GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO
ESCOLAR Y BECAS

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

RESOLUCIÓN EXENTA N° 3151

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.09.01.01 – Política de Control de Acceso
2. A.09.01.01 - Procedimiento de Control de Acceso

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

MBG/RFV/FFR/
DISTRIBUCIÓN:

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

DIRECCIÓN

POLITICA DE CONTROL DE ACCESO

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 lineamientos claros sobre el control de acceso lógico de usuarios, efectuado por sistemas informáticos de JUNAEB, administrados por el Departamento de Informática.

2. ÁMBITO DE APLICACIÓN

La presente política aplica a todo funcionario JUNAEB, independiente de su calidad jurídica o contractual, como planta, contrata, honorarios practicantes u otra persona natural o jurídica que tenga que tenga relación contractual con JUNAEB, que requiera acceso lógico a sistemas informáticos operativos, en cualquiera de las plataformas tecnológicas Institucionales administradas por el Departamento de Informática.

3. ROLES Y RESONSABILIDADES

JEFE DE DEPARTAMENTO DE INFORMÁTICA	Verificar la aplicación de la política, validando el ejercicio y conocimiento de la norma por los funcionarios y sus jefaturas.
ENCARGADA SEGURIDAD DE LA INFORMACIÓN	Verificar y monitorear la ejecución de la política.

4. POLÍTICA

Todo sistema informático administrado por el Departamento de Informática, posee un control de acceso lógico a sus funcionalidades y operaciones.

Dicho control de acceso se efectúa en una interfaz del sistema, en base a la autenticación del usuario, a partir de una validación mínima y conjunta de nombre de usuario y contraseña.

Estos datos individualizan al usuario del sistema de manera unívoca como persona, quién podrá realizar sólo un conjunto de operaciones determinadas, en base al perfil o rol que posea en el sistema.

Al proporcionar el usuario su contraseña, en la interfaz respectiva, el sistema oculta la escritura de la misma, manteniendo en todo momento el carácter secreto y personal de este dato.

Los sistemas informáticos, no permiten a usuarios no identificados la ejecución de procesos, participación en transacciones o la alteración de datos. En este sentido, para usuarios de tipo anónimo sólo son permitidas operaciones de consulta y la obtención de reportes destinados al público general. Si bien un sistema informático puede hacer uso de diferentes repositorios o bases de datos, sus usuarios sólo acceden a estos mediante las funcionalidades que implementa el sistema, habilitadas para un rol o perfil determinado.

La vigencia de las credenciales de usuario para su acceso lógico a sistemas, dependerá directamente de su cargo y/o labores asignadas por su jefatura directa, en el caso de funcionarios JUNAEB. En el caso de usuarios externos, la vigencia de sus credenciales de acceso, sistemas y perfil de operación, dependerán de lo estipulado en las cláusulas del contrato suscrito con la Institución.

DIRECCIÓN

5. 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.

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.

Todos los usuarios de la JUNAEB, tienen la responsabilidad de conocer la presente política y cumplir lo que en ella se indica.

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	Cambio	Fecha	Aprobado por:
BORRADOR	Elaboración inicial	19/08/2016	Departamento de Informática
01	Actualización de contenidos en base a definiciones ISO 27002	17/10/2016	Departamento de Informática
02	Actualización del Documento	03/08/2017	Departamento de Informática
03	Modificaciones menores	17/11/2017	Departamento de Planificación

DIRECCIÓN

PROCEDIMIENTO DE CONTROL DE ACCESO

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

INDICE

1. OBJETIVO

Establecer las actividades sobre el control de acceso lógico de usuarios, efectuado por sistemas informáticos de JUNAEB, administrados por el Departamento de Informática.

2. ÁMBITO DE APLICACIÓN

El procedimiento aplica al uso y operación de acceso lógico de usuarios de las plataformas administradas por el Departamento de Informática de JUNAEB, aplica a todo funcionario JUNAEB (planta, contrata, honorarios practicantes u otra persona natural o jurídica que tenga que tenga relación contractual con JUNAEB) y contratos y/o servicios externos que tengan relación con JUNAEB.

