las revisiones.

4.8 Adquisición de servicios de desarrollo, mantención, configuración o instalación de aplicativos, de software o de servicios en la nube

Será requisito, para estos tipos de adquisiciones, la evaluación técnica, financiera, legal/contractual y funcional de la propuesta que el proveedor realice por parte de la CNT y de la Unidad que requiera de dichos servicios.

La instalación o el uso de software estará sujeta a los acuerdos de licencia y en los contratos se consignarán garantías de calidad, soporte y mantenimiento que respalden a Mineduc en el caso que el aplicativo, software o servicio en la nube no cumpla en alguna forma con los requisitos del negocio, los que no obstante se validarán exhaustivamente antes de decidir la compra.

Por motivos de seguridad, en los procesos de compra de software, desarrollo o mantención de aplicativos o servicios en la nube se debe poner atención a la necesidad de actualizaciones o parches según corresponda al tipo de compra. Así mismo los contratos deberán considerar las condiciones de resguardo y recuperación de los datos 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.

5. 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 MINEDUC 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.

6. 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° 20.285, sobre Acceso a la Información Pública.
d) Ley N° 20.880, sobre Probidad en la Función Pública y Prevención de los Conflictos de Intereses.
e) Ley N° 21.459 que Tipifica Delitos Informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
f) Ley N° 21.663

g) D.F.L. N° 29 de 2004, que Fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo.

h) Decreto Supremo N° 83, del 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.

i) 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.

j) Norma Chilena NCh-ISO27001:2013 sobre "Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos".

7. 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.

En esta materia, la Coordinación Nacional de Tecnología aplicará las medidas necesarias para monitorear el cumplimiento de esta política, mantendrá a los usuarios informados sobre nuevas amenazas y cuidados con respecto al resguardo de los activos de información, de manera de evitar incidentes producidos por el no cumplimiento de esta Política.

8. 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) Servicios: Servicios de computación y comunicaciones. Utilidades generales (ej. electricidad, luz, aire acondicionado, acceso a internet, etcétera).

c) Personas: Constituidos por los usuarios, que utilizan la estructura tecnológica, el área de comunicaciones y que gestionan la información.

d) Intangibles: Constituidos por los activos referidos a la reputación e imagen de la institución.

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

f) 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.

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

II. **DÉJASE** sin efecto la Resolución Exenta N° 5.773, de 2021, del Ministerio de Educación, que Aprueba Política de Seguridad en el Desarrollo y Mantención de Sistemas para el Ministerio de Educación.

ANÓTESE, PUBLÍQUESE INTERNAMENTE Y ARCHÍVESE

ALEJANDRA ARRATIA MARTÍNEZ
SUBSECRETARIA DE EDUCACIÓN

Distribución:
- Gabinete Sr. Ministro
- Gabinete Sra. Subsecretaria de Educación
- División Jurídica – Comité de Control, Transparencia y ADP.
- División de Administración General.
- Oficina de Partes y Archivos Nivel Central.
- Archivo.
- Exp. 31.588-2023