Gobierno de Chile

MINEDUC DIVISIÓN JURÍDICA

MINISTERIO DE EDUCACIÓN
05 FEB 2021
DOCUMENTO TOTALMENTE TRAMITADO

APRUEBA NUEVA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE EDUCACIÓN Y DEFINE LAS LABORES DEL ÓRGANO ENCARGADO DE VELAR POR SU CUMPLIMIENTO

JPC/RVL/CAD

Solicitud N° 0353

SANTIAGO, 19 ENE 2021

RESOLUCIÓN EXENTA N° 0296

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° 2511 de 10 de mayo de 2019 que establece la Política de Seguridad de la Información del Ministerio de Educación y define las labores del órgano encargado de velar por su cumplimiento; en el Ord. N° 2757 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 la Resolución Exenta N° 2511 de 10 de mayo de 2019 se establece la Política de Seguridad de la Información del Ministerio de Educación y define las labores del órgano encargado de velar por su cumplimiento. Que a través del Ord. N° 2757 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 Seguridad de la Información del Ministerio de Educación y define las labores del órgano encargado de velar por su cumplimiento , 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 normas generales que regulen el uso y manejo de los activos de información de la Institución, a través de las distintas actividades que el personal del Ministerio de Educación realiza en el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los mismos.

Establecer los requisitos y condiciones generales de protección y resguardo de seguridad y ciberseguridad a las que se encuentra sujeta este Ministerio, de acuerdo con las normas legales y reglamentarias pertinentes, así como los riesgos a que están expuestos sus activos de información y, los principios y objetivos internos para el resguardo de sus operaciones.

Que, para la correcta implementación de esta normativa, es necesario contar con una Política de Seguridad de la Información del Ministerio de Educación, la que define las labores del órgano encargado de velar por su cumplimiento.

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.

La seguridad de la información es de responsabilidad de la totalidad de los usuarios que se relacionan con el Ministerio de Educación y que tengan acceso a los

Activos de Información de esta Cartera de Estado, sean estos funcionarios de planta o contrata, u honorarios, e incluye a los asesores, consultores, practicantes y, en general, toda aquella persona natural o jurídica que preste servicios al Ministerio de Educación. Por tal razón, las políticas establecidas en este documento son de conocimiento y cumplimiento obligatorio para todos a quienes se les otorgue acceso a estos activos. En el caso de las personas naturales o jurídicas externas, dicha obligación deberá expresarse en los contratos y/o acuerdos respectivos.

Asimismo, esta Política, es aplicable a todo activo de información que la organización posea actualmente o en el futuro, cubriendo prioritariamente aquellos activos que están asociados a procesos de provisión de los productos y objetivos estratégicos de la institución.

Que, este procedimiento fue elaborado por la División de Planificación y Presupuesto, según consta en Ord. N° 2757 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 Seguridad de la Información del Ministerio de Educación y define las labores del órgano encargado de velar por su cumplimiento", la cual se entiende parte integrante de la presente resolución.

2- Déjese sin efecto la Resolución Exenta N° 2511 de 10 de mayo de 2019 que establece la "Política de Seguridad de la Información del Ministerio de Educación y define las labores del órgano encargado de velar por su cumplimiento".

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

REPUBLICA DE CHILE
MINISTERIO DE EDUCACIÓN
SUBSECRETARIO

LEON PAUL GASTRO
SUBSECRETARIO DE EDUCACIÓN (S)

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

Exp. 42.362 - 2020

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE EDUCACIÓN Y DEFINE LAS LABORES DEL ÓRGANO ENCARGADO DE VELAR POR SU CUMPLIMIENTO.

I. DECLARACIÓN INSTITUCIONAL.

La Ley N° 18.956, que Reestructura el Ministerio de Educación Pública, entrega a la Subsecretaría de Educación, en su calidad de órgano de colaboración directa del Ministro de Educación, la administración interna del Ministerio y la coordinación de los órganos y servicios públicos del sector.

Para apoyar el cumplimiento de los fines institucionales del Ministerio de Educación (en adelante e indistintamente "el Ministerio" o "la Institución"), 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.
Así, los antecedentes que se encuentren en poder de las Subsecretarías que componen el Ministerio de Educación constituyen un bien estratégico del mismo, 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 su cargo y función le corresponda administrar y gestionar, de conformidad al marco legal actualmente vigente.

