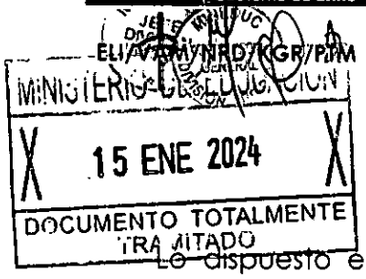
c/f



APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE EDUCACIÓN Y DEFINE LAS LABORES DEL ÓRGANO ENCARGADO DE VELAR POR SU CUMPLIMIENTO
Solicitud N° 2374

SANTIAGO, 08 de Mayo de 2023

RESOLUCIÓN EXENTA N° 2693

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.° 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 DFL 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.° 19.628, Sobre Protección de la Vida Privada; 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.° 296, de 2021, del Ministerio de Educación, que Aprueba Nueva Política de Seguridad de la Información del Ministerio de Educación y Define las Labores del Órgano Encargado de Velar por su Cumplimiento; 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, 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, los datos que se encuentran en poder de esta Subsecretaría de Educación son un bien estratégico para sus funciones, por lo que se requiere que sea protegida tanto en su obtención, como en su procesamiento, transmisión y almacenamiento. Dicho deber 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, en este contexto, es pertinente definir los requerimientos a establecer, implementar, mantener y mejorar de manera continua, regulando un sistema de gestión de la seguridad de la información dentro de esta Cartera de Estado.

Que, mediante la Resolución Exenta N.° 296, de 2021, de este origen, se aprobó la Política de Seguridad de la Información del Ministerio de Educación y Define las Labores del Órgano Encargado de Velar por su Cumplimiento.

Que, es necesario actualizar el contenido de la política referida y adoptar medidas de seguridad con la finalidad de disponer en forma segura los datos necesarios para la operación de los sistemas de información de la institución, dando continuidad al servicio.

RESUELVO:

I. **APRUÉBASE** la siguiente política de seguridad de la información:

"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y LABORES DEL ÓRGANO ENCARGADO DE VELAR POR SU CUMPLIMIENTO

Declaración institucional

El Ministerio de Educación, en adelante 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.

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, para cumplir con las funciones que le han sido encomendadas y le competen.

Así, los datos que se encuentran en poder de esta Subsecretaría son un bien estratégico para sus funciones, por lo que se requiere que sean protegidos tanto en su obtención, procesamiento, transmisión y almacenamiento. Por lo tanto, el personal que integra la organización será responsable de velar por su confidencialidad, integridad y disponibilidad según lo que de acuerdo a su cargo y función le corresponda administrar y gestionar, de conformidad al marco legal actualmente vigente.

Luego, con el fin de apoyar su organización, mediante la Resolución Exenta N.° 296, de 2021, de este origen, se aprobó una Nueva Política de Seguridad de la Información, junto con las definiciones de las labores del órgano encargado de velar por su cumplimiento.

En este orden de ideas y acorde al lineamiento que deriva de la Política de Seguridad de la Información antes referida, es necesario establecer su texto de modo de hacerlo operativo a las nuevas circunstancias tecnológicas y de hecho del Servicio.

A. DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE EDUCACIÓN

1. Objetivos

Los objetivos de esta política son:

a) Objetivo general

Establecer los principios y marco general de trabajo del Ministerio de Educación para administrar, mantener, sensibilizar, monitorear y revisar el Sistema de Gestión de Seguridad de la Información (SGSI) acorde a las definiciones estratégicas, la misión y objetivos estratégicos institucionales, asegurando la confidencialidad, integridad y disponibilidad de los activos de la información, a través de su adecuada implementación, asignación de roles, funciones y responsabilidades.

b) Objetivos específicos

Establecer los requisitos y condiciones generales de protección y resguardo de seguridad y ciberseguridad a las que se encuentra sujeto este Ministerio, de acuerdo con las normas legales y reglamentarias pertinentes.

