GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS Y ORDENA PUBLICACIÓN QUE INDICA.

JUNAEB
25 JUL 2017
OFICINA DE PARTES

RESOLUCIÓN EXENTA Nº 1.662

SANTIAGO, 5 de julio de 2017

VISTO: Lo dispuesto en la ley N° 15.720 que crea la Junta Nacional de Auxilio Escolar y Becas; el decreto supremo. N° 5.311, de 1968, del Ministerio Educación reglamento general de JUNAEB, el decreto ley N° 180, de 1973, que reorganiza a JUNAEB, el D.F.L. N° 29, del Ministerio de Hacienda, del 2004, que fija el texto refundido, coordinado y sistematizado de la ley N° 19.834 sobre Estatuto Administrativo, en la ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; en la ley N°19.880 que establece Bases de los Procedimientos Administrativos, en la ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica, y Servicios de Certificación de dicha Firma, en el decreto N° 181, de 2012, que aprueba el reglamento de la ley N° 19.799; en la ley N° 19.233 sobre Delitos Informáticos, en la ley N° 20.285 que regula el principio de Transparencia de la Función Pública y el derecho de Acceso a la Información; en el decreto supremo N° 83, 2004, del Ministerio Secretaría General de la Presidencia que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, en la Norma Chilena NCh-ISO 27001.Of2013 Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – Requisitos; en el decreto exento N° 1.106, de 2016, del Ministerio de Educación; que modifica el orden de subrogancia del cargo de secretario general de JUNAEB y en la resolución N° 1.600 de 2008 de la Contraloría General de la República que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1.- La necesidad de que la institución gestione adecuadamente la Seguridad de la Información, con objeto de mejorar los niveles de protección de los activos de información relevantes que dan sustento a sus procesos de provisión y soportes;

2.- Que la norma técnica aprobada mediante decreto N° 83, del 2004, del Ministerio Secretaría General de la Presidencia, establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado;

3.- Que, las exigencias y recomendaciones previstas en dicha norma, tienen por finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica entre los órganos de la Administración del Estado y entre éstos la ciudadanía y el sector público en general; y salvaguardar el uso del documento electrónico de manera segura, confiable y en el pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada;

4.- Que, en tal sentido los órganos de la Administración del Estado, regidos por el decreto N° 83 precitado, deben establecer un sistema de gestión en seguridad de la información que coordinen y orienten la materia de seguridad dentro de cada institución, reflejando claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional;

5.- Que, es conveniente contar con una Política General de Seguridad de la Información, que en función del marco normativo regulatorio, apoye y facilite al Sistema de Seguridad de la Información el establecimiento, mantención y mejora de los procesos necesarios en favor de proteger la información y los activos de información del Servicio.

RESUELVO:

ARTÍCULO 1°: APRUÉBESE la política general de seguridad de la información de **LA JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS**, cuyo texto se inserta a continuación:

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS CHILE

ÍNDICE

1. CONTEXTO

La Política General de Seguridad de la información de la Junta Nacional de Auxilio Escolar y Becas (JUNAEB), contribuye a la gestión de la seguridad de la misma fomentando una cultura que le permite identificar, evaluar, medir, reportar y tratar amenazas que afecten la seguridad de los activos de información o en su defecto, innovar e incorporar buenas prácticas para el resguardo oportuno de la información que maneja el Servicio.

En JUNAEB la información es entendida como un activo, y como tal, debe ser protegida.

Todas las áreas y los/as funcionarios/as de JUNAEB generan, manipulan y procesan información, soportada en diversos formatos físicos, magnéticos, electrónicos y ópticos. Esta información podría quedar expuesta a cambios, daños y revelación indebida, pudiendo afectar la función de la institución o la correcta implementación de los programas a su cargo.

2. OBJETIVO

Entregar lineamientos para la implementación y mantención de la Seguridad de la Información de la Junta Nacional de Auxilio Escolar y Becas (JUNAEB) que deben cumplir todos los funcionarios de la institución (cualquiera sea su calidad contractual) y terceros proveedores pertinentes, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y así asegurar la entrega de los programas a cargo del servicio.

3. ALCANCE

La Política General de Seguridad de la Información se aplica a todas las áreas y procesos relevantes del Servicio, tanto los de negocio (programas institucionales) como soporte, en los departamentos y unidades de la Dirección Nacional, las Direcciones Regionales y oficinas de la JUNAEB.

Forman parte integral de la Política General de Seguridad de la Información de la JUNAEB, todos los procedimientos que derivan de ésta y que, por su particularidad, requieren un mayor nivel de detalle y especialización para su definición, los cuales serán elaborados y actualizados por cada área, los que a su vez, pueden estar complementados por estándares, guías y manuales.

