Gobierno de Chile

Superintendencia de Educación

MPV/MFA/XBG/CNN/ PCC/LDZ/HCJ/RBC/PSY

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°2199, DE FECHA 25 DE NOVIEMBRE DE 2016, DE LA SUPERINTENDENCIA DE EDUCACIÓN Y APRUEBA POLÍTICA USO DE CONTRASEÑAS VERSIÓN N°3, EN EL MARCO DE LA SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0822

Santiago, 01 DIC 2017

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 el Decreto N°571, de 2014, del Ministerio de Educación; 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; 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, y la Resolución N°1600 de 30 de octubre de 2008, 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, en atención a que los Órganos de la Administración del Estado tienen la obligación de respetar la normativa vigente respecto de la Seguridad de la Información, esta Superintendencia procedió a la designación de un Encargado de Seguridad de la Información, que actuará como asesor del Jefe de Servicio en las materias relativas a la seguridad de los documentos electrónicos y los activos de información institucionales.

3. Que, con fecha 25 de noviembre de 2016 se dicta Resolución Exenta N°2199, de esta Superintendencia que aprobó la Política uso de contraseñas versión N°2.

4. Que, debido a una serie de cambios institucionales y a la revisión efectuada por el Encargado de Seguridad de la Información se ha estimado procedente, reestructurar y ajustar el contenido de la Política uso de contraseñas versión N°2, aprobada mediante Resolución Exenta N°2199 de fecha 25 de noviembre de 2016.

RESUELVO:

1. **DÉJESE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 2199, de 2016 de la Superintendencia de Educación.

2. **APRUÉBASE,** la Política uso de contraseñas versión N°3, de la Superintendencia de Educación, cuya transcripción, fiel, exacta e integra se adjunta a la presente Resolución.

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

4. **DISPÓNGASE,** que el/la Jefe/a de la División de Administración General, deberá tomar todas las medidas y acciones tendientes a la implementación de esta política.

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

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

ANÓTESE, COMUNIQUESE Y ARCHÍVESE

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACION
SUPERINTENDENTE

ALEXIS RAMIREZ ORELLANA
SUPERINTENDENTE
SUPERINTENDENCIA DE EDUCACIÓN

Distribución:
1. Gabinete.
2. División de Fiscalización.
3. División de Fiscalía.
4. División de Promoción y Resguardo de Derechos Educacionales.
5. Intendencia de Educación Parvularia.
6. División de Administración General.
7. Departamento de Finanzas.
8. Departamento Gestión de Personas.
9. Departamento de Administración.
10. Departamento de Tecnologías de Información.
11. Direcciones Regionales (15).
12. Departamento de Auditoría.
13. Coordinación de Gestión y Desarrollo.
14. Oficina de Partes.

Superintendencia de Educación
TOTALMENTE TRAMITADO

POLÍTICA DE USO DE CONTRASEÑAS

VERSIÓN 3.0

CONTROL ISO27002:2013

A.9.3.1

INDICE

1. Objetivo:

Para todo sistema informático de la Superintendencia de Educación (SUPEREDUC), el usuario debe señalar quién es (identificación) y luego debe comprobar que es quién dice ser (autenticación).

El objetivo de la presente política es hacer que los usuarios sean responsables de proteger su información de autenticación, la cual es privada, única e intransferible y no debe ser compartida.

2. Alcance:

Esta política se aplica a todas las áreas de la SUPEREDUC y a los procesos de provisión de bienes y servicios definidos en el Formulario A1 de Definiciones Estratégicas.

Esta política aplica a todos los Usuarios[1], ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes, otros trabajadores y empresas que presten servicios a la SUPEREDUC, que necesite tener acceso a los recursos de la red.

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

- A.09.03.01 Uso de información de autenticación secreta.

3. Roles y Responsabilidades:

- **Jefaturas Directas:**
  - Velar por el correcto cumplimiento de esta política.

- **Departamento de Tecnologías de Información:**
  - Gestionar y administrar la información de autenticación.
  - Custodiar las claves de cuentas de administración estándar de los sistemas.
  - Atender las peticiones y requerimientos de los usuarios de la institución, ante solicitudes asociadas a problemas con contraseñas.
  - **Gestor de Servicios TI:**
    - Registrar, clasificar y dar respuesta a los requerimientos reportados.
- **Usuarios:**
  - Cumplir con lo establecido en esta política.