Definir los principios generales para el resguardo de las operaciones críticas de la Institución y las responsabilidades respecto al uso de los recursos tecnológicos que provee el Servicio y al manejo de la información.

Establecer un marco de gestión de riesgo cibernético para cada sistema, proceso, actividad crítica, que permita alcanzar los objetivos estratégicos.

Implementar una metodología enfocada en la gestión del riesgo institucional.

2. Alcance

La presente Política de Seguridad de la Información aplica a todas las plataformas tecnológicas, redes, sistemas de información, aplicaciones, servicios de interoperabilidad con entidades externas, herramientas, repositorios de información y base de datos, así como otros activos de información que requieran acceso lógico y que se agreguen a futuro.

La seguridad es responsabilidad de la totalidad de las personas que se relacionan con la Subsecretaría de Educación y que tengan acceso a los Activos de Información de esta entidad, sean estos funcionarios (as) de planta, contrata o personal a honorarios, incluyendo a su vez a los asesores, consultores, practicantes y, en general, toda aquella persona natural o jurídica que preste servicios a la Subsecretaría de Educación. Por tal razón, las políticas establecidas en este documento son de conocimiento y cumplimiento obligatorio para todos (as) a quienes se les otorgue acceso a estos activos, por el motivo que sea.

Al efecto, en el caso de las personas naturales o jurídicas externas, dicha obligación deberá expresarse en los contratos o acuerdos respectivos, según se establece en las Políticas de Seguridad con Terceros y en Relación con Proveedores.

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 aquellos que están asociados a procesos de provisión de los productos estratégicos de la institución, según lo determine el Formulario A1 de la Ficha de Definiciones Estratégicas otorgada por la Dirección de Presupuestos (DIPRES) del Gobierno de Chile, con miras a proteger aquellos sistemas, sitios web, procesos, entre otros, que apoyan los objetivos estratégicos.

3. Roles y Responsabilidades

3.1 Subsecretario(a) de Educación: En su calidad de Jefe(a) Administrativo(a) del Ministerio de Educación le corresponde la aprobación de esta Política de Seguridad y de sus futuras modificaciones. Asimismo, velará por su

cumplimiento y será asesorado en la toma de decisiones por el Comité de Seguridad de la Información y Continuidad del Servicio.

3.2 Encargado(a) de Seguridad de la Información de la Subsecretaría de Educación: El (La) funcionario(a) -a cargo de esta función-, debe señalar los requisitos de seguridad de la información y velar por la correcta aplicación de las Políticas de Seguridad, lo que constituirá parte integrante de su contratación. Sin perjuicio de las funciones específicas definidas por la autoridad a través de Resolución Exenta que lo designe y, asimismo, de las competencias definidas para el cargo que desarrollará el Encargado de Seguridad de la Información, sus funciones incluirán a lo menos:

a) Tener a su cargo el desarrollo inicial de las políticas de seguridad y el control de su implementación, velar por su correcta aplicación y por su oportuna actualización, cuando los cambios externos lo requieran.
b) Coordinar las actividades de preparación para que la Institución pueda enfrentar de manera adecuada los incidentes de seguridad de la información.
c) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
d) Coordinar las actividades del Comité de Seguridad de la Información.
e) Promover acciones tendientes a la difusión, concientización y sensibilización de la seguridad de la información y ciberseguridad, entre los funcionarios de la Institución.

3.3 Coordinador(a) Nacional de Tecnología de la Subsecretaría de Educación: La persona que ejerza esta función debe gestionar los recursos necesarios para la implementación de las políticas de seguridad de la información y determinar los estándares relativos a la implementación de los controles y resguardo de los activos de información, manteniendo su confidencialidad, disponibilidad, e integridad.