Lo anterior, sin perjuicio de las facultades para tratar la información que corresponde a cada Subsecretaría en el ejercicio de sus funciones, así como de las facultades y deberes legales que sobre ella puedan tener, particularmente, en los términos establecidos en la Ley N° 19.628, sobre protección de la vida privada. De este modo, el resguardo de la misma sólo corresponderá a la Subsecretaría de Educación en la medida que esté soportada en sus plataformas, por lo tanto, no podrá hacer uso de los datos o información obtenidos por las otras Subsecretarías en cumplimiento de las normas que las rigen, salvo instrucción expresa del respectivo Subsecretario, el que será responsable del uso que se dé a la misma en los términos que la ley establece.

De este modo, es de suma importancia el correcto manejo de los activos de información, entendiéndose por tales a todo elemento en que se registre, almacene y/o procesen datos, sea a través de medios tecnológicos u otros soportes, tales como: sistemas informáticos, bases de datos y archivos, contratos y acuerdos, documentación de sistemas, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de continuidad operativa, información de auditorías, información archivada, activos de software, activos físicos como salas de computación, computadores y servidores, impresoras y redes de comunicaciones y servicios.

Debe considerarse, además, que las Subsecretarías que componen el Ministerio de Educación, tanto en sus sistemas de información y aplicativos, como en las respectivas redes, está enfrentando en forma creciente, constantes amenazas de seguridad desde una amplia gama de fuentes, tales como hechos naturales, fallas propias en los equipos, aplicaciones, o bien ataques intencionales, por lo que sus sistemas informáticos requieren estar total e integralmente protegidos, asegurando la continuidad operacional de los procesos.

Lo anterior significa el deber de contar con una preparación apropiado, en orden a reaccionar adecuadamente en caso de situaciones o eventos inesperados que impliquen una interrupción de los procesos de provisión de productos estratégicos[1]. Para ello, es necesario desarrollar las estrategias y planes que resulten necesarios para actuar de una manera eficaz, oportuna, ordenada y sistemática.

En esta línea, la seguridad de la información y la ciberseguridad deben ser considerados como componentes claves y estratégicos para el cumplimiento de los objetivos y la preservación de la imagen reputacional de la Institución.

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

1. Objetivos

Los objetivos de esta política son:

1. Establecer normas generales que regulen el uso y manejo de los activos de información de la Institución, a través de las distintas actividades que el personal del Ministerio de Educación realiza en el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los mismos.

2. Establecer los requisitos y condiciones generales de protección y resguardo de seguridad y ciberseguridad a las que se encuentra sujeta este Ministerio, de acuerdo con las normas legales y reglamentarias pertinentes, así como los riesgos a que están expuestos sus activos de información y, los principios y objetivos internos para el resguardo de sus operaciones.

2. Alcance

[1] Se entenderá por procesos estratégicos aquellos identificados en la Ficha de Definiciones Estratégicas de la Subsecretaría de Educación (Formulario A1), que publica la Dirección de Presupuesto.

La seguridad de la información es de responsabilidad de la totalidad de los usuarios que se relacionan con el Ministerio de Educación y que tengan acceso a los Activos de Información de esta Cartera de Estado, sean estos funcionarios de planta o contrata, u honorarios, e incluye a los asesores, consultores, practicantes y, en general, toda aquella persona natural o jurídica que preste servicios al Ministerio de Educación. Por tal razón, las políticas establecidas en este documento son de conocimiento y cumplimiento obligatorio para todos a quienes se les otorgue acceso a estos activos. En el caso de las personas naturales o jurídicas externas, dicha obligación deberá expresarse en los contratos y/o acuerdos respectivos.

Asimismo, esta Política, es aplicable a todo activo de información que la organización posea actualmente o en el futuro, cubriendo prioritariamente aquellos activos que están asociados a procesos de provisión de los productos y objetivos estratégicos de la institución.

3. Roles y Responsabilidades

Subsecretario de Educación: En su calidad de Jefe Administrativo 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.

Encargado de Seguridad de la Información de la Subsecretaría de Educación: 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 la respuesta a 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.

Coordinador Nacional de Tecnología de la Subsecretaría de Educación: le corresponderá tomar las medidas necesarias para resguardar los activos de información y mantener su disponibilidad, confiabilidad e integridad, de acuerdo con las directrices establecidas por la Resolución Exenta N° 4.505, de 2014, de este origen y, asimismo todas aquellas que se señalan

en la presente Política, controladas por el Comité de Seguridad de la Información.

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;
e) Proponer capacitaciones pertinentes para el personal del Ministerio de Educación;
f) Realizar capacitaciones a dicho personal referidas a la política de seguridad informática 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.

Sin perjuicio de lo anterior, y puestos en conocimiento de las personas que se desempeñan en las Subsecretarías que integran el Ministerio de Educación, será su obligación el respeto de los lineamientos que emanen de la presente política.

