Superintendencia de Educación
Ministerio de Educación
Gobierno de Chile

MIC/FTO/AAM/PRC/DLR

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0871, DE 2018 Y APRUEBA VERSIÓN N°5 DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN, DE LA SUPERINTENDENCIA DE EDUCACIÓN

RESOLUCIÓN EXENTA Nº 0723

Santiago, 17 DIC 2019

Superintendencia de Educación
TOTALMENTE TRAMITADO

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 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 674 y 871, ambas de 2019, de la Superintendencia de Educación; en el Oficio Gab. Pres. N° 008, de 23 de octubre de 2018, del Presidente de la República, por el cual imparte instrucciones en materia de ciberseguridad y Oficio Gab. Pres. N°001 de 2019, de Presidencia, que proporciona lineamientos para la transformación digital de la Administración del Estado, y en las Resoluciones N°s 6 y 7, 2019, de Contraloría General de la República, que fija las normas sobre exención del trámite de toma de razón.

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° 0698, de fecha 10 de diciembre de 2019, 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 el Comité de Seguridad de la Información Institucional, mediante Resolución Exenta N° 0871, de fecha 04 de diciembre de 2018, aprueba la versión N°4, de la Política General de Seguridad de la Información, de esta Superintendencia de Educación.

4. Que, debido a una serie de cambios institucionales y a la necesidad de contar con políticas y procedimientos que se adecuen de mejor manera a los requisitos institucionales y de Gobierno, el Comité Directivo 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 N°4 aprobado mediante la Resolución Exenta señalada precedentemente.

5. Que, a través del Oficio Gab. Pres. Nº008, de 2018, de Presidencia, se ha proporcionado instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

6. Que, a través del Oficio Gab, Pres. N°001 de 2019, de Presidencia, se ha proporcionado lineamientos para la transformación digital de la Administración del Estado, a través de la simplificación de los procesos, la digitalización de trámites y, en general, el aprovechamiento de las tecnologías para optimizar y mejorar el funcionamiento de sus órganos.

RESUELVO:

1. **DÉJASE,** sin efecto la Resolución Exenta N° 0871, de fecha 04 de diciembre de 2018, de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°5 de la Política General de Seguridad de la Información, de la Superintendencia de Educación, cuyo texto es el siguiente:

Política general de seguridad de la información
Versión N°5

Tabla de Contenidos

1. Declaración institucional 3
2. Objetivos de la gestión de seguridad de la información 3
3. Alcance o amplitud de la política de seguridad de la información 4
4. Referencia normativa 4
5. Definiciones 4
6. Roles y responsabilidades 5
7. Directrices 6
   7.1. Marco para la gestión de la seguridad de la información 6
   7.2. Tareas y funciones del Comité de Seguridad 7
   7.3. Marco general para la normativa de seguridad de la información 7
8. Evaluación y Difusión 9
9. Revisión del cumplimiento de la Política 9
10. Aceptación 9
11. Sanciones 9
12. Excepciones 10

ELABORADO POR	REVISADO POR	APROBADO POR
DANIELA LLANO RECABAL ENCARGADA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	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 sus 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 mantención del "**S**istema de **G**estión de **S**eguridad de la **I**nformación (SGSI)", basado en la norma chilena **NCH ISO 27001:2013** y en los lineamientos de ciberseguridad entregado por Presidencia, tendiente a homogeneizar los criterios de seguridad y ciberseguridad, con el objetivo de preservar los activos de información institucional con respecto a:

- **SU INTEGRIDAD:** La información y los activos de información estarán correctos y sin grado de corrupción alguno.

- **SU CONFIDENCIALIDAD:** La información y los activos de información estarán debidamente protegidos, y permitiendo el acceso solamente a las personas autorizadas.

- **SU DISPONIBILIDAD:** La información y los activos de información estarán disponibles y accesibles en forma oportuna cuando sea requerida por aquellas personas debidamente autorizadas.

