MIC/FTO/AAM/PBC/DLR

Superintendencia de Educación
TOTALMENTE TRAMITADO

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0827 2017 Y APRUEBA VERSIÓN N°3 DE LA POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, EN EL MARCO DE LA SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0789

Santiago, 30 DIC 2019

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 723, 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, con fecha 01 de diciembre de 2017, se dicta Resolución Exenta Nº 0827, que aprueba política de gestión de incidentes de seguridad de la información versión Nº2, en el marco de la Seguridad de la Información.

3. Que, con fecha 23 de octubre de 2018, el Presidente de la Republica dicta el Instructivo Presidencial Nº 008 que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

4. Que, con fecha 02 de diciembre de 2019 se dicta Resolución Exenta Nº 0674, que designa a Encargada de Seguridad de la Información y Ciberseguridad para la Superintendencia de Educación.

   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, un Sistema de Seguridad de la Información que se mantenga y mejore en el tiempo

RESUELVO:

1. **DÉJASE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0827, de 2017 de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°3 de la Política de gestión de incidentes de seguridad de la información en la Superintendencia de Educación, cuyo texto es el siguiente:

Política gestión de incidentes de seguridad de la información

Tabla de Contenidos

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. Objetivo

Se define 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 a una política, estándar o procedimiento de seguridad que no permite dar servicio computacional y afecta la operacional normal de la institución.

La siguiente política ha sido elaborada para establecer un método para detectar, identificar, analizar y gestionar los incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, sistemas de información, medios físicos de almacenamientos y las personas, que afecten la continuidad operacional de los procesos críticos de la Superintendencia de Educación (SUPEREDUC).

2. Alcance

Esta política se aplica a todas las áreas de SUPEREDUC y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas[1], y a todas las dependencias y servicios de SUPEREDUC, afectados por cualquier incidente que comprometa la confidencialidad, integridad o disponibilidad de la información o de los sistemas, detectados en forma interna o externa.

Es aplicable a todos los Usuarios, ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo empresas que presten servicios a la SUPEREDUC y que mantienen acceso a la información, plataforma tecnológica, proceso y aplicativos.

Esta política contempla los siguientes controles definidos en la norma NCh-ISO 27001:2013

- A.06.01.03 Contacto con las autoridades.
- A.06.01.04 Contacto con grupos de interés especiales.
- A.16.01.01 Responsabilidades y procedimientos.
- A.16.01.02 Informe de eventos de seguridad de la información.
- A.16.01.03 Informe de las debilidades de la seguridad de la información.
- A.16.01.04 Evaluación de y decisión sobre los eventos de seguridad de la información.
- A.16.01.05 Respuesta ante incidentes de seguridad de la información.
- A.16.01.06 Aprendizaje de los incidentes de seguridad de la información.
- A.16.01.07 Recopilación de evidencia.

3. Referencias normativas

- Noma Chilena NCh-ISO 27001/2013 tecnología de la información-técnica de seguridad-sistemas de gestión de la seguridad de la información.
- Política general de seguridad de la información de la Superintendencia de Educación vigente.
- Procedimiento de gestión de incidentes de seguridad de la información de la Superintendencia de Educación vigente.
- Plan de emergencia de la Superintendencia de Educación vigente.

[1] Publicado en el sitio web www.dipres.gobc.cl Inicio / Evaluación y Control de Gestión / Definiciones Estrategicas / Superitendencia de Educación.

- Decreto Supremo Nº83 del Ministerio Secretaría General de la Republica, que aprueba norma técnica para los órganos de la administración del estado sobre Seguridad y Confidencialidad de los Documentos Electrónica.