4. Organización de la Seguridad

El Ministerio de Educación contará con un **"Comité de Seguridad de la Información y Continuidad del Servicio"**, un órgano colegiado, cuya labor principal será prestar apoyo al Subsecretario 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 Subsecretario 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 Secretaría de Estado.

Este órgano deberá dictaminar marcos de trabajo sobre seguridad, ciberseguridad y continuidad, que incluya 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 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

El Ministerio de Educación mantendrá una organización para la gestión de la seguridad de la información basada en los requisitos de la norma NCh-ISO 27001:2013, a través de un programa de implementación de controles de seguridad basado en las recomendaciones NCh-ISO 27002:2013, alineado con el cumplimiento de lo establecido en la legislación vigente. Sin embargo, para ámbitos específicos y con el fin de contribuir de mejor manera a esta Política, se podrán considerar otras normativas o marcos de trabajo relacionadas con la materia, como referencia.

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

Esto 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 normativas se entienden parte de esta política.

1. La Política de Seguridad de la Información de este Ministerio de Educación, 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.
2. 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.
3. A partir de esta política general de seguridad de la información se elaborarán documentos específicos relativos a la materia, que establecerán los requisitos de seguridad en los dominios que la norma identifica.
4. Es responsabilidad de todos los funcionarios del Ministerio de Educación y, los terceros relacionados con el manejo de los activos de información de la Institución, hacer uso de los mismos 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.
5. 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.

6. Asimismo, la ciberseguridad debe estar incorporada en los procesos que se abordan anualmente en la matriz de riesgos institucional.
7. Por otra parte, es obligación de todos los funcionarios del Ministerio de Educación, relacionados con el manejo de los activos de información de la Institución, 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.
8. Por último, la institución reconoce que las actividades de capacitación, concientización y sensibilización de sus funcionarios 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

El Ministerio 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 programa de continuidad anual debe propender a la mejora continua y será preparado en el marco de los recursos disponibles.

Para dichos efectos, el programa de continuidad considerará aspectos tales como: identificación de las amenazas potenciales, evaluación del riesgo y su impacto en los procesos estratégicos del Ministerio de Educación, 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:

1. La definición y documentación de las estrategias de prevención y recuperación del servicio ante eventos detonantes de contingencias, desastres o emergencias.
2. Los riesgos de ciberseguridad asociados a dichos eventos detonantes.
3. El establecimiento de estrategias y planes para enfrentar desastres que comprometan la continuidad del servicio.
4. 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.

5. 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.
6. 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.
7. Que, en el caso de fallas operativas normales y mantenciones de sistemas, sean los dueños de los servicios, las personas responsables por desarrollar y mantener los procedimientos de recuperación asociados.
8. 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

Activo: aquello que tenga valor para la organización.
Activo de información: todo elemento en que se registre, almacene y/o procese datos e información, sea a través de medios tecnológicos u otros soportes, tales como: bases de datos y archivos, contratos y acuerdos, documentación de sistemas, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de continuidad operativa, información de auditorías, información archivada, activos de software, activos físicos como salas de computación, computadores y servidores, impresoras y redes de comunicaciones y servicios
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.
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.
Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
Continuidad del servicio: capacidad de la organización para continuar entregando productos o servicios a niveles aceptables predefinidos tras un incidente que interrumpa.
Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
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.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.
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.
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 anteriormente, podrá constituir una violación al principio de probidad administrativa y por ello, será sancionada en conformidad a lo dispuesto en la Ley N° 18.834, sobre Estatuto Administrativo, cuyo texto refundido, coordinado y sistematizado fue fijado por el D.F.L. N° 29, de 2004, del Ministerio de Hacienda, respecto de los dependientes que detentan la calidad de funcionarios públicos o sean administrativamente responsables por disposición de la ley. Todo lo anterior, sin perjuicio de la responsabilidad civil o penal que pudiera concurrir.

Por su parte y, respecto del personal a Honorarios o de carácter Externo al Ministerio de Educación, la infracción a las obligaciones que son materia de la presente política podrá constituir causal suficiente para producir el término inmediato y anticipado del respectivo contrato que los vincule con la Institución, sin perjuicio de otras responsabilidades civiles o penales, que la infracción pudiere irrogarles.

En esta materia, la Coordinación Nacional de Tecnología de la Subsecretaría de Educación 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.