4. MARCO JURÍDICO

La Política General de Seguridad de la Información de JUNAEB se fundamenta en las siguientes disposiciones legales y reglamentarias:

- Ley N° 17.336 de propiedad intelectual.
- Ley Nº 19.223. tipifica figuras penales relativas a la informática.
- Ley N° 19.628 sobre protección de la vida privada.
- Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley N° 19.927 sobre delitos de pornografía infantil.
- Ley N° 20.285 de 2008, sobre Acceso a la Información Pública.
- Decreto supremo N° 181, de 2002, del Ministerio de Economía Fomento y Turismo aprueba el reglamento de la ley N° 19.799.
- Decreto supremo N° 77, de 2004, del Ministerio Secretaria General de la Presidencia, norma técnica sobre eficiencia de las comunicaciones electrónicas entre los órganos de la Administración del Estado, y entre éstos y los ciudadanos.
- Decreto supremo N° 81, de 2004, del Ministerio Secretaria General de la Presidencia, norma técnica de los órganos del Estado sobre interoperabilidad de documentos electrónicos.
- Decreto supremo N° 83, de 2005, del Ministerio Secretaria General de la Presidencia Norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto supremo N° 100, de 2006, del Ministerio Secretaria General de la Presidencia Norma técnica para el desarrollo de los sitios web de los órganos de la Administración del Estado y de sus funcionarios.
- Decreto supremo N° 158, de 2007, del Ministerio Secretaria General de la Presidencia; que modifica el decreto supremo N° 81 de 2004.
- Decreto supremo N° 14, de 2014, del Ministerio de Economía, Fomento y Turismo, que modifica el decreto supremo N° 181, de 2002, reglamento de la ley N° 19.799.

- Norma ISO 27001:2013, sobre Tecnología de la Información – Técnicas de Seguridad – Sistema de Gestión de la Seguridad de la Información – Requisitos.
- Instructivo presidencial N° 05, de 2001; que define el concepto de Gobierno Electrónico.
- Instructivo presidencial N° 06, de 2002; que imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de

documentación en la Administración del Estado.

- Instructivo presidencial N° 8, de 2006, que imparte instrucciones sobre transparencia activa y publicidad de la información de la Administración del Estado.
- Circular N° 3, de 2007, del Ministerio Secretaria General de la Presidencia, que detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del instructivo presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado.
- Instructivo General N° 3, de 2009, del Consejo para la Transparencia, índice de los actos o documentos calificados como secretos o reservados.

5. RESPONSABILIDADES FRENTE A ESTA POLÍTICA

Secretario General: Revisión final y aprobación de la Política.

Encargado de Seguridad de la Información: Elaborar propuesta de política para el Secretario General.

Comité de seguridad: Proponer mejoras, ideas y recomendaciones para incluir en la Política; difundirla y comunicarla a los funcionarios; y apoyar en la verificación de su cumplimiento informando los incumplimientos detectados al encargado de seguridad de la información, al secretario general y/o comité directivo de JUNAEB.

Directores Regionales y Jefaturas de Departamentos de Dirección Nacional: difundir y comunicar la Política dentro del ámbito de su competencia. Verificar su cumplimiento informando el no cumplimiento al encargado de seguridad de la información, al secretario general y/o comité directivo de la Institución.

Contrapartes de Seguridad de la Información: Difundir y comunicar la Política a los funcionarios; Colaborar, coordinar y apoyar en la implementación de la Política.

Jefaturas de Unidad: Implementar la Política; y verificar su cumplimiento, informando su no cumplimiento al encargado de seguridad de la información y Jefatura directa del departamento a que pertenezca.

Funcionarios/externos trabajadores de JUNAEB, Proveedores/contratista y Red colaboradora: Conocer la Política; implementarla y alertar las situaciones que impidan la implementación de la política a Jefaturas directas e instancias respectivas.

6. DEFINICIONES

SSI: Sistema de Gestión en Seguridad de la Información.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas) para productos de áreas diversas.

JUNAEB: Junta Nacional de Auxilio Escolar y Becas.

DEPLACGE: Departamento de Planificación, Control de Gestión y Estudios, de JUNAEB.

UCGI: Unidad de control de gestión interna de JUNAEB.

Controles: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para dar protección a los activos de información.

Seguridad de los activos de información: Consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización.
Alta Dirección: Jefe superior de la organización.

