GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO
ESCOLAR Y BECAS

APRUEBA POLÍTICA Y PROCEDIMIENTO DE GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO QUE INDICA, EN EL MARCO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DE LA JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS.

RESOLUCIÓN EXENTA N° 3152

SANTIAGO, 30-11-2017

VISTO:

Lo dispuesto en la Ley N° 15.720 que crea la Junta Nacional de Auxilio Escolar y Becas; en la Ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen las Actas de los Órganos de la Administración del Estado; en el Decreto Supremo del Ministerio de Educación N° 5.311 de 1968, que aprueba el Reglamento General de JUNAEB; en el Decreto Ley del Ministerio de Educación N° 180 de 1973, que declara receso del consejo de JNAEB cuyas facultades otorga a su Secretario General; en el Decreto Supremo del Ministerio Secretaría General de Gobierno N°83 del 2005, que aprueba Norma Técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos; Decreto Supremo del ministerio de Secretaría General de Gobierno N° 77 del 2004, que aprueba Norma Técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre estos los ciudadanos del Ministerio Secretaría General de la Presidencia; en el Decreto exento del Ministerio de Educación N° 1106 de noviembre de 2016 que nombra a don Jaime Tohá Lavanderos como Secretario General (S) de la Junta Nacional de Auxilio Escolar y Becas; y 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. Que en virtud del Decreto Exento del Ministerio de Hacienda N° 194 de 17 de mayo de 2017, que modifica el Decreto Exento 290 de agosto de 2016, se aprueba el Programa Marco de los Programas de Mejoramiento de la Gestión (PMG) para el año 2017; el cual consta de dos áreas prioritarias y tres sistemas de gestión con sus respectivos objetivos, debiendo los servicios formular compromisos en uno o más sistemas de gestión, dependiendo del grado de desarrollo alcanzado a la fecha de la formulación.

2. Que, en lo que respecta a la Junta Nacional de Auxilio Escolar y Becas, uno de los Programas de Mejoramiento de Gestión dice relación con el Sistema de Seguridad de la Información, correspondiente al área de Calidad de Servicio y que

DIRECCIÓN

tiene por objetivo de gestión "*Gestionar los riesgos de seguridad de la información de los activos que soportan los procesos de provisión de bienes y servicios, mediante la aplicación de controles basados en la Norma NCH-ISO 27001 Of2013 del Instituto Nacional de Normalización, sobre Sistemas de Seguridad de la Información*".

3. Que, en este sentido, la referida la Norma NCHI-ISO 27001 Of2013; dispone en el punto 4.4 denominado "*Sistema de Seguridad de la Información" que "la organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma*"

RESUELVO:

ARTÍCULO 1°: **APRUEBASE** los siguientes documentos relativos al Sistema de Seguridad de la Información de la Junta Nacional de Auxilio Escolar y Becas, cuyos textos se adjuntan a la presente resolución y se entiende incorporado, de acuerdo al siguiente nombre:

1. A.09.02.03 – Política Gestión de Derechos de Acceso Privilegiado
2. A.09.02.03 - Procedimiento Gestión de Derechos de Acceso Privilegiado

ARTÍCULO 2°: **PUBLÍQUESE** la presente resolución una vez tramitada, en la sección Actos y Resoluciones ubicado en el mini sitio "Gobierno Transparente", en el portal web de JUNAEB, a objeto de dar cumplimiento con lo previsto tanto en el artículo 7° de la ley N°20.285, sobre Acceso a la Información Pública, como en el artículo 51° de su Reglamento.

Junta Nacional de Auxilio Escolar y Becas - SECRETARIO GENERAL

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

DIRECCIÓN

MBG/RFV/FRR/jhs
DISTRIBUCIÓN:

1. Departamentos de Dirección Nacional y Direcciones Regionales
2. Oficina de Partes

DIRECCIÓN

POLÍTICA GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO

Autorizado Firma Jefe del Informática	Autorizado Encargado de Seguridad de la Información
Elaborado por: Departamento de informática	Revisado por: Departamento de Planificación

INDICE

DIRECCIÓN

1 OBJETIVO

Proporcionar directrices sobre el uso de derechos de acceso con privilegios especiales para funcionarios JUNAEB que ejercen como "administrador de sistema" de un sistema informático determinado.