Por su parte y, en el ámbito de la seguridad de la información, sus funciones incluirán, a lo menos:

a) Asegurar el adecuado funcionamiento de las redes, enlaces y plataformas que permitan la efectiva operación del Ministerio de Educación;
b) Proponer la adquisición para la implementación y administración de la infraestructura informática necesaria que sustente la operación de los distintos sistemas;
c) Proponer y asegurar el funcionamiento de las medidas de seguridad que resguarden la confidencialidad, integridad y disponibilidad de la

información, en conformidad a las instrucciones impartidas por el Comité de Seguridad de la Información y Continuidad del Servicio;

d) Proponer disposiciones generales para el uso de activos de información y mantener un inventario actualizado de aquellos bajo su custodia;
e) Proponer capacitaciones en el uso de activos de información pertinentes para el personal del Ministerio de Educación;
f) Realizar capacitaciones a dicho personal referidas a las políticas de seguridad de la información y de procedimientos de la Coordinación Nacional de Tecnología de la Subsecretaría de Educación (CNT), en las competencias requeridas conforme al perfil de cada cargo.
g) Informar al Comité de Seguridad de la Información y al Encargado de Seguridad de la Información, acerca de cambios significativos en los ambientes o estándares tecnológicos, que puedan hacer variar los riesgos de seguridad de la información.

3.4 Usuarios(as): sean estos funcionarios (as) de planta, contrata o personal a honorarios, incluyendo a su vez a los asesores, consultores, practicantes y, en general, toda aquella persona natural o jurídica que preste servicios a la Subsecretaría de Educación, quienes deberán:

a) Conocer y cumplir la política general y las políticas específicas de seguridad de la información, así como procedimientos específicos de seguridad.
b) Utilizar adecuadamente los activos de información a su cargo.
c) Informar cualquier situación detectada, que pueda comprometer o haya comprometido la seguridad de la información, a través de los canales definidos.
d) Realizar la devolución de los activos de información proporcionados por la Institución al concluir su relación con la Institución.

4. Organización de la Seguridad: Comité de Seguridad de la Información y Continuidad del Servicio

El Ministerio de Educación contará con un "Comité de Seguridad de la Información y Continuidad del Servicio", el cual corresponderá a un órgano colegiado cuya labor principal será prestar apoyo al (a la) Subsecretario(a) de Educación en la adopción de decisiones en materias relacionadas con la seguridad de la información y la continuidad de los servicios críticos con los que funciona esta Secretaría de Estado. Por su intermedio, el (la) Subsecretario(a) de Educación determinará, autorizará y vigilará los controles y prácticas de seguridad y ciberseguridad que ayuden a mejorar los niveles de protección y resguardo de los activos de esta entidad.

Este órgano deberá dictaminar marcos de trabajo sobre seguridad, ciberseguridad y continuidad, que incluyan la relación con entidades externas a la institución y/o terceros que presten servicios de cualquier índole al Ministerio de Educación.

Asimismo, estará constituido por autoridades y funcionarios(as) claramente definidos, que tendrán como misión velar por la confidencialidad, integridad y disponibilidad de la información, y por la Continuidad de los Servicios del Ministerio, con foco en sus productos estratégicos.

5. Gestión de la Seguridad de la Información y ciberseguridad

La Subsecretaría de Educación mantendrá una organización para la gestión de la seguridad de la información, con un enfoque de mejora continua y a través de una adecuada provisión de recursos para lograr la satisfacción de usuarios y beneficiarios, la continuidad de los servicios a niveles aceptables de operación, el cumplimiento de los objetivos establecidos manteniendo la confidencialidad, integridad y disponibilidad de la información, monitoreando y optimizando los controles de seguridad, sobre la base de los requisitos de la norma NCh-ISO 27001:2013 y a través de un programa de implementación de controles de seguridad según las recomendaciones de la norma NCh-ISO 27002:2013, alineado con el cumplimiento de lo establecido en la legislación vigente.

De manera especial, esta entidad deberá ocuparse de la ciberseguridad de las redes, plataformas y sistemas informáticos que forman parte de su plataforma tecnológica.

Lo anterior, implica asumir la gestión de los riesgos asociados a la ciberseguridad, incluyendo las actividades orientadas a la protección preventiva de infraestructuras tecnológicas y sus datos, la detección de anomalías e incidentes, la mitigación del impacto de estos, así como la respuesta y recuperación oportuna frente a incidentes que la afecten.