4. Definiciones

Concepto	Descripción
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.
Evento de seguridad de la información	Cualquier ocurrencia relacionada con los activos de información, sistemas informáticos o el entorno que indique un posible compromiso de las políticas o las fallas de los controles de seguridad, casos de ejemplos de un evento de seguridad son: la detección de una falla en las medidas de seguridad de la información, una posible violación a las políticas o procedimientos de seguridad de la información y ciberseguridad o una situación desconocida hasta el momento en un sistema, servicio o red que pueda ser relevante para la Institución. Los eventos de seguridad no, necesariamente constituye un incidente de seguridad.
Gestión de incidente de seguridad de la información	Proceso para la detección, notificación, evaluación, respuesta y aprendizaje frente a la ocurrencia de incidentes de seguridad de la información. El primer objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto, para asegurar la continuidad operacional de la organización.
Integridad	Se entiende como la característica que implica la corrección y completitud de los datos o de la información manejada, contar con todas sus partes y estar completo.
Disponibilidad	Es el aseguramiento de que los usuarios autorizados tienen acceso a la información, sistemas y a los activos de la superintendencia, cuando es requerido.
Confidencialidad	Es la propiedad de la información, un documento o mensaje que únicamente está autorizado para ser leído o entendido por algunas personas o entidades. Mantiene la cualidad de mantenerse reservada para el conocimiento de una persona o de algunas, pero no debe ser expuesta en forma masiva.
Mesa de Servicio	Servicio orientado a satisfacer las necesidades, solicitudes e inquietudes de índole informática de toda la comunidad usuaria de la Superintendencia, mediante un canal único de registro, atención y/o escalamiento de solicitudes y requerimientos de usuarios hacia el Departamento de Tecnologías y Procesos

5. Roles y Responsabilidades

Rol	Responsabilidades
Mesa de Servicios, Departamento de Tecnologías y Procesos	a) A nivel operativo, proporcionar un único punto de contacto para ofrecer asesoramiento, orientación y la rápida restauración de servicios a sus usuarios. a) Escalar posibles eventos de seguridad notificados a la mesa de servicio, al encargado de Infraestructura Operacional del Departamento de Tecnologías y Procesos para su evaluación y diagnóstico.
Usuario	a) Todo los funcionarios, colaboradores, practicantes, proveedores o personal externo que preste servicio permanente o temporal, que usan los activos de información y los sistemas computacionales de la institución. Son responsables de notificar cualquier tipo de evento que pueda afectar el normal funcionamiento del Sistema de Seguridad de la Información o cualquier debilidad sospechosa en la Seguridad de la Información en los Sistemas o Servicios. Los canales para notificar son email mesadeservicio@supereduc.cl y/o al anexo 55555

Unidad de Infraestructura y Operaciones del Departamento de Tecnologías y Procesos.	a) Recepcionar y mantener un registro de las notificaciones realizadas por los usuarios en la Mesa de Servicio. b) Generar las acciones que aseguren prevenir, revertir o mitigar efectos de un incidente de Seguridad de la Información en el ámbito de gestión relacionado con su área. c) Gestionar el adecuado nivel de calidad, seguridad, continuidad y rendimiento de los servicios de tecnologías de información suministrados a la SUPEREDUC. d) Supervisar, coordinar y gestionar las actividades de soportes y mantención entregadas al Departamento de Tecnología y Procesos, a nivel nacional. e) Colaborar y proponer directrices, procedimientos y controles de uso de los recursos y seguridad informáticos. f) Promover y desarrollar planes de mejoramiento, a corto y largo plazo, de los sistemas y procesos informáticos, con el objetivo de generar cambios de mejoras en el servicio y seguridad de los sistemas que administra el Departamento de Tecnología y Procesos de la SUPEREDUC. a) Proveer las evidencias digitales potenciales en sistemas, redes, dispositivos, entre otros de su competencia, para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.
Encargado/a de Seguridad de la Información y Ciberseguridad.	a) De acuerdo con el Instructivo Presidencial N°8 publicado con fecha 23 de octubre de 2018, será responsable de la seguridad informática de su servicio y velar por las medidas de seguridad establecidas en dicho instructivo. b) Velar por el correcto funcionamiento y operación de la gestión de incidentes de seguridad de la información, evaluarlos de acuerdo con sus circunstancias particulares y escalar a las autoridades pertinentes según se define en este procedimiento. c) Velar por la correcta identificación, recopilación, adquisición y preservación de las evidencias sobre los incidentes y eventos de seguridad que se presenten en la institución. d) Coordinar la oportuna respuesta y priorización al tratamiento de incidentes y eventos vinculados a los activos de información y sistemas informáticos institucionales. e) Ejecutar, aplicar e implementar las medidas de Ciberseguridad que sean instruidas por Presidencia, de acuerdo al Oficio Gab. Pres. N° 008, de 23 de octubre de 2018, del Presidente de la República.