2 ÁMBITO DE APLICACIÓN

La política aplica a todos los funcionarios JUNAEB y que cuenten con el rol de "administrador del sistema" en algún sistema informático que posea un módulo de administración de usuarios y un registro histórico de cambios de perfilamiento.

3 ROLES Y RESPONSABLES

JEFES DE DEPARTAMENTOS Y UNIDADES JUNAEB	Determinar qué rol o perfil de usuario deberá poseer determinado funcionario, en un sistema, para el desarrollo de sus funciones.
JEFE DE DEPARTAMENTO DE INFORMÁTICA	Definir normas de acceso lógico a sistemas de uso institucional, disponibles en plataforma productiva de JUNAEB.
ENCARGADO UNIDAD DE DESARROLLO Y MANTENCIÓN DE SISTEMAS	Controlar los perfiles de "administrador del sistema" en los sistemas informáticos con módulo de administración de usuarios.
ADMINISTRADOR DEL SISTEMA	Otorgar y/o denegar permisos de acceso y uso de roles específicos a funcionarios de su unidad de negocio, para un sistema de información determinado. Responder por las operaciones realizadas por funcionarios con permisos o roles indebidamente otorgados.
ENCARGADO SEGURIDAD DE LA INFORMACIÓN	Verificar y monitorear la ejecución de la política

4 POLITICA

Todo sistema informático destinado a apoyar los procesos de negocio de un departamento o unidad determinada y que posea un módulo para administración de usuarios, cuenta con un funcionario con el perfil de "*administrador funcional del sistema*", en adelante "administrador", y cuenta con un derecho de acceso especial que le permite:

- Incorporar nuevos usuarios
- Eliminar usuarios existentes
- Asignar roles o perfiles a usuarios
- Quitar roles o perfiles a usuarios
- Modificar contraseña de usuarios
- Revisar listado de usuarios activos

La asignación de roles y perfiles en un sistema informático es un aspecto restringido y controlado, privilegio especial exclusivo del "administrador", dado que potencialmente puede ser causa de incidentes de seguridad de la información.
Cualquier operación que efectúe el "administrador" sobre el conjunto de usuarios con roles y perfiles definidos, debe ser previamente autorizada por su jefatura directa. Debido a que se trata de una tarea asignada por la jefatura y no es una tarea que el operador de sistemas realice por su propia iniciativa.

DIRECCIÓN

Solo se podrá otorgar acceso a personas que se encuentren en desempeño de funciones como funcionarios activos de JUNAEB y/o cuya definición de usuario en el sistema sea complaciente con lo estipulado en la Política de Control de Acceso y Política de Segregación de Funciones, que integran el Sistema de Seguridad de la Información. Hay que tener en cuenta que existe un gran número de colaboradores que no son funcionarios de la institución, como empresas prestadoras, usuarios de otras instituciones, que tienen acceso a sistemas internos, pero con perfiles específicos a su función.
La ocurrencia de un incidente de seguridad de la información como producto del mal uso de los privilegios especiales que posee el rol de "administrador", puede dar lugar a las acciones y procesos legales estipulados en el documento de Responsabilidades y Procedimientos ante incidentes de seguridad de la información, en el Sistema de Seguridad de la Información.

5 REVISION

El Encargado de Seguridad de la Información, efectuará una revisión de este documento al menos una vez cada tres años desde su entrada en vigencia. Sin perjuicio de lo anterior, el documento puede ser evaluado y/o actualizado en cualquier momento, dependiendo de la necesidad de la organización por seguridad de la información.

6 DIFUSIÓN

El presente documento será difundido a través de correo electrónico y del portal de intranet Institucional, al cual todos los funcionarios de JUNAEB independiente de su calidad jurídica tienen acceso, mediante login y password.

