Superintendencia de Educación
TOTALMENTE TRAMITADO

Gobierno de Chile

Superintendencia de Educación

MIC/CBC/FTO/AAM/PBC/PSY

DÉJA SIN EFECTO RESOLUCIÓN EXENTA N° 703, DE 2017 Y APRUEBA VERSIÓN 4.0 DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN, DE LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA Nº 0871

Santiago, 04 DIC 2018

VISTO:

Lo dispuesto en el DFL Nº 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en el Decreto con Fuerza Ley Nº 29, de 2004, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley Nº 18.834, sobre Estatuto Administrativo; en la Ley Nº 19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; en el Decreto N°132, de 2018, del Ministerio de Educación; en la Ley Nº 20.529, de 2011, del Ministerio de Educación, sobre el Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización; en el Decreto con Fuerza de Ley Nº 5, de 2012, del Ministerio de Educación; en la Norma Chilena NCh-ISO 27001/2013 tecnología de la información-técnicas de seguridad-sistemas de gestión de la seguridad de la información; en la norma Chilena NCh-ISO 27002-2013, tecnología de la información- código de prácticas para la gestión de la seguridad de la información; en las Resoluciones Exentas N°s 1592, de 2016 y 703 de 2017, ambas de la Superintendencia de Educación, y en la Resolución N°1600 de 2008, de Contraloría General de la República, que fija las normas sobre exención del trámite de toma de razón y sus modificaciones.

CONSIDERANDO:

1. Que, de acuerdo a lo dispuesto en el artículo 47 de la Ley N°20.529, sobre el Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su fiscalización, se crea la Superintendencia de Educación, como "un servicio público funcionalmente descentralizado y territorialmente desconcentrado, dotado de personalidad jurídica y patrimonio propio y que se relaciona con el Presidente de la Republica por intermedio del Ministerio de Educación".

2. Que, mediante Resolución Exenta N° 0570, de fecha 03 de agosto de 2018, se nombró al Comité de Seguridad de la Información Institucional, para que, en función del marco legal y tecnológico, proponga a este Jefe de Servicio, una Política de Seguridad de la Información, la implante, mantenga y mejore en el tiempo.

3. Que, en razón de lo anterior, mediante Resolución Exenta N° 703, de fecha 17 de octubre de 2017, se aprueba versión N°3, de la Política General de Seguridad de la Información, de esta Superintendencia de Educación.

4. Que, debido a una serie de cambios al interior del servicio y a la necesidad de contar con procedimientos que se adecuen de mejor manera a los requisitos institucionales, el Comité de Seguridad de la Información ha estimado por acuerdo unánime ajustar y actualizar el contenido de la Política General de Seguridad de la Información, para la Superintendencia de Educación, Versión 3.0 aprobado mediante la Resolución Exenta señalada precedentemente.

RESUELVO:

1° DÉJASE, sin efecto la Resolución Exenta N° 0703, de fecha 17 de octubre de 2017, de la Superintendencia de Educación.

2° APRUÉBASE, la versión 4.0 de la Política General de Seguridad de la Información, de la

Política General de Seguridad de la Información
Superintendencia de Educación

Versión N°4.0

CONTROL ISO27001:2013
A.5.1.1

Tabla de Contenidos

Superintendencia de Educación, cuyo texto es el siguiente:

ELABORADO POR	REVISADO POR	APROBADO POR
Pablo Silva Yañez **Encargado de Seguridad de la Información**	**Angie Aracena Medina** **Comité Operativo Seguridad de la Información**	**Mauricio Irarrazabal Cerpa** **Comité Directivo Seguridad de la Información**

1. Declaración institucional

Gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, y que consiste básicamente en la realización de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles adecuados **de integridad, confidencialidad y disponibilidad**, de todos los activos de información relevantes para la institución, como un principio clave en la gestión de sus procesos.