7. DIRECTRICES

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Junta Nacional de Auxilio Escolar y Becas hace suyo el compromiso de proteger la información, la tecnología y activos que la soportan, a través de la implantación de un conjunto adecuado de controles, tales como políticas, procedimientos, estructuras organizacionales y funciones de software y hardware, que permita el logro de niveles apropiados de integridad, confidencialidad y disponibilidad, asegurando con ello la continuidad de las operaciones, la prestación de servicios a la ciudadanía y el cumplimiento de la misión y los objetivos estratégicos institucionales.

La Seguridad de la Información, se implementará de acuerdo a la metodología emitida por el Ministerio del Interior y la Dirección de Presupuestos del Ministerio de Hacienda, considerando como referencia el Anexo A de la norma internacional ISO 27001. Of2013 "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la Seguridad de la Información", con el firme compromiso de satisfacer los requisitos del Sistema de Gestión de la Seguridad de la Información de JUNAEB.

8. REVISIÓN

La Política de Seguridad de la Información tendrá una vigencia de tres años calendario desde su aprobación; no obstante, el Secretario General podrá autorizar revisiones y modificaciones antes del periodo de vencimiento.

9. DIFUSIÓN

La Política General de Seguridad de la Información, será comunicada y difundida a todo el personal de la Institución, a través de la publicación en la intranet institucional para su conocimiento y libre consulta del personal cualquiera sea su calidad jurídica (contrata-honorario-planta) de JUNAEB, a la cual puede acceder con login y password personal. Para personas externas, ya sea proveedor, colaborador o contratista, se pública dentro del Banner de Gobierno Transparente del servicio, al cual pueden acceder por la página online: www.junaeb.cl

10. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SSI)

En JUNAEB, se desarrolla un sistema de gestión que tiene por finalidad establecer, implementar, mantener y mejorar los procesos de coordinación necesarios que permitan llevar a cabo la seguridad de la información y los activos asociados[1].

10.1 OBEJETIVOS SSI

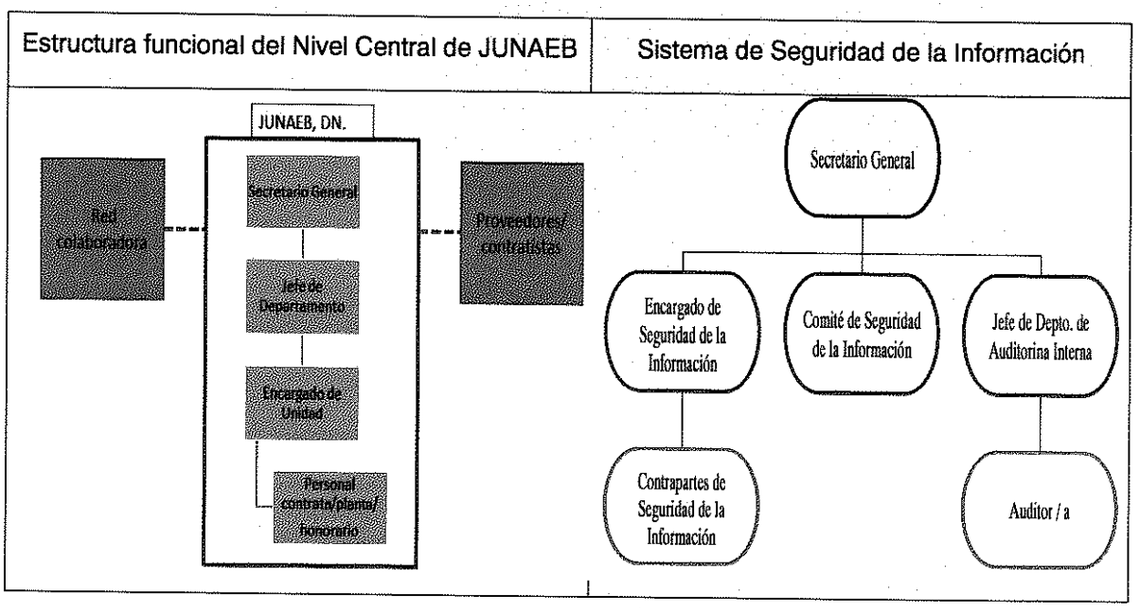
Como sistema de gestión, se pretende:

- Asentar la gestión de la seguridad de la información al interior de JUNAEB, según alcance definido.
- Colaborar en la protección de la información, y activos que la soportan, mediante la coordinación necesaria para la aplicación de controles definidos en el anexo A de la Norma ISO 27.001:2013.
- Entregar lineamientos, apoyo y guía para las restantes áreas y procesos de JUNAEB, que permitan su vinculación en la protección y seguridad de la información, estableciendo coordinación y nexos de interacción y comunicación entre las diferentes áreas y departamentos pertinentes.