6. Directrices

6.1. Reporte de eventos y debilidades en la Seguridad de la Información

a) Todo los usuarios de la SUPEREDUC, en coordinación con su jefatura, es responsable de notificar tan pronto sea posible cualquier tipo de evento que identifique y que pueda afectar el normal funcionamiento del Sistema de Seguridad de la Información. Esta notificación se realizará a través del email mesadeservicio@supereduc.cl o al anexo 55555, indicando todos los antecedentes del evento identificado.

b) La mesa de servicio dependiende del Departamento de Tecnologia y Procesos, es el responsable de registrar el evento o posible incidente de seguridad repotado por el usuario, el cual avaluará si se trata de un evento de seguridad y activara las acciones que se describen en el *"Procedimiento de gestión de incidente de seguridad"* vigente.

c) Es importante que los usuarios reporten los evento o posible incidente de seguridad que han identificado en el sistemas informatico o en el sistema de informacion de la SUPEREDUC, tan pronto sean posible al Departamento de Tecnología y Procesos. El usuario no está facultado para realizar acciones, sobre el incidente, sin el apoyo técnico correspondiente.

d) Todo usario deberá estar siempre aleta tanto al cumplimiento, respeto de las politicas y procedimiento que establezca el sistema de seguridad de la información y ciberseguridad de la SUPEREDUC. Teniendo en consideración que sus acciones son pueden ser blanco u objetivos de un ataque mediante el cual se podria acceder a información sensible y confidencial relevante de la institución.

6.2. Gestión de incidentes de seguridad

Si el evento reportado es identificado como incidente de seguridad de la información, porque afecta de manera significativa la disponibilidad, integridad y/o confidencialidad de uno o mas activos de información o sistemas informáticos de la SUPEREDUC, pudiéndose traducir en la interrupción de los procesos críticos de la institución, se deberá gestionar el incidente, de acuerdo con los siguientes puntos:

6.2.1. Registro y Clasificación del Incidente

a) El Departamento de Tecnología y Procesos establecerá un único canal para reportar un incidente, mediante la Mesa de Servicio, quien generará el registro del incidente según lo establezca el *"Procedimiento Gestión de incidentes de seguridad de la información"*, vigente en la Superintendencia.

b) El encargado de la Mesa de Servicio de TI deberá clasificar el incidente, de acuerdo al tipo de origen y nivel de criticidad según lo detalle el *"Procedimiento Gestión de incidentes de seguridad de la información"*, vigente en la Superintendencia.

6.2.2. Análisis y Gestión de Riesgo

Con los antecedentes recopilados se realizará un análisis, por el Depatamento de Tecnologia y Procesos. Respecto del tipo de incidente, alcance y nivel de criticidad. Además se determinará el tratamiento al riesgo donde :

a) **Mitigar el riesgo**: Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

b) **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la Dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

c) **Transferir el riesgo a un tercero:** Asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

d) **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

6.2.3. Escalamiento

a) Si el Jefe/a del Departamento de Tecnologìa y Procesos determinará que el incidente detectado requiere un tratamiento urgente, de ser así, debe procederse a establecer una solución con la mayor celeridad posible e informar al Encargado/a de Seguridad de la Información y Ciberseguridad, quien monitoreara la resolución del incidente, activará el apoyo del Comité Operativo y mantendra los contacto correspondientes con las

autoridades o grupos externos que manejen los problemas relacionados con los incidentes de seguridad de la información.

