Gobierno de Chile

APRUEBA LA POLÍTICA DE REGISTROS DE AUDITORÍA PARA LA SUBSECRETARÍA DE EDUCACIÓN.

Solicitud N° 720

SANTIAGO, 28 ENE 2026

RESOLUCIÓN EXENTA N° 506

LIP/CAM/MDB/PTM

MINISTERIO DE EDUCACIÓN
30 ENE 2026
DOCUMENTO TOTALMENTE TRAMITADO

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° 17.336, de Propiedad Intelectual; 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° 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 N° 21.663 Marco sobre Ciberseguridad; 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° 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; 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 Norma Chilena NCh-ISO27001:2013 sobre "Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos; 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° 24 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, 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, en este orden de ideas, es preciso generar una Política de Registros de Auditoría, otorgando lineamientos de resguardo para el proceso de desarrollo

y mantenimiento de los sistemas de información, en orden a gestionar adecuadamente la seguridad de la información institucional, velando por el resguardo de la información propia y de usuarios internos y la comunidad escolar.

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

RESUELVO:

I. **APRUÉBASE** la Política de Registros de Auditoría, cuyo el 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 Registros de Auditoría.

2.- OBJETIVO

La presente Política tiene como objetivo establecer lineamientos respecto a la recopilación y uso de registros de auditoría, logs en adelante, para detectar, monitorear y mitigar las diversas amenazas tecnológicas externas e internas, las que pueden afectar gravemente las operaciones de los servicios y sistemas informáticos de la Subsecretaría de Educación o bien revisar eventos o incidentes ya ocurridos. Este objetivo se enmarca en lo que establece la Nch 27001-2022, relativa a "Seguridad de información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información".

3.- ALCANCE

La Política de Registros de Auditoría 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.

Asimismo, se aplica a los sistemas críticos que tengan la capacidad de generar logs en sistemas informáticos, dispositivos de red, seguridad y sistemas de acceso remoto

De igual manera, 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).

Para el adecuado entendimiento de esta política, se comprenderá por "registro de auditoría", "log", "historial de log" o "registro de log", a la grabación secuencial en un archivo o en una base de datos de los acontecimientos (eventos o acciones) que afectan a un proceso particular gestionado por una aplicación, dispositivo de una red informática, etc. o al registro de las acciones realizadas por un usuario a través de sistemas, aplicativos o dispositivos como por ejemplo el inicio y cierre de sesión y los accesos que realiza. De esta forma, constituye una evidencia del comportamiento del activo de información que se monitorea o de los usuarios

En este sentido, se considerarán los siguientes tipos de logs pertenecientes a la Subsecretaría de Educación:

a) Plataforma de Redes de nivel estratégico, tales como: DMZ (demilitarized zone o zona desmilitarizada) y Core.

b) Plataforma de Servidores (físicos y virtuales).

c) Dispositivos de Seguridad.

d) Mecanismos de acceso remoto como VPNs. Sistemas estratégicos, sistemas que manejen datos personales y aquellos relacionados con gestión de recursos financieros.

e) Directorio activo (Active Directory) y controladores de dominio.

4.- POLÍTICA

4.1 ROLES Y RESPONSABILIDADES

4.1.1. 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.

4.1.2. 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.

4.1.3. Encargado(a) de Operaciones

Es la persona responsable de asegurar la continuidad operacional en la generación de los registros de log en las plataformas, dispositivo, sistemas estratégicos, que manejen datos personales y de gestión financiera, dispositivos de red y seguridad, y todo elemento dentro del alcance; además de un correcto contenido de los registros, en el sentido de poder identificar el origen, destino, acción y fecha/hora del evento, con el objetivo de lograr una eficaz utilización en la investigación de excepciones, fallas y eventos de seguridad de la información.

4.2 CLASIFICACIÓN DE LOS REGISTROS DE LOGS

El contenido de los Registros de Logs se clasificará como activo de información crítico y por ello de acceso restringido, debido a que su contenido puede considerar información sensible de usuarios, posibles vulnerabilidades, eventos o incidentes que afecten a la infraestructura, sistemas, dispositivos, etcétera.

4.3 ACCESO Y PROTECCIÓN DE LOS REGISTROS DE LOGS

Al contener información clasificada, debe ser protegida contra el acceso no autorizado para revisiones o modificaciones no deseadas, siendo éste restringido y controlado para las personas que, por razones de operación o de alguna investigación autorizada, así lo requieran.