Por lo anterior, las siguientes estipulaciones se entienden parte de esta política.

a) La Política de Seguridad de la Información contenida en el presente acto, establece los lineamientos generales con respecto al buen uso de los activos de información, tanto compartidos como de cada uno de los usuarios internos o externos.

b) Estas directrices de carácter general están destinadas a servir de guía para la definición de normas específicas que se contendrán en las disposiciones complementarias de carácter administrativo y técnico, que se dicten para su cumplimiento.

c) Es responsabilidad de todos los(as) usuarios(as) y, los terceros relacionados con el manejo de los activos de información de la Institución, el hacer uso de

estos en forma autorizada y en directa y exclusiva relación con las funciones que desempeñan y, en concordancia con la normativa existente y el marco legal. A su vez, reportar cualquier situación o evento que pueda exponer o afectar la integridad, confidencialidad o disponibilidad de los activos de información, de acuerdo con los procedimientos publicados en la Intranet para estos efectos. De este modo, sólo funcionarios específicos tienen las atribuciones para determinar y calificar la real exposición de los activos en los eventos o situaciones que se informan.

d) En el ámbito de los sistemas de información, todos los proyectos de nuevos sistemas o evolución de los existentes deben considerar los recursos humanos, técnicos y financieros para la implementación de los controles de seguridad y ciberseguridad establecidos, de acuerdo con el resultado de los análisis de riesgos correspondientes.

e) La ciberseguridad debe estar incorporada en los procesos que se abordan anualmente en la matriz de riesgos institucional.

f) La institución reconoce que la capacitación, concientización y sensibilización de sus funcionarios(as) en materias de seguridad de la información, es una tarea que debe realizarse de manera permanente, en el marco de los recursos disponibles.

6. Gestión de la Continuidad de los Servicios

La Subsecretaría de Educación establecerá lineamientos por medio de una política específica y, asimismo, determinará las prácticas de gestión de continuidad del servicio mediante un programa de continuidad anual, el cual debe propender a la mejora continua en el marco de los recursos disponibles.

Para dichos efectos, el referido programa considerará aspectos tales como: identificación de las amenazas potenciales, evaluación del riesgo y su impacto en los procesos estratégicos del Mineduc, la definición de estrategias de continuidad en los ámbitos de personas, información y datos, infraestructura, tecnologías de información y comunicaciones, proveedores y la elaboración de los planes y procedimientos de continuidad, en los niveles que corresponda.

Todo proceso de la institución que sea declarado como estratégico o que tenga relación con un servicio que sea prestado a la comunidad, debe considerar:

a) La definición y documentación de las estrategias de prevención y recuperación del servicio ante eventos detonantes de contingencias, desastres o emergencias.

b) Los riesgos de ciberseguridad asociados a dichos eventos detonantes.

c) El establecimiento de estrategias y planes para enfrentar desastres que comprometan la continuidad del servicio.

d) Los lineamientos esenciales establecidos mediante acuerdos tomados por el Comité de Seguridad de la Información y Continuidad del Servicio, en la construcción de planes de continuidad y de recuperación en relación con materias relacionadas a la criticidad de los servicios y los tiempos de recuperación de los mismos como es el caso del tiempo de pérdida de datos que puede tolerar la institución, tiempo para recuperar sistemas y/o recursos que han sufrido una alteración y el tiempo máximo de inactividad aceptable.

e) Que cada Plan de Continuidad cuente con un responsable de su mantención y vigencia en el tiempo. Además, debe estar regularmente actualizado y difundido, de modo que no pierda operatividad con los cambios a los sistemas o procesos de negocio.

f) Asimismo, éstos deben probarse en forma recurrente de modo que todas las personas de la Institución que participan en él estén preparadas para su puesta en operación, cuando sea necesario.

g) Que, en el caso de fallas operativas normales y mantenciones de sistemas, sean los dueños de los servicios, las personas responsables de desarrollar y mantener los procedimientos de recuperación asociados.

h) Se debe planificar con anticipación todos aquellos cambios a la capacidad de equipos, en orden a asegurar la disponibilidad de los recursos y, a la evaluación del posible impacto en los planes de contingencia y procedimientos de recuperación.