En el entendido de que los riesgos que se logren identificar estarán siempre presentes, ya que no se pueden eliminar, la Superintendencia de Educación se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, a través de un programa de implantación de lo que se denominará un "**S**istema de **G**estión de **S**eguridad de la **I**nformación (SGSI)", basado en la norma chilena **NCH ISO 27001:2013**, tendiente a homogeneizar los criterios de seguridad, con el objetivo de preservar los activos de información institucional con respecto a:

- **SU INTEGRIDAD:** La información estará correcta y sin grado de corrupción alguno.
- **SU CONFIDENCIALIDAD:** La información estará debidamente protegida, y permitiendo el acceso solamente a las personas autorizadas.
- **SU DISPONIBILIDAD:** La información estará disponible y accesible en forma oportuna cuando sea requerida por aquellas personas debidamente autorizadas.

La implementación del SGSI permite asegurar la continuidad operacional de los procesos y servicios de la Superintendencia de Educación

2. Objetivos de la gestión de seguridad de la información

2.1. Proteger eficientemente los activos de información institucionales, asegurando su confidencialidad, integridad y disponibilidad.
2.2. Establecer procedimientos, instrucciones u otros documentos para la clasificación y catastro de los activos de información de la Superintendencia de Educación.
2.3. Establecer procedimientos para efectuar una evaluación anual de riesgos destinada a proteger eficazmente los activos de información de la Superintendencia de Educación y prevenir la ocurrencia de incidentes de seguridad de la información.
2.4. Definir una estructura y un marco de políticas, estándares y procedimientos en materia de seguridad de la información dentro de la Superintendencia de Educación.
2.5. Establecer los mecanismos de difusión de la presente Política para el conocimiento de todos los funcionarios de planta y a contrata y personal a honorarios del Servicio, especialmente en lo referente a capacitaciones periódicas en materias de seguridad de la información.
2.6. Establecer los mecanismos de difusión de la presente Política para el conocimiento de terceras partes, especialmente en lo referente a la confidencialidad de la información de la que tome conocimiento mientras dure el contrato y convenios, sus derechos y obligaciones en materia de seguridad de la información del Servicio y las consecuencias en caso de no cumplimiento en materias de seguridad de la información, que se establecen en los respectivos contratos y convenios.
2.7. Mantener la continuidad de sus procesos.

3. Alcance o amplitud de la política de seguridad de la información

El ámbito de aplicación de la Política de Seguridad contempla los dominios contenidos en la Nch-ISO 27002:2013 y que son los siguientes:

1) Políticas de Seguridad de la Información.
2) Organización de la seguridad de la información.
3) Seguridad Ligada a Recursos Humanos.
4) Gestión de Activos.
5) Control de Acceso.
6) Criptografía.
7) Seguridad Física y Ambiental.
8) Seguridad en las Operaciones.
9) Seguridad en las Comunicaciones.
10) Adquisición, desarrollo y mantenimiento de los sistemas de información.
11) Relación con Proveedores.
12) Gestión de Incidentes de Seguridad de la Información.
13) Aspectos de Seguridad de la Información en la Gestión de Continuidad de Negocio.
14) Cumplimiento.

La presente política, y aquellas asociadas, son aplicables a todas las autoridades de gobierno, funcionarios, personal a honorarios, funcionarios en comisión de servicio que efectivamente se desempeñen en la institución o cualquier persona, clientes y proveedores que esté involucrada con

los activos de información institucionales y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas de la Institución.

El Comité de Seguridad es responsable de implantar esta política y tendrá el apoyo de la Alta Dirección de la Superintendencia de Educación, quien la ha aprobado.

4. Referencia normativa

El marco legal para el Sistema de Seguridad de la información se señala en el documento "Listado de normativa vigente aplicable a la Superintendencia de Educación" publicado en la Intranet.