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

2. Objetivos

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 un ambiente razonablemente seguro, alineado a la misión de la Superintendencia de Educación, resguardando el uso adecuado de los recursos y gestión del riesgo, con el fin de mantener la continuidad de sus procesos. Monitorear el cumplimiento de los procedimientos, normal y políticas de seguridad de la información, mediante el uso de herramientas de diagnósticos y auditorías internas planificadas a intervalos regulares y de acuerdo a la disponibilidad de recursos en la institución.
2.8. Implementar acciones correctivas y de mejoras al Sistema de Gestión de Seguridad de la Información.
2.9. Ejecutar, aplicar e implementar las medidas de ciberseguridad instruidas mediante el oficio a Gab. Pres. Nº 008, de Presidencia, donde se proporcionan lineamientos para la transformación digital de la Administración del Estado.

3. Alcance

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

3.1. Políticas de Seguridad de la Información.

3.2. Organización de la seguridad de la información.

3.3. Seguridad relativa a los Recursos Humanos.

3.4. Gestión de Activos.

3.5. Control de Acceso.

3.6. Criptografía.

3.7. Seguridad Física y del entorno.

3.8. Seguridad de las Operaciones.

3.9. Seguridad de las Comunicaciones.

3.10. Adquisición, desarrollo y mantenimiento de los sistemas de información.

3.11. Relación con Proveedores.

3.12. Gestión de Incidentes de Seguridad de la Información.

3.13. Aspectos de Seguridad de la Información en la Gestión de Continuidad de Negocio.

3.14. 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, practicantes o cualquier persona y proveedores que estén involucrados 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 implementar 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
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	La posibilidad de sufrir daños o perdidas, la amenaza es un componente del riesgo y se puede considerar como: un agente de amenazas ya sea humano o no humano. 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.

Concepto	Descripción
Proceso	Conjunto de actividades íntimamente relacionadas que existen para generar un bien o servicio, el cual tiene un cliente externo o interno a la organización en que opera. Los procesos pueden ser estratégicos, de negocio/operación o de apoyo/soporte.
Incidente de seguridad	Evento único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer la operación de negocio y de amenazar la seguridad de la información. Por lo tanto, un incidente de seguridad se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información: un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información del organismo.
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 y Ciberseguridad	Persona responsable por la implementación de medidas de control que garanticen la seguridad de la información, así como también aplicar las medidas de ciberseguridad que promueve el Estado. Adicionalmente es responsable de la coordinación entre los distintos comités de seguridad.
Comité de Seguridad de la Información Institucional	Agrupación de personas 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. Arbitrar conflictos que se generen en materias de seguridad de la información, apoyar planes de difusión y formación de la cultura de la seguridad de la información, cuya organización es la siguiente: • Comité Directivo: Tiene como principal objetivo establecer prioridades y directrices de acción, control y supervisión del programa de trabajo anual de seguridad de la información y ciberseguridad. Revisando, una vez al año, el funcionamiento del sistema. • Comité Operativo: Estará compuesto por un equipo multidisciplinario y transversal a la Superintendencia de Educación y su objetivo será apoyar la ejecución del programa de trabajo que defina el Encargado de Seguridad de la Información y apruebe el Comité Directivo, la implementación práctica y operativa del Sistema de Seguridad de la Información al interior de la institución.

6. Roles y responsabilidades

Rol	Responsabilidad
Comité de Seguridad de la Información Institucional	a) Responsable del ciclo de vida de las políticas de seguridad de la información en la Superintendencia de Educación. b) Velar por la implementación de los controles de seguridad en la plataforma tecnológica. c) Fomentar planes de difusión y capacitación y formación de la cultura de la seguridad de la información. d) Arbitrar conflictos que se generen en materias de seguridad de la información. e) Revisar, al menos una vez al año, el funcionamiento del SGSI.
Comité Operativo de Seguridad de la información	a) Apoyar la ejecución del programa de trabajo que defina el encargado de seguridad de la información y aprueba el comité directivo. b) Asistir y ayudar la implementación práctica y operativa del Sistema de Seguridad de la Información al interior de la institución. c) Generar análisis de incidentes de seguridad, implementar acciones inmediatas que permitan corregir los incidentes de seguridad de la información detectado para lograr la continuidad de las operaciones, analizar las causas del incidente a fin de proponer medidas o acciones de mejoras futuras.