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:

b) 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.

c) Activos de Software: constituidos por las aplicaciones de software sistemas, herramientas de desarrollo y utilidades.

d) Activos Físicos: constituidos por el equipamiento computacional, equipamiento de comunicaciones, medios móviles y otros equipamientos.

e) Ciberespacio: entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física.

f) Ciberseguridad: condición de estar protegido en contra de consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resulten del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el Ciberespacio que se pueda considerar no deseable.

g) Confidencialidad: garantía de que accedan a la información sólo aquellas personas autorizadas a hacerlo.

h) Continuidad del servicio: capacidad de la organización para continuar entregando productos o servicios a niveles aceptables predefinidos tras un incidente.

i) 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.

j) Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del servicio y amenazar la seguridad de la información.

Se entenderán por Incidentes de Seguridad de la Información, los siguientes:

j.1) Robo o pérdida de un equipo que almacena información, como por ejemplo un computador personal o un teléfono inteligente que contenga información sensible.

j.2) Robo o pérdida de documentación sensible como por ejemplo informes (en papel o digitales), archivadores, contratos, etc.

j.3) Filtraciones de datos especialmente sensibles hacia el exterior, como por ejemplo datos de funcionarios, estudiantes, sostenedores, establecimientos educacionales, etc.

j.4) Denegación de servicio sobre equipos de red y comunicaciones, afectando la operación normal de la Institución. Entiéndase una denegación de servicio, como un tipo de ataque informático especialmente dirigido a redes de computadoras y que tiene como objetivo lograr que un servicio específico o recurso de la red, quede completamente inaccesible a los usuarios legítimos de la red.

j.5) Presencia de virus, código malicioso u otro tipo de infección computacional.

j.6) Fallas graves en sistemas informáticos institucionales.

j.7) Ingresos no autorizados a los sistemas de información, como por ejemplo uso de cuentas ajenas.

j.8) Cualquier evento que impida el acceso o dañe los sistemas de almacenamiento de información relevante del Ministerio de Educación, como, por ejemplo, incendios, terremotos, inundaciones, etc.

k) Integridad: mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.

l) Sistema de Gestión de Continuidad de Servicios: parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del servicio.

m) Sistema de Gestión de Seguridad de la Información: parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

8. Acciones Disciplinarias

La infracción a las obligaciones establecidas en este documento, podrá constituir una violación al principio de probidad administrativa y por ello, acarreará responsabilidad administrativa que 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 en caso de que dicho instrumento así lo contemple o pueda entenderse como una afectación grave al principio de probidad, 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.

9. Marco Normativo

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

b) Ley N.° 17.336, de Propiedad Intelectual, y sus actualizaciones

c) Ley N.° 19.628, sobre Protección de la Vida Privada.

d) Ley N.° 19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Dicha Firma.

e) Ley N.° 20.285, sobre Acceso a la Información Pública.

f) Ley N.° 21.180, sobre Transformación Digital.

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) Decreto Supremo N.° 83 de 2004 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 Supremo N.° 93 de 2006 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.

j) Decreto N.° 273 de 2022 Ministerio del Interior y Seguridad Pública, que establece Obligación de Reportar Incidentes de Ciberseguridad.

k) 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.

l) Política Nacional de Ciberseguridad.

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

n) Norma Chilena NCh-ISO22301:2013 sobre "Seguridad de la sociedad - Sistemas de gestión de la continuidad del negocio – Requisitos".

Lo anterior, sin perjuicio de otras normas que, por su naturaleza, le sean aplicables o las reemplacen, o las que en el futuro se dicten, las que incluyen los instructivos presidenciales que rijan la materia.