5. Definiciones

Concepto	Descripción
Manual de Seguridad	Manual que integra el marco normativo de la Seguridad de la Información en la Superintendencia de Educación, consistente en buenas prácticas que definen la protección de la confidencialidad, disponibilidad de integridad de los activos de información institucionales.
Activos de Información	Recursos del sistema de información, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Una organización incluye diferentes tipos de activos: - Activos relacionados con el entorno (edificios, instalaciones, equipamientos) y personal. - Activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones). - Activos relacionados con la información (datos, metadatos y soportes). - Activos relacionados con las funcionalidades de la organización (productos, servicios). - Activos intangibles (credibilidad, conocimiento acumulado).
Riesgo	Se entiende por la contingencia de un daño a un activo de información. A su vez contingencia significa que el daño en cualquier momento puede materializarse o no hacerlo nunca.
Seguridad de la Información	Proceso encargado de asegurar que los recursos de un sistema de información sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.
Proceso	Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un determinado fin.
Incidente de seguridad	Cualquier evento o situación que comprometa de manera IMPORTANTE la disponibilidad, integridad y confidencialidad de la información, junto con la plataforma tecnológica, procesos y aplicativos que permitan acceder a esta en forma oportuna. En general es una violación de una política, estándar o procedimiento de seguridad que no permita dar un servicio computacional.
Integridad	Se entiende por la corrección y completitud de los datos o de la información manejada.
Confidencialidad	Es la propiedad de un documento o mensaje que únicamente está autorizado para ser leído o entendido por algunas personas o entidades.
Disponibilidad	Es el aseguramiento de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando es requerido.
Encargado de Seguridad	Persona responsable por la implementación de medidas de control que garanticen la seguridad de la información. Adicionalmente es responsable de la coordinación entre los distintos comités de seguridad.
Comité de Seguridad de la Información Institucional	Agrupación de personas directivas que tienen como misión validar y aprobar las políticas de seguridad de la información y los controles tendientes a regular el uso y manejo de la información.

6. Roles y responsabilidades

Rol	Responsabilidad
Comité de Seguridad de la Información Institucional	a) Responsable del ciclo de vida de las políticas en la Superintendencia de Educación. b) Validar, y difundir las políticas a través de la Intranet y los medios de comunicación establecidos dentro de la Superintendencia de Educación. c) Velar por la implementación de los controles de seguridad en la plataforma tecnológica. d) Promover la realización de los cursos en formato e-learning de Seguridad de la información para todos los funcionarios. e) Revisar, al menos una vez al año, el funcionamiento del SGSI.
Jefe del Departamento de Gestión de Personas	a) Incorporar, de acuerdo a la disponibilidad de recursos, el tema de aplicación y observancia de las políticas de seguridad de la información en plan de capacitación institucional. b) Velar por la correcta inducción de los funcionarios en materias de seguridad de la información.
Encargado de Seguridad de la Información	a) Proponer, desarrollar y actualizar las políticas de seguridad de la información al interior de la institución, coordinar su implementación y evaluación, velando por su correcta aplicación. b) Promover acciones en materia de seguridad de la información que permitan mantener la continuidad de los procesos de la institución. c) Coordinar la respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información institucionales. ante incidentes de seguridad de la información. d) Mantener coordinación con otras unidades de la Superintendencia para apoyar los objetivos de seguridad. e) Establecer enlaces con encargados de seguridad de la información de otros organismos públicos, con las instancias gubernamentales encargadas de S.I y con especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos de seguridad de la información pertinentes. f) Mantener actualizado el registro de activos de información del Servicio, de acuerdo a los procedimientos definidos. g) Mantener informado periódicamente al Comité Directivo de Seguridad de la Información acerca del estado del Sistema de Seguridad de la Información en la Institución. h) Promover acciones tendientes a la difusión y sensibilización respecto a la Seguridad de la Información a los funcionarios y al personal a honorarios vinculado a la institución.
Usuarios(as)	Son las personas, funcionarios o personal externo que preste servicios permanentes o temporales, que usan los activos de información y los sistemas de procesamiento. Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente, así como las políticas específicas, normas y procedimientos asociados al SGSI y además tienen la obligación de reportar cualquier incidente de seguridad del que tengan conocimiento.
Jefaturas de la SUPEREDUC	Las jefaturas de las Divisiones, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política, así como las políticas específicas, normas y procedimientos asociados al SGSI

7. Directrices

7.1. Marco para la gestión de la seguridad de la información

7.1.1. El Comité de Seguridad adoptará para todo efecto lo dictado en la norma estándar NCH ISO 27001:2013 constituyéndose está en la base de todo el marco de gobernabilidad de la seguridad.