7. VIGENCIA

La vigencia de la presente política tendrá una duración de tres años, una vez que aprobada la resolución exenta que da origen a su entrada en vigencia.

8 CONTROL DE CAMBIOS

Nº Revisión	Cambio	Fecha	Aprobado por:
00	Creación de documento.	05/09/2016	Departamento de Informática
01	Actualización del Documento punto 4 y 5	17/11/2017	Departamento de Informática

DIRECCIÓN

PROCEDIMIENTO GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO

Autorizado Firma Jefe del Informática	Autorizado Encargado de Seguridad de la Información
Elaborado por: Departamento de informática	Revisado por: Departamento de Planificación

INDICE

DIRECCIÓN

1 OBJETIVO

Establecer las actividades de operación sobre la gestión de derechos de acceso con privilegios especiales para funcionarios de JUNAEB que ejercen como "administrador de sistema" de un sistema informático determinado.

2 ÁMBITO DE APLICACIÓN

El procedimiento aplica al uso y operación de cuentas de las plataformas administradas por JUNAEB.

3 ROLES Y RESPONSABLES

RESPONSABLE	ACTIVIDAD
Jefe Departamento de Informática	Velar por la ejecución del procedimiento descrito, comunicándolo a las áreas involucradas.
Unidad de Soporte	Implementar el procedimiento y el registro de su cumplimiento.
Solicitante Responsable	Persona responsable de pedir la creación de una cuenta, o de mantener la responsabilidad de la misma
Administrador Funcional	Persona a cargo de una plataforma o sistema

4 DEFINICIONES

Para los propósitos de este procedimiento, las siguientes palabras se entenderán en el sentido que a continuación se indica:

Sistema de Mesa de Ayuda: Sistema informático web, que permite el registro y seguimiento de las actividades relativas a un caso asignado a especialistas de la Unidad de Soporte Informático.

5 PROCEDIMIENTO

5.1 Gestión de derechos

1-El solicitante responsable de pedir acceso a los deberá proveer los datos según los indica la política y procedimiento de Sistema de Gestión de Contraseñas.

2-El Administrador funcional del Sistema debe otorgar la alta o baja de los usuarios, asignar roles o perfiles a usuarios, quitar roles o perfiles a usuarios y/o Modificar contraseña de usuarios según el requerimiento solicitado.

3-El administrador funcional debe informar mediante mesa de ayuda el cierre del caso, además de informar si lo requiere al funcionario de la acción realizada vía mail y teléfono la acción realizada.

DIRECCIÓN

4-El Administrador funcional del Sistema debe al menos una vez al año solicitar al Departamento de Gestión de Personas, programáticos y/o de apoyo la validación de los usuarios con el perfil de acceso que tiene al sistema o a la plataforma a través de la ficha de gestión de derechos a sistema.

5-El Departamento de Gestión de Personas, programático o de apoyo debe validar y enviar a la mesa de ayuda el formulario de acceso indicando si los usuarios provistos deben tener acceso, el perfil correspondiente como la fecha de vigencia del mismo. Para posteriormente ingresar en el flujo que señala el punto a. Gestión de derecho de este mismo documento.

