GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO
ESCOLAR Y BECAS

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

RESOLUCIÓN EXENTA N° 3156

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

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.09.04.03 – Política para Gestión de Contraseñas.
2. A.09.04.03 - Procedimiento de Gestión de contraseñas.

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
DIRECCIÓN

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

MBG/RFV/FFR/jhs
DISTRIBUCIÓN:
1. Departamentos de Dirección Nacional y Direcciones Regionales
2. Oficina de Partes

DIRECCIÓN

POLÍTICA PARA GESTIÓN DE CONTRASEÑAS

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

El objetivo de esta política es entregar directrices del uso y mantención de contraseñas de cada cuenta de usuario pertenecientes a JUNAEB.

2 ÁMBITO DE APLICACIÓN

La presente política aplica a personal contratado en calidad jurídica de Planta, Contrata y Honorarios del nivel regional y Central de JUNAEB, para que en el desempeño de sus funciones precise autenticarse y hacer uso seguro de la red interna de la Institución.

3 ROLES Y RESPONSABLES

JEFE DEL DEPARTAMENTO DE INFORMÁTICA	Velar por el cumplimiento de las directrices impartidas. Aplicar controles que sean necesarios para el uso y mantención de contraseñas de los usuarios.
UNIDAD DE SISTEMAS E INFRAESTRUCTURA	Crear nuevas cuentas de usuario y definición de contraseñas según requerimiento. Realizar cambio periódico de todas las contraseñas de administración de sistema. Cambiar las contraseñas por defecto asociadas a los sistemas o aplicaciones nuevas, antes de poner estos sistemas en producción. Desactivar aquellas cuentas "por defecto" que no sean imprescindibles.
DEPARTAMENTO DE GESTIÓN DE PERSONAS	Notificar al Departamento de Informática el ingreso de nuevas contrataciones, eliminaciones y suspensiones de cuentas de usuarios.
FUNCIONARIO JUNAEB (CONTRATADO EN CALIDAD JURÍDICA DE PLANTA, CONTRATA Y HONORARIOS).	Cumplir las directrices estipuladas sobre el uso y mantención de su contraseña.
ADMINISTRADORES FUNCIONALES DE SISTEMAS	Crear nuevas cuentas de usuario y definición de contraseñas según requerimiento del sistema funcional responsable. Realizar cambio periódico de todas las contraseñas de administración del sistema funcional responsable. Cambiar las contraseñas por defecto asociadas a los sistemas o aplicaciones nuevas, antes de poner estos sistemas en producción, del sistema funcional responsable. Desactivar aquellas cuentas "por defecto" que no sean imprescindibles del sistema funcional responsable.
ENCARGADO SEGURIDAD DE LA INFORMACIÓN	Verificar y monitorear la ejecución de la política.

DIRECCIÓN

4 DIRECTRICES

4.1 CREACIÓN DE CONTRASEÑA

La creación de contraseña de usuario se encuentra regulada de acuerdo a las siguientes directrices:

- Toda contraseña nueva o reasignada[1] a un usuario es de carácter temporal, ya sea para su primer ingreso o cuando se le reasigne una contraseña nueva.
- Toda contraseña nueva o reasignada es única y aleatoria para cada asignación. Es decir, no se pueden asignar contraseñas temporales iguales a todos los usuarios o utilizar una contraseña por "Defecto" o "Tipo".
- Las cuentas de usuario que tengan privilegios de sistema a través de su pertenencia a grupos o por cualquier otro medio, deben tener contraseñas distintas del resto de cuentas mantenidas por dicho usuario en los servicios y recursos.
- Toda contraseña temporal asignada posee una extensión mínima de 6 caracteres alfanuméricos, sin espacios, debiendo incluir letras minúsculas y mayúsculas.
- Una contraseña temporal no debe ser igual a alguna de las 3 últimas contraseñas utilizadas o asignadas al usuario.
- Se debe utilizar en una misma contraseña dígitos, letras y caracteres especiales.

Todas las contraseñas de sistema y de usuario de recursos y servicios deben respetar las recomendaciones descritas en la presente política.