b) Cada vez que se registre un incidente de seguridad, los profesionales del Departamento de Tecnología y Procesos debe ejecutar las acciones inmediatas según sea el tipo de incidentes para su rápida resolución y respuesta.

c) En los casos de que no se pueda resolver el problema, se realiza un escalamiento interno, donde se realizara una transferencia a una persona de soporte técnico más elevado, que tenga mayor conocimiento o experiencia, recursos para solucionar situaciones complejas y mayor poder en la toma de decisiones, de acuerdo a lo detallado en "*Procedimiento Gestión de incidentes de seguridad de la información*".

6.2.4. Respuesta inmediata

La jefatura designada del Departamento de Tecnologìa y Procesos, para dar respuesta inmediata al incidente, es responsable del desarrollo de las siguientes acciones inmediatas:

Actividad	Descripción
Contener el daño y minimizar el riesgo	Evitar que se propaguen los daños o efectos del incidente, coordinando las actividades necesarias para su disminución, probabilidad y consecuencia.
Reclasificar el incidente	Si es necesario, reclasificar según lo descrito en el *Procedimiento Gestión de incidentes de seguridad de la información.*
Proteger las evidencias	Resguardar las evidencias recopiladas durante la gestión del incidente.
Notificar a terceros relevantes	Cuando sea necesario, notificar a organismos externos (carabineros, bomberos, PDI, etc.), según lo descrito en el *Procedimiento Gestión de incidentes de seguridad de la información.*
Compilar y organizar la documentación del incidente	Recopilar todos los antecedentes y evidencias relacionados con el incidente, entregarlos al Encargado/a de Seguridad de la Información y Ciberseguridad.
Entregar lineamientos para la respuesta al incidente	El Encargado/a de Seguridad de la Información y Ciberseguridad, debe apoyar a la jefatura correspondiente en esta etapa, para responder de manera adecuada al incidente detectado.

6.2.5. Continuidad de las operaciones y servicios

En caso de que el incidente no pueda ser controlado y ponga en riesgo las operaciones y entrega de servicios de la SUPEREDUC, el Encargado/a de Seguridad de la Información y Ciberseguridad, el Jefe del Departamento de Tecnologías y Procesos y el Comité Operativo de Seguridad de la Información evaluarán la pertinencia de activar el Plan de Continuidad de Operaciones, vigente en la institución.

6.2.6. Recolección de evidencia

a) La recolección de evidencia es responsabilidad del Encargado/a de Seguridad de la Información y Ciberseguridad. Ésta debe ser clara y suficiente para respaldar el incidente. Para ello se debe considerar lo siguiente:
   - **Información en formato papel:** El original se debe guardar de manera segura con información del individuo que encontró el documento, dónde y cuándo fue encontrado y quién fue testigo del descubrimiento. Se debe procurar que el documento original no sea adulterado intencional o accidentalmente.
   - **Información en formato digital:** Las imágenes o copias de cualquier medio removible, la información contenida en discos duros o en memorias, deben ser retenidas de manera segura para garantizar su disponibilidad. El registro de todas las acciones durante el proceso de copiado, se debe guardar y el proceso se debe realizar en presencia de testigos. Los medios originales y el registro se deben guardar de manera segura, evitando la adulteración de la evidencia.

b) El encargado/a de Seguridad de la Información y Ciberseguridad deberá realizar un informe y registro del incidente, con todos los antecedentes recabados. Este documento deberá ser enviado al Comité Directivo de Seguridad quien tomará las decisiones correspondientes.

c) Cualquier trabajo forense se debe realizar sólo sobre copias del material de evidencia. Se debe supervisar y registrar cuándo y dónde fue ejecutado el proceso, quién lo ejecutó y qué herramientas y/o programas se utilizaron. Esta información es entregada al Comité Directivo de Seguridad de la Información, para la evaluación y aprendizaje del incidente y eventuales acciones legales y disciplinarias.