10. Vigencia

Esta norma entrará en vigor cuando el acto 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 deberá tomar conocimiento por escrito de la presente política, la cual se encontrará en formato electrónico en la Intranet para futuras consultas.

B. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL SERVICIO

1. Alcance

Los actos administrativos, las instrucciones y las comunicaciones que emita el Subsecretario de Educación como resultado de las propuestas del Comité de Seguridad de la Información y Continuidad del Servicio, se aplicarán a todas las Subsecretarías que componen el Ministerio de Educación, en virtud de lo dispuesto por los artículos 5° y 6° de la Ley N.° 18.956, que Reestructura el Ministerio de Educación.

2. Funciones

El Comité de Seguridad de la Información y Continuidad del Servicio (en adelante el Comité), es un órgano colegiado, cuya labor principal, además de las señaladas en la Política de Seguridad de la Información, será prestar apoyo al (a la) Subsecretario (a) de Educación en la adopción de decisiones en materias relacionadas con la seguridad de la información y la continuidad de los servicios críticos con los que funciona esta entidad.

Por su intermedio, el (la) Subsecretario(a) de Educación determinará, autorizará y vigilará los controles y prácticas de seguridad que ayuden a mejorar los niveles de protección y resguardo de los activos de la institución.

Para ello, el (la) Presidente(a) del Comité, podrá requerir la asistencia de personal de la Subsecretaría de Educación o de consultores externos, conforme a su experiencia, experticia o área de desempeño, en calidad de asesores, en tanto se estime que su participación es necesaria para la correcta adopción de decisiones técnicas específicas y quienes sólo tendrán derecho a ser oídos.

3. Integrantes del Comité

El Comité estará conformado por las personas que ejerzan los cargos que a continuación se señala, o por quienes estas designen especialmente para tal efecto, quienes actuarán con voz y voto:

a) El (La) Jefe(a) de Gabinete de la Subsecretaría de Educación, quién, además, presidirá el Comité.

b) El (La) Jefe(a) de la División de Planificación y Presupuesto de la Subsecretaría de Educación.

c) El (La) Jefe(a) de la División de Administración General de la Subsecretaría de Educación.

d) El (La) Jefe(a) de la División Jurídica de la Subsecretaría de Educación.

e) El (La) Jefe(a) de la División de Educación General de la Subsecretaría de Educación.

f) El (La) Coordinador(a) Nacional de Tecnología (CNT) de la Subsecretaría de Educación.

g) El (La) Encargado(a) de Seguridad de la Información, quien asumirá el rol de Secretario(a) Ejecutivo(a) del Comité.

h) El (La) Jefe(a) de la Unidad de Reducción de Riesgo de Desastres de la Subsecretaría de Educación.

i) El (La) Jefe(a) de la División de Administración y Finanzas de la Subsecretaría de Educación Parvularia.

j) El (La) Jefe(a) de Área Administración y Presupuesto de la Subsecretaría de Educación Superior.

4. Obligaciones y responsabilidades del Comité de Seguridad de la Información y Continuidad del Servicio

Será la entidad encargada de realizar las acciones que se describen a continuación:

a) Proponer las definiciones estratégicas, lineamientos y prioridades, así como también los recursos e insumos, que permitan orientar y focalizar las políticas, planes, programas e iniciativas en materias de seguridad de la información.

b) Adoptar decisiones sobre los riesgos de seguridad y ciberseguridad más críticos y monitorear el avance de los planes de acción para mitigarlos.

c) Impulsar y proponer al (a la) Subsecretario(a) de Educación las políticas y directrices definidas en materia de seguridad de la información.

d) Apoyar y promover la seguridad de la información dentro de la Institución, mediante la difusión, educación y concientización sobre las políticas y otras medidas de seguridad.

e) Prestar asesoría al (a la) Subsecretario(a) de Educación en el establecimiento de los lineamientos necesarios para la implementación y desarrollo adecuado de programas que den continuidad a los servicios.

Se considerará además cualquier otra función que sea necesaria de acuerdo con los objetivos planteados.