10.2 ALCANCE DE SSI

El alcance del SSI de JUNAEB comprende la implementación de los controles que permiten dar seguridad a la información como asimismo los activos (soporte) en los departamentos y unidades de la Dirección Nacional de JUNAEB[2].

10.3 ORGANIZACIÓN



[1] El sistema de gestión de seguridad de la información también lidera el sistema de gestión de incidentes en seguridad de la información (control 16.01.01 al control 16.01.05) coordinando a los departamentos y áreas pertinentes.

[2] Cabe señalar que, el alcance regional será trabajado una vez que la totalidad de los controles se encuentren aplicados a nivel central, independiente de la implementación de buenas prácticas entorno a la seguridad de la información en las direcciones regionales de JUNAEB a modo de preparación y acercamiento.

10.4 ROLES Y RESPONSABILIDADES DEL SSI

Cargo	Rol	Responsabilidades
Secretario General.	• Alta Dirección. • Líder del SSI.	• Liderar el Sistema de Seguridad de la Información a través de un fuerte y sostenido compromiso; • Asegurar los recursos necesarios para la gestión del SSI; • Entregar lineamientos y dirección al SSI a través de órdenes directas en reuniones de directivos, aprobación de documentación (manuales, procedimientos, etc.) y resultado de la revisión de la dirección; • Comunicar la importancia de gestionar la Seguridad de Información y el cumplimiento del SSI; • Establecer el marco de trabajo del SSI mediante la Política General de Seguridad de Información, en compatibilidad con la planeación estratégica de la organización; • Asegurar que los requisitos del SSI sean integrados o asumidos por los procesos de la organización; • Designar roles y responsabilidades necesarios para la implementación y mantención del SSI, mediante resolución exenta; (incluyendo la designación del Encargado de Seguridad de la Información y del Comité de Seguridad de la Información) • Realizar la revisión de los datos arrojados por el SSI, tomando las decisiones necesarias para garantizar el mantenimiento, logro de los resultados esperados y mejoramiento continuo del sistema; • Ordenar la instrucción de procesos disciplinarios en contra de los funcionarios cuando éstos infrinjan la normativa legal y/o reglamentaria referente a la seguridad

Cargo	Rol	Responsabilidades
		de la información, aplicando las sanciones cuando corresponda.
Jefe del Depto. Planificación, Control de Gestión y Estudios.	• Encargado de Seguridad de la Información de la Institución. • Presidente del Comité de SSI.	• Velar por la implementación, mantención y mejora del sistema de gestión de seguridad de la información; • Brindar a la Alta Dirección apoyo en la implementación de la Política General de la Seguridad de la Información y determinación del alcance del SSI; • Establecer anualmente objetivos específicos de SSI en niveles y funciones relevantes con relación a la Seguridad de la Información, monitoreando los planes consecuentes para su logro; • Liderar la evaluación de criticidad y necesidades de protección (también llamado evaluación de riesgo SSI) como proceso colaborativo, cada tres años; • Informar a la Alta Dirección sobre el desempeño de SSI, preparando la revisión por la dirección y comunicando los avances o situaciones de contingencias en las reuniones directivas; • Revisar la documentación de los controles (políticas, procedimientos, manuales, instructivos u otros) con la finalidad de introducir oportunidades de mejora al departamento o área involucrada en el control; • Tener a su cargo la elaboración inicial de la documentación relativa a la seguridad de la información o asesorar en dicha materia, además de velar por su correcta aplicación; • Coordinar la respuesta de incidentes que afecten a los activos de información; • 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.
Algunas Jefaturas de Depto.	• Miembros del comité de sistema de seguridad de la información.	• Apoyar al SSI, colaborando en la implementación, mantención y mejora del sistema de gestión de seguridad de la información; • Establecer el contexto del SSI; • Establecer las partes interesadas para el SSI y determinar la estrategia para la interacción con ellas; • Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades; • Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización; • Aprobar modificaciones a documentos de seguridad de la información que impliquen inclusiones o correcciones menores.
Jefaturas de Depto.	• Integrantes del sistema de seguridad de la información. Propietarios de activos de información de su área táctica.	• Velar por los activos que está a cargo su depto. como propietario, siendo responsable de su uso, manejo, resguardo, conservación, disponibilidad, integridad y disposición/eliminación/expurgo; • Conocer, desarrollar y/o cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización; • Reportar debilidades, incidentes o eventos de seguridad de la información que se generen en las actividades desarrolladas a su cargo y/o al de sus compañeros; • Establecer y realizar revisión a las políticas, procedimientos y -en general- toda documentación que tenga a cargo, concerniente a la seguridad de la información con la finalidad de introducir actualizaciones necesarias por cambio en el entorno organizacional,