9. Legislación

La presente Política de Seguridad de la Información tiene como fuentes las normas que se indica a continuación:

Ley N° 17.336, de Propiedad Intelectual, y sus actualizaciones
Ley N° 19.223, que Tipifica Figuras Penales relativas a la Informática.
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.
Ley N° 20.285, sobre Acceso a la Información Pública.
Ley N° 18.834, sobre Estatuto Administrativo, cuyo texto refundido, coordinado y sistematizado fue fijado por el D.F.L. N° 29, de 2004, del Ministerio de Hacienda Decreto Supremo N° 83 del 2005 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 del 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.
Norma Chilena NCh-ISO27001:2013 sobre "Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos".
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 que en el futuro se dicten, las que incluyen los instructivos presidenciales que rijan la materia.

III. 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, obligarán 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.

2. Funciones

El Comité de Seguridad de la Información y Continuidad del Servicio, en adelante e indistintamente, "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 Subsecretario 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 Subsecretario 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 Ministerio de Educación.

Para ello, el Presidente del Comité, en adelante e indistintamente "el Presidente", 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. Integración del Comité

El Comité de Seguridad de la Información y Continuidad del Servicio, estará conformado por las personas que ejerzan los cargos que a continuación se señala, o por quienes estas designen especialmente para tal efecto, todos quienes actuarán con voz y voto:

a) El Jefe de la División de Planificación y Presupuesto de la Subsecretaría de Educación, quién, además, presidirá el Comité;
b) El Jefe de la División de Administración General (DAG) de la Subsecretaría de Educación;
c) El Jefe de la División Jurídica de la Subsecretaría de Educación;
d) El Coordinador Nacional de Tecnología (CNT) de la Subsecretaría de Educación;
e) El Encargado de Seguridad de la Información, quien asumirá el rol de Secretario Ejecutivo del Comité;
f) La jefa de la Unidad de Reducción de Riesgo de Desastres de la Subsecretaría de Educación.
g) El Jefe de la División de Administración y Finanzas de la Subsecretaría de Educación Parvularia.
h) La Jefa 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

a) Proponer al Subsecretario de Educación el o los planes de mejoramiento de la seguridad de la Información.
b) Revisar el estado de avance de dichos planes y, asimismo, adoptar todas las medidas que resulten necesarias, en caso de que existan modificaciones en la planificación antes mencionada.
c) Proponer uno más planes de acción al Subsecretario de Educación que resulten necesarias para prevenir y resolver los incidentes de seguridad de la Información.
d) Diseñar la alineación de los objetivos de seguridad de la información con los objetivos estratégicos institucionales.
e) Proponer la aprobación, promoción y control del cumplimiento de las políticas y estándares para el adecuado uso de los activos de información, a la autoridad pertinente.
f) Prestar asesoría al Subsecretario de Educación en el establecimiento de los lineamientos necesarios para la implementación y desarrollo adecuado de programas que den continuidad a los servicios.

Y, en general, cualquier otra función que sea necesaria de acuerdo con los objetivos planteados.

5. Sesiones

Las sesiones del Comité serán coordinadas por el Encargado de Seguridad de la Información de la Subsecretaria de Educación, en su carácter de Secretario Ejecutivo del Comité, ya sean de carácter ordinario o extraordinario, para lo que se aplicará la siguiente pauta de convocatoria:

a) Sesiones Ordinarias.

Éstas se llevarán a efecto cada dos meses, previa convocatoria a través de correo electrónico que, al efecto, realice el Presidente 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 Presidente 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 Presidente, en cuyo caso no regirá esta limitación.

c) 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 Secretario Ejecutivo del Comité, de conformidad con lo que, al efecto, indique el Presidente del Comité.

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

6. 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 Secretario Ejecutivo del Comité.

Los empates serán resueltos por el voto dirimente del Presidente del Comité.

7. Tareas del Presidente del Comité de Seguridad de la Información y Continuidad del Servicio.

Corresponderá al Presidente, 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 Jefe de Servicio sobre las decisiones adoptadas en el Comité de Seguridad de la Información.

8. De los Incidentes de Seguridad de la Información.

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

a) Robo o pérdida de un equipo que almacena información, como por ejemplo un computador personal o un teléfono inteligente que contenga información sensible.
b) Robo o pérdida de documentación sensible como por ejemplo informes (en papel o digitales), archivadores, contratos, etc.
c) Filtraciones de datos sensibles hacia el exterior, como por ejemplo datos de funcionarios, estudiantes, sostenedores, establecimientos educacionales, etc.
d) 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.
e) Presencia de virus, código malicioso u otro tipo de infección computacional.
f) Fallas graves en sistemas informáticos institucionales.
g) Ingresos no autorizados a los sistemas de información, como por ejemplo uso de cuentas ajenas.
h) 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.