3. ROLES Y RESPONSABILIDADES

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

DIRECCIÓN

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

El solicitante responsable de pedir acceso deberá proveer datos según lo indica la política y procedimiento de Sistema de Gestión de Contraseñas.

b. Acceso para conexiones externas

El Departamento de Informática contempla como servicios de conexiones externas VPN para funcionarios y empresas externas que tengas relación contractual con JUNAEB que requieran conexión remota a la red de datos institucional. La autenticación a los servicios VPN para usuarios con conexiones externas, para administrar este servicio deberá seguir el siguiente procedimiento:

1 - El solicitante responsable de pedir acceso deberá proveer según los indica la política y procedimiento de Sistema de Gestión de Contraseñas y además deberá llenar el formulario de solicitud de VPN que deberá ser entregado por la Unidad de Ingeniería de Sistemas e Infraestructura en formato digital y papel.

2 - El formulario debe ser aprobado por el Jefe del Departamento Demandante.

3 - El documento debe ser resguardada por la Unidad de Ingeniería de Sistemas e Infraestructura en formato digital y papel.

Responsabilidades

Es de responsabilidad del funcionario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.

El uso del sistema VPN debe ser controlado utilizando una contraseña de autenticación fuerte.

Cuando esté conectado activamente a la red del JUNAEB, el sistema VPN obligará a todo el tráfico hacia y desde el equipo computacional pasar a través del túnel de VPN, el resto del tráfico será denegado.

La utilización de múltiples conexiones no está permitida, sólo se debe utilizar una conexión por usuario.

Las puertas de enlace VPN serán configuradas y administradas por la Unidad de Ingeniería de Sistemas e Infraestructura.

Los usuarios del Sistema VPN serán automáticamente desconectados de las redes del JUNAEB, una vez que hayan pasado 30 minutos de inactividad.

El usuario deberá autenticarse nuevamente para reconectarse a la red, El concentrador VPN está limitado para un tiempo de conexión absoluta de 24 horas.

4- La Unidad de Ingeniería de Sistemas e Infraestructura realizará Monitoreo de las conexiones VPN.

DIRECCIÓN

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

Departamento de Informática

FORMULARIO DE SOLICITUD DE VPN

FECHA: ____ /____ /_____

Este formulario debe ser llenado digitalmente para UNA solicitud (timbrado y firmado por Jefe departamento o Encargado de la unidad), adjuntando formulario al sistema ARANDA.

El objetivo de las cuentas VPN, es poder conectar a usuarios o empresas que están fuera de la Red JUNAEB, a los distintos Sistemas Institucionales (portal, intranet, etc.).

I. IDENTIFICACIÓN DE LA CUENTA SOLICITADA

NOMBRE COMPLETO DEL USUARIO/EMPRESA	
DEPARTAMENTO/OFICINA/EMPRESA	
CARGO/PUESTO/FUNCION:	
JEFE DEPTO O ENCARGADO DE UNIDAD QUIEN OTROGA PERMISOS	
CORREO DEL USUARIO/EMPRESA:	
TELEFONO/ANEXO DE USUARIO/EMPRESA:	
EN CASO DE CONEXIÓN A SERVIDORES	
SERVIDORES	
NOMBRE	
IP	
NOMBRE DE USUARIO SERVIDOR	
PUERTOS REQUERIDOS	

II. VIGENCIA DE LA SOLICITUD

Fecha Inicio de operaciones (dd/mm/año): ____ / _____ / _____
Fecha Cierre de operaciones (dd/mm/año): ____ / _____ / _____

III. DESCRIPCIÓN DE LA UTILIZACIÓN DEL SERVICIO:

IV. CONDICIONES GENERALES

1. **Este formulario debe ser llenado digitalmente para UNA solicitud (timbrado y firmado por Jefe departamento o Encargado de la unidad), adjuntando formulario al sistema ARANDA.**
2. **El acceso estará disponible en 48 horas desde la entrega del formulario.**

_____
FIRMA & TIMBRE
UNIDAD SOLICITANTE

Departamento de Informática

Fuente propia, Departamento de informática

DIRECCIÓN

7. DIFUSION

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