Rol	Responsabilidad
Jefe/a Departamento Gestión y Desarrollo 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, colaboradores y practicantes en materias de seguridad de la información y ciberseguridad.
Encargado/a 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 operacional de los procesos de la institución c) Monitorear el correcto funcionamiento de los procedimientos vinculados al Sistema de Seguridad de la Información. d) Coordinar la respuesta y priorización al tratamiento de incidentes y eventos vinculados a los activos de información institucionales. e) Mantener coordinación con otros departamentos y unidades de la Superintendencia para apoyar el cumplimiento de los objetivos de seguridad. f) 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 y ciberseguridad pertinentes. g) Mantener actualizado el inventario de activos de información del Servicio, de acuerdo con los procedimientos definidos. h) Mantener informado periódicamente al Comité Directivo y operativo de Seguridad de la Información acerca del estado del Sistema de Seguridad de la Información en la Institución. i) Promover acciones tendientes a la difusión y sensibilización respecto a la Seguridad de la Información y ciberseguridad a los funcionarios, colaboradores y practicantes vinculados a la institución. j) Ejecutar, aplicar e implementar las medidas de Ciberseguridad que sean instruidas por Presidencia.
Usuarios(as)	Son las personas, funcionarios, colaboradores, practicantes o personal externo que preste servicios permanentes o temporales, que usan los activos de información y los sistemas computacionales de la Institución. Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente, así como las políticas específicas, manuales y procedimientos asociados al SGSI y a la ciberseguridad y, además, tienen la obligación de reportar cualquier incidente o evento de seguridad del que tengan conocimiento.
Jefaturas de la SUPEREDUC	Las jefaturas de las Divisiones, Intendencia, Direcciones Regionales, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política, así como las políticas específicas, manuales y procedimientos asociados al SGSI

7. Directrices

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

7.1.1. El Comité Directivo 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. Así como también los lineamientos presidenciales en cuanto lo que dicte lineamientos de Ciberseguridad del estado.

7.1.2. Se deberá mantener un conjunto de políticas tendientes a velar por la implementación de las buenas prácticas de seguridad y ciberseguridad en los diferentes campos y ámbitos del quehacer de la Superintendencia de Educación.

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

7.2. Tareas y funciones del Comité de Seguridad

Tendrá como principal objetivo, implantar las distintas políticas de Seguridad de la Información y Ciberseguridad al interior de la Superintendencia de Educación. Velar por su cumplimiento, evaluar su mantención y adecuarlas en el tiempo de acuerdo con la normativa vigente, Su organización es la siguiente:

- Comité Directivo: Tiene como principal objetivo establecer prioridades y directrices de acción, control y supervisión del programa de trabajo anual de seguridad de la información y ciberseguridad. También deberá revisar una vez al año el funcionamiento del sistema. Está compuesto por: Superintendente de Educación, Fiscal, Jefaturas de División de Fiscalización, Administración General, Comunicación y Denuncias, Intendente/a de Educación Parvularia, Jefatura del Departamento de Gestión Institucional y Encargado/a de Seguridad de la Información y ciberseguridad Institucional.

- Comité Operativo: Compuesto por un equipo multidisciplinario y transversal a la Superintendencia de Educación, tiene como objetivo principal apoyar la ejecución del programa de trabajo que defina el Encargado de Seguridad de la Información y apruebe el Comité Directivo, la implementación práctica y operativa del Sistema de Seguridad de la Información al interior de la institución.

Las funciones y responsabilidades del Comité de Seguridad de la Información se especifican en Resolución Exenta N° 0698 del 10 de diciembre del 2019 que establece su conformación.

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

Objetivos de seguridad

Los objetivos por cumplir por parte del Sistema de gestión de seguridad de la información en la Superintendencia de Educación son los siguientes:

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

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

7.3.3. Establecer un marco de trabajo de la dirección para 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, contratistas y proveedores que tengan acceso a los sistemas y/o activos de información de la institución 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 y medidas de seguridad de la información.

7.3.6. Establecer los requisitos de seguridad de la información pertinentes de con cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.

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

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

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

7.3.10. Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de almacenamiento: magnéticos (discos duros, cintas), removibles (pendrive, discos duros portátiles, etc.) o vía web.

