Gobierno de Chile

APRUEBA NUEVA POLÍTICA DE REGISTRO DE LOGS PARA LA SUBSECRETARÍA DE EDUCACIÓN

MINEDUC/DPC/RVL/CAD

Solicitud N° 0351

SANTIAGO, 19 ENE 2021

RESOLUCIÓN EXENTA N° 0294

MINISTERIO DE EDUCACIÓN
05 FEB 2021
DOCUMENTO TOTALMENTE TRAMITADO

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 2005, 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 Resolución Exenta N°6300 de 27 de noviembre de 2017 que aprueba la Política de Registro de Logs para la Subsecretaria de Educación; en el Ord. N° 2758 de 28 de diciembre de 2020 del Jefe de la División de Planificación y Presupuesto de la Subsecretaria de Educación y en la Resolución N° 7 de 2019, que Fija Normas sobre Exención del Trámite de Toma de Razón, de la Contraloría General de la República.

CONSIDERANDO:

Que, mediante Resolución Exenta N°6300 de 27 de noviembre de 2017 se apruebo la Política de Registro de Logs para la Subsecretaria de Educación. Que a través de Ord. N° 2758 de 28 de diciembre de 2020 del Jefe de la División de Planificación y Presupuesto de la Subsecretaria de Educación, se remite la Nueva Política de Registro de Logs para la Subsecretaría de Educación, en el marco de la norma chilena NCH-ISO 27001-2013, sobre tecnologías de información, técnicas de seguridad, sistemas de gestión de la seguridad de la información y sus requisitos, cuyo objetivo es establecer lineamientos respecto al uso de registros de logs para poder

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.

Que, para la correcta implementación de esta normativa, es necesario contar con una Actualización de la Política de Registro de Logs para la Subsecretaría de Educación.

La NCH ISO 27001-2013 es una norma chilena que ha sido elaborada y difundida por el Instituto Nacional de Normalización (INN), la cual permite garantizar la confidencialidad e integración de la información que manipulan las organizaciones.

La norma NCH ISO27001-2013 para los Sistemas de Gestión de Seguridad de la Información o SGSI hace posible que las organizaciones lleven a cabo una evaluación del riesgo y adopte los controles imprescindibles para lograr mitigarlos e incluso eliminarlos. Para llevar a cabo una adecuada Gestión de la Seguridad de la Información en las organizaciones, se necesita del uso de buenas prácticas o controles que están establecidos por la norma NCH-ISO 27002-2013.

Esta norma define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de la organización. Esta norma incluye además los requisitos para la evaluación y tratamiento de los riesgos de la seguridad de la información que se adapta a las necesidades de la organización. Los requisitos definidos en esta norma son genéricos y tienen por objetivo ser aplicables a todas las organizaciones, sin importar el tipo, tamaño o naturaleza.

Para apoyar el cumplimiento de sus funciones, la Subsecretaría de Educación ha desarrollado, para el apoyo de la gestión ministerial, una plataforma tecnológica a través de la cual se registra procesa, transmite y almacenan datos, antecedentes e información, a través de diferentes Activos de Información, que permiten interactuar tanto con los funcionarios en todo el país, con otros servicios públicos, entidades privadas, la comunidad escolar y con la ciudadanía en general.

Esta política aplica a los sistemas críticos que tengan la capacidad de generar logs en sistemas informáticos, dispositivos de red y seguridad.

En este sentido, debe ser conocida por todos los funcionarios de la Subsecretaría de Educación, ya sea que se encuentren contratados en calidad jurídica de planta, contrata u honorarios. Asimismo, respecto de todo el personal de empresas externas, que presten servicios a la Subsecretaría de Educación.

De igual manera, estas directrices, como las demás relativas a la seguridad de este organismo, es empleable ante 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 y objetivos estratégicos de la entidad (Formulario A1 de definiciones estratégicas).

Para el adecuado entendimiento de esta política se entiende por log, historial de log o registro de log, 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, etc.). De esta forma constituye una evidencia del comportamiento del sistema.

Que, este procedimiento fue elaborado por la División de Planificación y Presupuesto, según consta en Ord. N° 2758 de 28 de diciembre de 2020 del Jefe de la División de Planificación y Presupuesto de la Subsecretaria de Educación.

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

RESUELVO:

1-Apruébese la "Nueva Política de Registro de Logs para la Subsecretaría de Educación", la cual se entiende parte integrante de la presente resolución.

2- Déjese sin efecto la Resolución Exenta N°6300 de 27 de noviembre de 2017 que aprueba la "Política de Registro de Logs para la Subsecretaria de Educación".

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

REPUBLICA DE CHILE
MINISTERIO DE EDUCACION
SUBSECRETARIO

LEON PAUL CASTRO
SUBSECRETARIO DE EDUCACIÓN (S)

Distribución:
- Of. Partes
- Gabinete Sr. Ministro
- Gabinete Sr. Subsecretario
- División Jurídica
- División de Planificación y Presupuesto

Exp. 412.371- 2020

POLÍTICA DE REGISTRO DE LOGS PARA LA SUBSECRETARÍA DE EDUCACIÓN.