6.2.7. Resolución del incidente

La resolución de un incidente de seguridad de la información se realizará por las acciones y medidas que accione el Departamento de Tecnología y Procesos, de acuerdo con el *"Procedimiento de gestión de incidentes de seguridad de la información"*, vigente de la Superintendencia.

6.2.8. Contacto con Autoridades o Grupos de Interés

a) Independiente del origen y tipo de evento reportado, aquellos casos en que los incidentes sean clasificados como **Alto Impacto, Critico** o **Urgencia Alta,** deberán ser reportados a las altas autoridades de la Superintendencia de Educación, por el Encargado de Seguridad de la Información y Ciberseguridad. Donde se le comunicara el estado del incidente, avances y tiempos estimados de solución. En los casos que clasifiquen y que las autoridades de la Superintendencia lo definan, se deberá informar el incidente al Centro de Coordinación de entidades de Gobierno, CSIRT.

b) Es responsabilidad del Encargado de Seguridad y Ciberseguridad mantener un registro actualizado con contacto con autoridades para realizar un contacto oportuno. Así como también mantener un registro actualizado con los grupos de interés especiales o foros de seguridad de especialistas y asociaciones profesionales.

c) El Superintendente, Comité Directivo de Seguridad o el Encargado de Seguridad de la Información y Ciberseguridad, son los únicos autorizados para reportar incidentes de seguridad antes las autoridades. Así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas y de mantener contacto con grupos de interés externos o foros que se encargan de los asuntos en relación con los incidentes de seguridad de la información.

6.2.9. Análisis de causa y cierre

En esta etapa el Encargado/a de Seguridad de la Información y Ciberseguridad con el apoyo del Departamento de Tecnología y Procesos deberán:

a) Realizar un análisis de causa del incidente.
b) En caso de ser necesario, debe diseñar e implementar un plan de acción adecuado que prevenga incidentes futuros.
c) Registrar el cierre del incidente.
d) Aplicar lecciones aprendidas y ajustar los procedimientos y vías de comunicación con el objeto de contar con mejores herramientas para un eventual futuro incidente.
e) Tomar las medidas para que se cuantifiquen las pérdidas económicas, si las hubiere.
f) Preparar un Informe ejecutivo al Comité Directivo de Seguridad de la Información y Comité Operativo según corresponda, dependiendo de la magnitud e impacto del incidente.

7. Evaluación y Difusión

La presente política será evaluada por el Superintendente de Educación 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 e/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 podrían ser página web institucional, intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

8. Revisión

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.

9. Aceptación

Todos los usuarios de la SUPEREDUC sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar esta 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 y ciberseguridad 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.

10. 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.

11. 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.

12. Revisiones de la política

REVISIONES DE LA POLITICA			
N° Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
1.0	Octubre 2016	Versión inicial	Versión inicial
2.0	Noviembre 2017	Revisión Política	- Punto 2.0, se incorpora al alcance las definiciones de Ficha A1 y los controles de la norma Nch:27.001 desarrollados en esta política. -Punto 5, se elimina NchISO27001:2013 y NchISO27002:2013. - Puntos 6.1, se modifica email de contacto y anexo de mesa de servicios TI. - Punto 9, se incorpora la evaluación y revisión anual de la política. - Punto 11, se modifica formato de tabla.
3.0	Diciembre 2019	Actualización de Política	Todas las páginas.

3. **ESTABLÉZCASE,** la obligación de el/la Encargado/a de Seguridad de la Información y Ciberseguridad de la Superintendencia de Educación, de difundir la política fijada por este instrumento y de velar junto con el Comité Operativo de Seguridad de la Información por su estricto cumplimiento.

4. **DÉJESE,** expresa constancia que la presente Resolución Exenta no erogará gasto alguno para esta Superintendencia de Educación.

5. **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.

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

ANÓTESE, COMUNÍQUESE Y ARCHIVESE.

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACION

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 de Finanzas.
- 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.
- Unidad de Transparencia.
- Encargado/a de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.