4.2 USO Y MANTENCIÓN DE CONTRASEÑA

El uso y mantención de una contraseña se encuentra regulada por las siguientes directrices:

El Funcionario JUNAEB[2] es responsable de:

- Una vez que el funcionario haya recibido su contraseña temporal, este debe modificarla y transformarla en una contraseña definitiva según los siguientes requisitos:
- Extensión mínima de 6 caracteres alfanuméricos, sin espacios, debiendo incluir letras minúsculas y mayúsculas.
- La contraseña no debe coincidir con alguna de las últimas 3 contraseñas empleadas anteriormente.
- La contraseña no debe incluir palabras de uso común como nombres de familiares, mascotas, amigos, nombre de la institución, información personal, fechas de cumpleaños, patrones de letras o números.
- Las contraseñas definitivas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.

[1] Una contraseña de usuario puede ser reasignada por la solicitud del usuario o su jefatura, por ejemplo, a causa del olvido de la misma. La contraseña reasignada a un usuario es temporal y deberá ser cambiada en su próximo inicio de sesión.
[2] En adelante, es referenciado como "usuario".

DIRECCIÓN

- Cada vez que modifique su contraseña deberá realizarlo de manera autónoma y sin la ayuda o supervisión de terceros.
- Debe mantener la contraseña en secreto y no divulgarla por algún medio. En caso de que ésta sea conocida por terceros, o que existiesen indicios de haber sido conocida, debe modificar la contraseña.
- Deben cambiar sus contraseñas cada 180 días, o cuando el sistema así lo requiera.
- No debe guardar contraseñas en un repositorio visible (cuaderno de apuntes, post-it pegados al computador o escritorio u otros medios no seguros).

4.3 BLOQUEO DE CUENTA

Los responsables del bloqueo de cuenta serán, la Unidad de Sistemas e Infraestructura, el Departamento de Gestión de Personas, y los Administradores Funcionales de Sistemas.
Todo funcionario JUNAEB que no se encuentre vigente en JUNAEB, ya sea por retiro de la institución o por la suspensión de sus funciones, deberá ser bloqueada su cuenta de acceso y contraseña para autenticación en la red interna y en los diferentes aplicativos a los cuales se le otorgó acceso.
Es importante señalar que, el bloqueo de cuenta es informado al Departamento de Gestión de Personas.
El Departamento de Informática, a su vez, informará a los respectivos Administradores Funcionales de Sistemas, los bloqueos que les corresponda realizar según su responsabilidad.

5 REVISIONES

Esta Política de Gestión de Contraseñas tendrá vigencia de tres años calendario desde su aprobación; no obstante, el Secretario General podrá autorizar revisiones y modificaciones antes del periodo de vencimiento.

6 DIFUSION

La Política de Gestión de Contraseñas, se comunica y difunde a todo el personal de la institución, informando de su publicación en la intranet institucional, lo cual permite su libre consulta a todo el personal de JUNAEB. El acceso a la intranet institucional es a través de su login y password personal.

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.	17/11/2017	Departamento de Informática

DIRECCIÓN

PROCEDIMIENTO DE GESTIÓN DE CONTRASEÑAS

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 de gestión de contraseñas.

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

A) CUENTAS DE ACCESO PARA USUARIOS

1-El solicitante responsable de pedir una cuenta de usuario y/o contraseña deberá proveer los datos nombre completo, departamento o regional donde se desempeña, calidad jurídica de contrato, honorarios y/o practicante, fecha de ingreso y fecha de término según sea su contrato, función a cumplir.

2-En caso de ser una cuenta para usuarios de empresas o servicios externos que tengan relación contractual con JUNAEB debe enviar nombre completo, departamento o regional donde se desempeña, proyecto o contrato que lo rige, funcionario responsable del contrato, fecha de ingreso y fecha de término según sea su contrato, función a cumplir.

3-Los puntos 1 y 2 deben ser enviados por el sistema de mesa de ayuda del departamento de informática y/o por correo electrónico a mesa.ayuda@junaeb.cl, al correo del Jefe de Informática y/o Encargado de Control de Gestión. Debe señalar también los accesos a los sistemas o servicios que requiere. Debiéndose regir además por la Política de Gestión de Acceso con privilegios especiales.

4-La mesa de ayuda, validará los datos, de ser correctos asignará el caso a la unidad de sistema y/o a el administrador Funcional de los sistemas solicitado. De lo contrario denegará la solicitud.