5. Sesiones

Las sesiones del Comité serán coordinadas por el (la) Encargado(a) de Seguridad de la Información de la Subsecretaría de Educación, en su carácter

de Secretario(a) Ejecutivo(a) del Comité, ya sean de carácter ordinario o extraordinario, para lo que se aplicará la siguiente pauta de convocatoria:

a) Sesiones Ordinarias: Se llevarán a efecto cada dos meses, previa convocatoria a través de correo electrónico que, al efecto, realice el (la) Presidente(a) del Comité con al menos, 7 días hábiles de anticipación. En la citación, se hará indicación de la fecha, hora y lugar del encuentro, el que será obligatorio para todas las personas que lo integran o para quienes éstas hayan designado.

b) Sesiones Extraordinarias: Se celebrarán por convocatoria que al efecto realice el (la) Presidente(a) del Comité o bien, a solicitud de alguno de sus miembros titulares, y tendrá por único objeto la resolución de algún incidente de seguridad que ponga en riesgo la continuidad operativa del servicio y sin perjuicio de las medidas adoptadas por el Subsecretario de Educación para controlar o disminuir dicho riesgo.

La convocatoria deberá efectuarse con, a lo menos, 7 días hábiles de anticipación, salvo en aquellos casos en que se trate de situaciones de emergencia, debidamente calificadas por el Subsecretario de Educación, o en su defecto, por el (la) Presidente(a), en cuyo caso no regirá esta limitación.

6. Reglas comunes.

La citación de las sesiones, tanto ordinarias como extraordinarias, deberán ser realizadas por oficio o correo electrónico, indicando el lugar, día y hora fijados por el (la) Secretario(a) Ejecutivo(a) del Comité, de conformidad con lo que, al efecto, indique el (la) Presidente(a) del Comité.

b.2) El (La) Encargado(a) de Seguridad de la Información, en su calidad de Secretario(a) Ejecutivo(a) del Comité, levantará un Acta o Minuta de lo obrado y los acuerdos a los que se arribó en cada sesión, la que debe ser suscrita por todos los miembros presentes.

7. Decisiones.

Las decisiones del Comité se adoptarán por mayoría simple de los miembros presentes y sus acuerdos, quedarán registrados en las respectivas actas o minutas, las que serán mantenidas en un registro por el (la) Secretario(a) Ejecutivo(a). Los empates serán resueltos por el voto dirimente del (de la) Presidente(a) del Comité.

8. Tareas del (de la) Presidente(a) del Comité de Seguridad de la Información y Continuidad del Servicio.

Corresponderá al (a la) Presidente(a), las siguientes labores:

a) Representar al Comité de Seguridad de la Información dentro y fuera del Ministerio de Educación.

b) Dirigir los debates en las sesiones.

c) Dirimir con su voto los empates que se produzcan en la toma de decisiones.

d) Someter a la aprobación del Comité los acuerdos que se deriven de las sesiones respectivas y vigilar su cumplimiento.

e) Suscribir los documentos que emita el Comité.

f) Informar al (a la) Jefe(a) de Servicio sobre las decisiones adoptadas en el Comité de Seguridad de la Información."

II. **DÉJASE** sin efecto la Resolución Exenta N.° 296, de 2021, del Ministerio de Educación, que Aprobó Nueva Política de Seguridad de la Información del Ministerio de Educación y Define las Labores del Órgano Encargado de Velar por su Cumplimiento.

ANÓTESE, PUBLÍQUESE INTERNAMENTE Y ARCHÍVESE

ALEJANDRA ARRATIA MARTÍNEZ
SUBSECRETARIA DE EDUCACIÓN

Distribución:

- Gabinete Sr. Ministro
- Gabinete Sr. Subsecretario de Educación
- Gabinete Sra. Subsecretaria de Educación Parvularia
- Gabinete Sra- Subsecretario de Educación Superior
- División Jurídica
- División de Administración General.
- División de Planificación y Presupuestos
- División de Educación General
- Oficina de Partes y Archivos.
- Archivo.
  Expediente N° . .