7.3.11. Restringir el acceso a la información y a las instalaciones de procesamiento de información a personas que no cuenten con la debida autorización.

7.3.12. Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios de la Superintendencia.

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

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

7.3.15. Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la Superintendencia de Educación.

7.3.16. Prevenir pérdidas, daños, hurtos o el compromiso de los activos, así como la interrupción de las actividades de la Superintendencia de Educación.

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

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

7.3.19. Proteger en contra de la pérdida de datos.

7.3.20. Registrar eventos de seguridad y generar evidencia sobre su tratamiento.

7.3.21. Asegurar la integridad de los sistemas operacionales.

7.3.22. Evitar la explotación de las vulnerabilidades técnicas.

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

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

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

7.3.26. Asegurar que la seguridad de la información y ciberseguridad sea parte integral de los sistemas de información de la Superintendencia de Educación.

7.3.27. Resguardar que la seguridad de la información está incorporada dentro del ciclo de desarrollo de los sistemas de información de la Superintendencia.

7.3.28. Resguardar la protección de los datos usados en ambientes de desarrollo y testing.

7.3.29. Resguardar la protección de los activos de la organización a los que tienen acceso los proveedores.

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

7.3.31. 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.

7.3.32. Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del servicio de la Superintendencia de Educación.

7.3.33. Resguardar la disponibilidad de las instalaciones de procesamiento de la información.

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

7.3.35. Resguardar que la seguridad de la información y la ciberseguridad se implemente y funcione de acuerdo a las políticas, manuales y procedimientos de la institución.

7.3.36. Monitorear y reportar el cumplimiento de los requisitos de seguridad de la información mediante el uso de herramientas diagnósticas y auditorías internas o externas planificas a intervalos regulares, de acuerdo a los recursos disponibles para lograr alcanzar los objetivos institucionales.

7.3.37. Implementar acción acciones preventivas, correctivas y de mejoras para el Sistema de Gestión de Seguridad de la Información.

7.3.38. Incorporar la gestión de los riesgos e implementación de medidas asociadas a Ciberseguridad de las redes, plataformas y sistemas informáticos que son de responsabilidad de la Superintendencia de Educación.

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 su continua idoneidad, eficiencia y efectividad.

Una vez que el documento entre en vigencia el/la Encargado/a de Seguridad de la Información y Ciberseguridad deberá difundir al personal y externos considerado en el alcance mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrán ser página web institucional, 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 o mejora 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, manuales 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/la Encargado/a de Seguridad de la Información y Ciberseguridad 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.

REVISIONES DE LA POLÍTICA			
N° Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
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. Punto 11,12,13,14, 15 y 16 se modifican su numeración.
05	31/07/2019		Actualización de formato de acuerdo a la metodología documental vigente en la Superintendencia de Educación Se incluye en el considerando, texto normativo que rige la política de Ciberseguridad Actualiza encargado de Seguridad de la Información en "Elaborado Por". Punto 2: Se modifica punto 2.7 y se incluyen punto 2.8, 2.9 y 2.10. Punto 5: Se incluyen funciones a encargado de seguridad, relativo a materias de ciberseguridad. Se incluye en Comité de Seguridad de la Información Institucional, los comités operativos y directivos. Punto 6: Se incluyen roles y responsabilidades a encargado de seguridad, relativo a materias de ciberseguridad. Se incluye además la letra C sobre encargado de Seguridad de Información. Se agregan roles y responsabilidades al Comité Operativo de Seguridad de la Información. Punto 7.1: Se incluyen materias de ciberseguridad en ítem 7.1.1 Punto 7.2: Se modifica y se incluye definición respecto los comité directivos y operativos. Punto 7.3: Se incluyen punto 7.3.35, 7.3.36 y 7.3.37.

3. **DISPÓNGASE,** anualmente la evaluación y revisión tanto del contenido como el cumplimiento de la Política de Seguridad de la Información de la Superintendencia de Educación por el 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, Intendencia, Direcciones Regionales, Departamentos, Unidades y de la Superintendencia de Educación, de acuerdo con 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.

CRISTIÁN O'RYAN SQUELLA
SUPERINTENDENTE DE EDUCACIÓN

Distribución:

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