7.1.2. Dentro de las condiciones básicas de la norma antes mencionada, se deberá implementar un conjunto de políticas tendientes a velar por la implementación de las buenas prácticas de seguridad en los diferentes campos y ámbitos del quehacer de la Superintendencia de Educación.

7.1.3. El Encargado de Seguridad, velará por la existencia y actualización de un conjunto organizado de Políticas de Seguridad que pongan de manifiesto el enfoque de la institución con respecto a la gestión de la seguridad de la información y formalicen su compromiso con la protección de la información.

7.2. Tareas y funciones del Comité de Seguridad

El desarrollo, actualización y promoción de esta política general de seguridad de la información, lo ejercerá el Comité de Seguridad de la Información Institucional.

7.3. Marco general para la normativa de seguridad de la información

Objetivos de seguridad

Los objetivos a cumplir por parte de normativa de seguridad de la información en la Superintendencia de Educación son los siguientes:

7.3.1. Integrar el modelo de seguridad con las metodologías y políticas existentes en la Superintendencia de Educación.

7.3.2. Cumplir con las normas legales y reglamentarias referidas a seguridad, tanto para la información, como para los medios que la contienen.

7.3.3. Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.

7.3.4. Garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles.

7.3.5. Asegurar que los empleados y contratistas entiendan sus responsabilidades, que sean aptos para los roles para los cuales están siendo considerados y que estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información.

7.3.6. Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.

7.3.7. Identificar los activos de la organización y definir las responsabilidades de protección pertinentes.

7.3.8. Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.

7.3.9. Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.

7.3.10. Restringir el acceso a la información y a las instalaciones de procesamiento de información.

7.3.11. Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios.

7.3.12. Responsabilizar a los usuarios del cuidado de su información de autenticación.

7.3.13. Evitar el acceso sin autorización a los sistemas y aplicaciones.

7.3.14. Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización.

7.3.15. Prevenir pérdidas, daños, hurtos o el compromiso de los activos, así como la interrupción de las actividades de la organización.

7.3.16. Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

7.3.17. Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.

7.3.18. Proteger en contra de la pérdida de datos.

7.3.19. Registrar eventos y generar evidencia.

7.3.20. Asegurar la integridad de los sistemas operacionales.

7.3.21. Evitar la explotación de las vulnerabilidades técnicas.

7.3.22. Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

7.3.23. Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.

7.3.24. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

7.3.25. Asegurar que la seguridad de la información sea parte integral de los sistemas de información en todo el ciclo.

7.3.26. Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.

7.3.27. Asegurar la protección de los datos usados en ambientes de desarrollo y testing.

7.3.28. Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores.

7.3.29. Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor.

7.3.30. Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

7.3.31. Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del servicio de la institución.

7.3.32. Asegurar la disponibilidad de las instalaciones de procesamiento de la información.

7.3.33. Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.

7.3.34. Asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos de la institución.

8. Evaluación y Difusión

La presente política será evaluada por el Superintendente de Educación al menos una vez al año o, bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.

Una vez que el documento entre en vigencia el responsable de su elaboración deberá difundir al personal considerado en el alcance mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrán ser intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

9. Revisión del cumplimiento de la Política

Con una periodicidad concordante a la de la evaluación definida en el punto anterior, y a través de auditorías, ya sean internas o externas, y en tanto los recursos institucionales se encuentren disponibles para ello, se revisará el cumplimiento de la presente política con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento de la misma.

10. Aceptación

Todos los usuarios de la SUPEREDUC, sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar ésta política y procedimientos relacionados.