FIRMA DE LOS RESPONSABLES

ELABORADO POR	REVISADO POR	APROBADO POR
Juan Antonio Serrano Encargado de Seguridad	Jonny Heiss Schmidt Coordinador Nacional de Tecnología	Francisco Jeria León Presidente Comité de Seguridad de la Información

CONTROL DE VERSIONES

REVISIONES DEL DOCUMENTO DE POLITICA				
N° Revisión	**Fecha Aprobació**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
0(Cero)		Elaboración inicial	Todas	Juan Antonio Serrano

1. DECLARACIÓN INSTITUCIONAL

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

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

Así, la información que se encuentra en poder de esta Subsecretaría de Educación, es un bien estratégico para sus funciones, por lo que se requiere que sea protegida 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.

De esta manera, por medio de las Resoluciones Exentas N°s 4.503, de 2014, 3.862, de 2016, y 3.106, de 2017, todas de este origen, se designa el Encargado de Seguridad de los Activos de Información; se aprueba la Política de Seguridad de la Información; y la Política de Organización de Seguridad de la Información, respectivamente, creando y actualizando lineamientos para esta Subsecretaría en la materia.

En este contexto, es necesario contar con la Política de Registro de Logs, como un marco de referencia para el establecimiento de criterios de seguridad para el proceso de desarrollo y mantenimiento de los sistemas de información.

2. OBJETIVO

La presente política tiene como objetivo establecer lineamientos respecto al uso de registros de logs para poder 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. Este objetivo se enmarca en lo que establece la Nch 27001-2013, y su control A.12.4.1 "Registro de eventos".

3. ALCANCE

Esta política aplica a los sistemas críticos que tengan la capacidad de generar logs en sistemas informáticos, dispositivos de red y seguridad.

En este sentido, debe ser conocida por todos los funcionarios de la Subsecretaría de Educación, ya sea que se encuentren contratados en calidad jurídica de planta, contrata u honorarios. Asimismo, respecto de todo el personal de empresas externas, que presten servicios a la Subsecretaría de Educación.

De igual manera, estas directrices, como las demás relativas a la seguridad de este organismo, es empleable ante 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 y objetivos estratégicos de la entidad (Formulario A1 de definiciones estratégicas).

Para el adecuado entendimiento de esta política se entenderá por log, historial de log o registro de log, 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, etc.). De esta forma constituye una evidencia del comportamiento del sistema.

Para la correcta aplicación de esta política se considerarán los siguientes tipos de logs pertenecientes a la Subsecretaría de Educación:

- Plataforma de Redes de nivel estratégico Ej. DMZ (demilitarized zone o zona desmilitarizada), Core.
- Plataforma de Servidores (físicos y virtuales)
- Dispositivos de Seguridad.
- Aplicaciones con registros de auditoria relacionados con gestión de recursos financieros.

4. POLÍTICA

4.1 ROLES Y RESPONSABILIDADES

Comité de Seguridad de la Información: Es el encargado de aprobar y sancionar la Política de Registro de Logs.

Coordinador(a) Nacional de Tecnología: Es quien gestiona y provee los recursos necesarios para el cumplimiento de estos lineamientos.

Encargado(a) de Seguridad de la Información: Es el responsable de controlar la implementación de esta política y velar por su correcta aplicación.

Encargado(a) de Operaciones: Es quien tiene a su cargo asegurar continuidad operacional en la generación de los registros de log en los sistemas críticos, dispositivos de red y seguridad, 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 Log se clasificará de acceso restringido, debido a que su contenido puede contener información sensible de usuarios, posibles vulnerabilidades e infraestructura de los sistemas.

4.3 ACCESO A LOS REGISTROS DE LOGS

Al contener información clasificada, debe ser protegida contra el acceso no autorizado, siendo éste restringido a las personas que por razones de operación o de alguna investigación lo requieran.

Los recursos relacionados al registro de logs deben considerarse como parte de la infraestructura crítica de este Ministerio.

4.4 USO DE LOS REGISTROS DE LOGS

El uso de los registros se hará para obtener información de los sistemas en caso de realizar investigaciones, actividades de monitoreo, análisis forense y de vulnerabilidades.

4.5 ALMACENAMIENTO DE LOS REGISTROS DE LOGS

Se realizará por un período mínimo de 1 mes, utilizando los medios apropiados para este proceso.

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.

4.7 REGISTROS AUDITORÍA DE LOGS

Los jefes de proyectos deberán evaluar la incorporación de registros de auditoría, en el caso de estar relacionados con sistemas gestión de recursos financieros.

5. VIGENCIA

Esta norma entrará en vigencia 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 para futuras consultas.

6. LEGISLACIÓN VIGENTE

Ley N° 17.336, de Propiedad Intelectual.

Ley N° 19.223, que Tipifica Figuras Penales relativas a la Informática.

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.

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.

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.

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.

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, podrá 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, 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, y 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:

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

Disponibilidad: Derecho de los usuarios autorizados a tener acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

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

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.

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.

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.

Log, historial de log o registro de log: 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, etc.). De esta forma, constituye una evidencia del comportamiento del sistema.