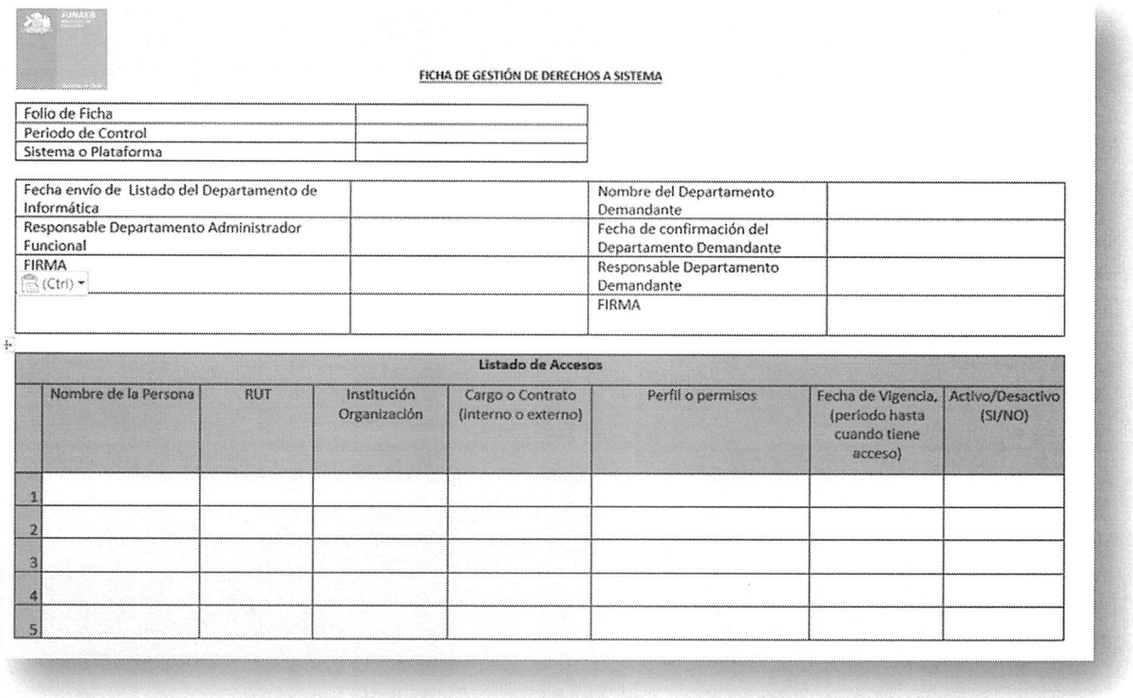
6 REGISTROS

Registro de requerimiento o caso en sistema Aranda (Mesa de Ayuda)

Las solicitudes deben ser ingresadas por separado (un Aranda por cada solicitud) **Descripción: (a continuación describa el caso lo más detallado posible)**
Acciones realizadas: (que ha hecho antes de reportar el caso)
Número de contacto: (Anexo o Celular)

Fuente propia, Departamento de Informática

DIRECCIÓN



FICHA DE GESTIÓN DE DERECHOS A SISTEMA

Folio de Ficha	
Periodo de Control	
Sistema o Plataforma	

Fecha envío de Listado del Departamento de Informática		Nombre del Departamento Demandante	
Responsable Departamento Administrador Funcional		Fecha de confirmación del Departamento Demandante	
FIRMA (Ctrl)		Responsable Departamento Demandante	
		FIRMA	

Listado de Accesos

	Nombre de la Persona	RUT	Institución Organización	Cargo o Contrato (interno o externo)	Perfil o permisos	Fecha de Vigencia, (período hasta cuando tiene acceso)	Activo/Desactivo (SI/NO)
1							
2							
3							
4							
5							

Fuente propia Departamento de Informática.

7 DIFUSIÓN

El presente documento será difundido a través de correo electrónico y del portal de intranet Institucional, al cual todos los funcionarios de JUNAEB independiente de su calidad jurídica tienen acceso, mediante login y password.

8. REVISIÓN

El Encargado de Seguridad de la Información, efectuará una revisión de este documento al menos una vez cada 3 años desde su entrada en vigencia. Sin perjuicio de lo anterior, el documento puede ser evaluado y/o actualizado en cualquier momento, dependiendo de la necesidad de la organización por seguridad de la información.

9. VIGENCIA

La vigencia de la presente política tendrá una duración de tres años, una vez que aprobada la resolución exenta que da origen a su entrada en vigencia.

10. CONTROL DE CAMBIOS

Nº Revisión	Cambio	Fecha	Aprobado por:
00	Creación procedimiento	20/10/2017	Departamento de Informática

DIRECCIÓN