Cargo	Rol	Responsabilidades
		comercial, condiciones legales o el entorno técnico/tecnológico; • Documentar los controles, es decir, escribir procedimientos, políticas, instructivos u otro donde sus procesos a cargo tengan involucramiento y participación; • Resguardar y controlar los registros y documentación arrojados por la operación de sus procesos a cargo y la implementación de los controles de seguridad.
UCGI o profesional Contrapartes de Seguridad de la Información designado por Jefatura de Depto.	• Integrantes del sistema de seguridad de la información. • Coordinador a nivel operativo.	• Conocer desarrollar y/o cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización; • Alertar debilidades, incidentes o eventos de seguridad de la información que se generen en las actividades desarrolladas a su cargo y/o al de sus compañeros; • Reportar al DEPLACGE periódicamente los avances en materia de seguridad de la información y según sea solicitado; • Apoyar a jefaturas, encargados de unidad y funcionarios, consolidando datos, transmitiendo o difundiendo información, traspasando noticias provenientes del SSI.
Jefaturas de Unidad.	• Integrantes del sistema de seguridad de la información. • Encargado de los activos de información de su área.	• Conocer, desarrollar y/o cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización; • Reportar debilidades, incidentes o eventos de seguridad de la información que se generen en las actividades desarrolladas a su cargo y/o al de sus compañeros; • Establecer y documentar planes preventivos o correctivos para responder a incidentes o eventos de seguridad de la información que se generen en las actividades a su cargo.
Funcionarios y externos trabajadores de JUNAEB.	• Integrantes del sistema de seguridad de la información. • Usuario de activos de información. • Elaborador de información.	• Conocer y cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización; • Alertar debilidades, incidentes o eventos de seguridad de la información que se generen en las actividades desarrolladas a su cargo y/o al de sus compañeros.
Proveedores y contratistas.	• Colaborador del sistema de seguridad de la información. • Usuario de activos de información. • Elaborador de información.	• Conocer y cumplir con las medidas de Seguridad de la Información que se definan en los procedimientos de trabajo pertinentes a su actividad y/o de acuerdo a lo definido en los contratos vigentes; • Alertar debilidades, incidentes o eventos de seguridad de la información que se generen en las actividades desarrolladas a su cargo.
Red colaboradora.	• Colaborador del sistema de seguridad de la información. • Usuario de activos de información. • Elaborador de información.	• Conocer y cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo pertinentes a su actividad; • Alertar debilidades, incidentes o eventos de seguridad de la información que se generen en las actividades desarrolladas a su cargo.
Jefatura de Depto. de Auditoria Interna.	• Colaborador del sistema de seguridad de la información.	• Proporcionar información sobre el SSI a intervalos planificados mediante la realización de auditorías internas al SSI y/o de uno o más de sus controles, que evalúen las políticas, procedimientos u otro instructivo versus la operatoria efectiva; • Organizar, direccionar y realizar el control jerárquico de las auditorías que se ejecuten, debiendo para ello

Cargo	Rol	Responsabilidades
		entregar las instrucciones y lineamientos específicos tanto al supervisor como al equipo, y aprobar los informes que se emitan como resultado del trabajo realizado.
Auditor/a.	• Colaborador del sistema de seguridad de la información.	• Desarrollar el trabajo de auditoría, revisando una muestra de la implementación de controles de seguridad de la información, recolectando evidencias, analizando documentación y reportando en el informe de auditoría situaciones de debilidad, para su mejora y eficacia.

ARTÍCULO 2°: DÉJESE sin efecto la resolución exenta N° 1597, de 2016, de JUNAEB y cualquier otro acto administrativo sobre la misma materia.

ARTÍCULO 3°: PUBLÍQUESE la presente resolución una vez que se encuentre totalmente tramitada en la subsección "Actos con Efectos sobre Terceros" de la sección "Actos y Resoluciones", ubicado en el mini sitio "Gobierno Transparente" contenido en el portal web de JUNAEB a objeto de dar cumplimiento a lo previsto tanto en el artículo 7° de la ley N° 20.285 sobre acceso a la información pública como con lo dispuesto en el artículo 51 de su reglamento.

ANÓTESE.

JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS
SECRETARIO GENERAL

JAIME TOHA LAVANDEROS
SECRETARIO GENERAL (S)
JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

RDM/RFV/xah

DISTRIBUCIÓN:

1. Departamentos de JUNAEB
2. Direcciones Regionales
3. Oficina de Partes

Minuta Dpto. Jurídico N° 1.558/2017