Para el caso de terceros y por solo hecho de participar en algún proceso de compras del servicio, el oferente debe dar cumplimiento a la política y procedimientos vigentes de seguridad de la información de la SUPEREDUC, publicados en el sitio web www.supereduc.cl y sus correspondientes modificaciones, la cuales se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

11. Sanciones

El incumplimiento o violación a esta Política, de las Políticas específicas del Sistema, Procedimientos u otros documentos que se deriven de éstos, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios/as de la SUPEREDUC, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

12. Excepciones

La presente Política, y las Políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el

Encargado/a de Seguridad de la Información y debidamente autorizados por la Jefatura de Gabinete.

REVISIONES DE LA POLÍTICA			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
01	21/10/2014	Elaboración del documento Rex N°1112 de 21.10.2014	Todas las paginas
02	21/12/2015	En revisión realizada por el comité Directivo, se decide actualizar la Política General de Seguridad de la Información.	Todas las paginas
03	26/10/2017	En revisión realizada por el comité Directivo, se acuerda actualizar la Política General de Seguridad de la Información.	Se deja sin efecto documento Rex N° 1422 de 26.10.2015 Reestructuración y ajuste al documento. Se elimina de la portada: "nota de confidencialidad de acuerdo a clasificación". Se incorpora en el punto N°3 alcance: "y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas de la Institución." Punto N°6: Encargado de Seguridad de la información, se modifica por completo este punto. Punto N°6: Usuarios, se modifica por completo este punto. Revisión y medición punto N° 9: Se cambia las palabras mantenida y actualizada a "evaluada y revisada al menos una vez al año o cuando ocurran cambios significativos para el SSI". Se modifica por completo el punto N°10 Aceptación. Se modifica por completo el punto N°11 Sanciones. Se incorpora el punto: N°12 Excepciones. Se incorpora el punto: N°14 Tabla de modificaciones. Se incorpora el punto: N°15 Responsabilidades de elaboración y aprobación del documento.
04	12/11/2018		Se deja sin efecto documento Rex N° 0713 de 17.10.2017. Se cambia formato de la política. Punto N°1: Se modifica por completo este punto. Punto N°5: Se elimina letra b. Punto N°6: Se modifica letra i), iii), iv), v), viii) Punto N°8: Se modifica: por completo este punto. Punto N°9: Se modifica: por completo este punto.

REVISIONES DE LA POLÍTICA			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
			Punto 11,12,13,14, 15 y 16 se modifican su numeración.

3° ESTABLÉZCASE, que anualmente se deberá efectuar una evaluación y revisión tanto del contenido, como del cumplimiento de la Política de Seguridad de la Información de la Superintendencia de Educación, por parte del Comité Directivo de Seguridad de la Información o cuando se produzca un cambio o incidente significativo que la impacte.

4° REMÍTASE, copia de la presente Resolución Exenta todas las Divisiones, Departamentos, Unidades y Direcciones Regionales de la Superintendencia de Educación, de acuerdo a la distribución indicada en la presente resolución

5° PUBLÍQUESE, una vez totalmente tramitada la presente Resolución Exenta, en la Intranet institucional y en el sitio web www.supereduc.cl.

ANÓTESE, COMUNÍQUESE Y ARCHÍVASE.

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACIÓN

SEBASTIÁN IZQUIERDO RAMÍREZ
SUPERINTENDENTE
SUPERINTENDENCIA DE EDUCACIÓN

Distribución:

- Gabinete Superintendente.
- Jefes/as de División.
- Intendente/a de Educación Parvularia.
- Directores Regionales I a XVI región.
- Jefe/a Departamento de Finanzas.
- Jefe/a Departamento Gestión de Personas.
- Jefe/a Departamento de Administración.
- Jefe/a Departamento de Tecnologías de Información.
- Unidad de Gestión Institucional.
- Unidad de Auditoria.
- Unidad de Transparencia.
- Encargado de Seguridad de la Información.
- Oficina de Partes.