Los recursos relacionados al registro de logs deben considerarse como parte de la infraestructura crítica de este Ministerio, por lo que es obligatorio sincronizar los relojes para que los registros tengan horas consistentes, para ello se debe tener configurado y habilitado el protocolo correspondiente de red (Network Time Protocol).

4.4 USO DE LOS REGISTROS DE LOGS

El uso de los registros se enmarca en la búsqueda, correlación y obtención de información de las plataformas, dispositivos, mecanismos y sistemas en caso de realizar investigaciones, actividades de monitoreo o análisis forense.

4.5 ALMACENAMIENTO DE LOS REGISTROS DE LOGS

La Coordinación Nacional de Tecnología (CNT) definirá el período de retención de los registros de auditoría, sobre la base de las capacidades de almacenamiento y recursos disponibles, siendo deseable que este tiempo sea de un año (mínimo) o lo que se instruya o recomiende a los Órganos de la Administración del Estado.

Los registros de auditoría se almacenarán en un repositorio central colector de logs y pueden estar sujetos a auditorías de terceros.

4.6 ESTRUCTURA DE LOS REGISTROS DE LOGS

Debe ser adecuada, con el objeto de poder realizar las actividades de investigación de forma eficaz, entregando información certera del origen, destino, acción y fecha/hora del evento.

Elementos recomendables que deben contemplar los registros de logs según el tipo de activo relacionado son:

a) Identidad de los usuarios y actividades realizadas (fechas, horas, dirección IP, nombre del dispositivo y eventos específicos).

b) Actividades del sistema (fechas, horas y comunicaciones automáticas con otros sistemas).

c) Privilegios utilizados.

d) Ficheros utilizados y accesos a bases de datos.

e) Direcciones de red accedidas.

f) Intentos y denegaciones de acceso a los sistemas.

g) Cambios en la configuración y privilegios.

h) Alarmas originadas por los sistemas de monitoreo.

i) Desactivación de los mecanismos de protección.

j) Modificaciones en los permisos de acceso;

k) Funcionamiento o finalización anómalos de aplicativos;

l) Aproximación a los límites de uso de ciertos recursos físicos, como capacidad de disco, memoria, ancho de banda de red y uso de CPU.

m) Indicios de actividad sospechosa detectada por antivirus, Sistemas de Detección de Intrusos (IDS), etcétera.

4.7 REGISTROS AUDITORÍA DE LOGS

Los jefes de proyectos deberán incorporar registros de auditoría, en el caso de los sistemas estratégicos, sistemas gestión de recursos financieros y de aquellos que manejen o contengan datos personales.

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 en formato electrónico en la Intranet de la institución para futuras consultas.

6. RESPONSABILIDAD ANTE INFRACCIONES

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 podría 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.

7. 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: Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.

c) Core de red: Dispositivo de red central, encargado de desviar las peticiones de tráfico del usuario, de la capa de distribución hacia los servicios corporativos tales como correo, ambientes de testing y desarrollo o acceso a Internet.

d) Disponibilidad: Propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

e) Dispositivos de seguridad: Corresponden a los equipos computacionales que forman parte de la infraestructura de seguridad, con el objetivo de

enfrentar las amenazas de seguridad de red mediante políticas establecidas, ejerciendo diferentes funciones de control, tales como: control de acceso, control de tráfico de red, malware, denegación de servicio y ataques informáticos sobre sistemas y servicios.

f) DMZ: Zona Desmilitarizada (en inglés demilitarized zone) o red perimetral, es una zona segura ubicada en la red interna, asegurada con cortafuegos que controlan las conexiones de los servicios publicados hacia la internet, protegiendo contra intrusos que puedan comprometer la seguridad.

g) Integridad: Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.

h) Registro de auditoría, log, historial de log o registro de log: Es la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etcétera). De esta forma, constituye una evidencia del comportamiento del sistema y de aquellos activos que interactúan con el sistema.

i) SIEM: Administración de eventos e información de seguridad (en inglés Security Information Event Management), es una herramienta para la gestión de información y eventos de seguridad, la que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad, según criterios definidos para su discriminación. Se utiliza para detectar patrones de tráfico o comportamiento no habituales que permitan detectar en forma temprana eventuales ciberincidentes.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

REPUBLICA DE CHILE
MINISTERIO DE EDUCACIÓN

ALEJANDRA ARRATIA MARTÍNEZ
SUBSECRETARIA DE EDUCACIÓN

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

Expediente N° 46.082-2023