La solicitud de acceso a sistemas o cuentas para los cuales el solicitante no tenga ninguna responsabilidad en función de trabajo, serán denegados.

DIRECCIÓN

En casos que existan dudas por la solicitud deberá pedir la aprobación al Jefe del Departamento de Informática quien determinara su aprobación o rechazo.

5-El o los administradores Funcionales de sistemas deberán realizar lo solicitado e informar el procedimiento a seguir según el sistema o plataforma a acceder por correo electrónico y por teléfono según corresponda al funcionario solicitante.

B) USO Y MANTENCIÓN DE CONTRASEÑA

1-El solicitante responsable debe pedir el cambio de una cuenta de usuario y/o contraseña deberá proveer los datos necesarios para cada plataforma, ej: cambio de perfil de acceso, cambio de contraseña. Deben ser enviados por el sistema de mesa de ayuda del departamento de informática y/o por correo electrónico a mesa.ayuda@junaeb.cl, al correo del Jefe de Informática y/o Encargado de Control de Gestión.
2-La mesa de ayuda, validará los datos, de ser correctos asignará el caso a la unidad de sistema y/o a el administrador Funcional de los sistemas solicitados. De lo contrario denegará la solicitud.
La solicitud de acceso a sistemas o cuentas para los cuales el solicitante no tenga ninguna responsabilidad en función de trabajo, serán denegados.

En casos que existan dudas por la solicitud deberá pedir la aprobación al Jefe del Departamento de Informática quien determinara su aprobación o rechazo.

3-El o los administradores Funcionales de sistemas deberán realizar lo solicitado e informar el procedimiento a seguir según el sistema o plataforma a acceder por correo electrónico y por teléfono según corresponda al funcionario solicitante.
4-El Encargado de Mesa de ayuda deberá monitorear que el requerimiento se cierre acorde a lo solicitado.

C) BLOQUEO DE CUENTA

1 – Funcionarios:
El Departamento de Gestión de Personas deberá informar al Departamento de Informática cuando un funcionario de cualquier categoría o practicante de JUNAEB que deje de ejercer como tal, ya sea por retiro de la institución o por la suspensión o término de sus funciones, renuncia, despido, jubilación, traslado, muerte, licencia extraordinaria, informando el bloqueo de su cuenta de acceso y contraseña para autenticación en la red interna y en los diferentes aplicativos a los cuales se le otorgó acceso, al Encargado de Control de Gestión y al Jefe del Departamento de informática.
2- Contratos con empresas o servicios externos:
El Responsable del Contrato de JUNAEB deberá informar al Departamento de Informática cuando la empresa o el servicio deje de prestar funciones con JUNAEB informando el bloqueo de su cuenta de acceso y contraseña para autenticación en la red interna y en los diferentes aplicativos a los cuales se le otorgó acceso al Encargado de Control de Gestión y al Jefe del Departamento de informática.
3-. Departamento de Informática:

3.1- El Encargado de Control de Gestión o el Jefe del Departamento de informática informará a la Mesa de ayuda por correo electrónico del bloqueo la cuenta del Funcionario o Contratos con empresas o servicios externos según sea el caso.

3.2-El Encargado de Mesa de ayuda deberá registrar el caso en el Sistema de mesa de ayuda para luego derivar a los Administradores Funcionales de Sistemas, los bloqueos que les corresponda realizar según su responsabilidad.

5- Excepciones
El Director del servicio y/o el Jefe del Departamento de informática tendrá la potestad de solicitar directamente bloqueo de cuentas producto de cualquier evento que afecte la seguridad, confidencialidad, integridad o disponibilidad de información o por otra decisión justificada mediante correo electrónico a la mesa de ayuda del Departamento de Informática para seguir los pasos del punto C.1 de este mismos documento.

DIRECCIÓN

D) SEGURIDAD

1-Los usuarios serán responsables de todas las actividades y accesos que se realicen bajo su usuario, por lo que está expresamente prohibido ceder o comunicar la contraseña o mecanismo de autenticación a otros. Las contraseñas deben custodiarse debidamente y las mismas no deben teclearse bajo la mirada de otros.
2-En el caso de necesitar compartir datos o correos se usarán otros mecanismos como carpetas, directorios públicos o sistemas de trabajos en grupo.

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.

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 REVISION

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