4. Definiciones:

a) **Username**: Nombre utilizado para identificar al usuario que está accediendo a un determinado sistema o recurso informático.

[1] Se entiende por Usuarios a los funcionarios/as en calidad jurídica planta, contrata, personas contratadas a honorarios suma alzada y terceros que trabajen para SUPEREDUC

b) **Password**: Contraseña secreta utilizada para autenticar al usuario según sus derechos de acceso y privilegios.

5. Documentos relacionados:

a) Política general de seguridad de la información.
b) Política uso de computadores.
c) Política para el uso de internet y correo electrónico institucional.
d) Anexo A: Procedimiento para generación de contraseñas seguras.
e) Procedimientos internos o estándares en construcción.

6. Política:

6.1. Identificación y contraseñas requeridas

a) Antes de tener acceso a cualquier recurso de la red de SUPEREDUC, todos los usuarios deben ser identificados exitosamente mediante su nombre de usuario y su contraseña.
b) El nombre de usuario y su contraseña deben ser individuales, es decir, debe ser privada, única e intransferible, no debe ser compartida, el usuario será el único responsable de las acciones efectuadas bajo el uso de su cuenta personal.
c) Se debe mantener la información de autenticación secreta como confidencial, está prohibida su divulgación, sin excepciones.
d) Se debe evitar mantener un registro (es decir, en papel, archivo de software o en un dispositivo de mano) de la información de autenticación secreta.
e) Se debe cambiar la información de autenticación secreta cuando exista alguna indicación de su posible compromiso.
f) Se sugiere seleccionar contraseñas con una longitud mínima suficiente que tengan las siguientes características:
    i. Fáciles de recordar.
    ii. Que no se basen en nada que otra persona pueda adivinar u obtener fácilmente mediante la información relacionada con la persona, es decir, nombres, números de teléfono y fechas de nacimiento, etc.
    iii. Que no sean vulnerables a ataques de diccionario (es decir, que no conste de palabras incluidas en los diccionarios).
    iv. Que estén libre de caracteres idénticos consecutivos, que sean todos numéricos o alfabéticos.
g) Está prohibido compartir la información de autenticación secreta de usuario, ya sea propia o de un tercero.
h) Se debe evitar utilizar la misma contraseña en todos los sistemas y/o las utilizadas para uso personal.

i) Evitar el autoguardado de contraseñas en los exploradores de internet o en cualquier aplicación que lo solicite.

6.2. Cambio periódico de las contraseñas

a) Todos los usuarios deben cambiar su contraseña cada 120 días[2].

b) Las contraseñas no deben ser reutilizadas en el tiempo ni en distintos sistemas. Los usuarios no deben construir contraseñas que sean idénticas o similares a las últimas ya utilizadas, de acuerdo al valor definido como estándar de SUPEREDUC para cantidad de contraseñas históricas a chequear.

6.3. Asignación de contraseñas expiradas y reasignación de contraseñas

a) La contraseña asignada a una nueva cuenta obligará al usuario a cambiarla durante su primera conexión.

b) La solicitud de cambio de contraseña por olvido, se debe efectuar al Departamento de Tecnologías de Información al anexo 55555, previa identificación positiva del usuario que lo solicita.

c) Toda reasignación de contraseñas será registrada en la bitácora del sistema y debe notificarse al usuario de la cuenta, a su casilla de correo registrada al crear la cuenta asociada. Esto permite detectar suplantación de identidad.

d) El Departamento de Tecnologías de Información dispondrá de herramientas que eviten posibles tácticas de suplantación de identidad de usuarios[3] u otros artilugios para obtener información a la cual no tiene acceso normalmente.

6.4. Límite a intentos fallidos de ingreso

a) Para prevenir ingresos mediante la prueba de varias posibles contraseñas, se limita la aceptación de 3 intentos consecutivos de ingreso, configurado como estándar de SUPEREDUC. Después de los intentos fallidos, la cuenta de usuario será bloqueada.

b) El usuario notificará al Departamento de Tecnologías de Información al anexo 55555, quien habilitará la cuenta (desbloqueo), previa verificación de la identidad del usuario y generando el informe de atención respectivo.

7. Publicación y comunicación de esta política

La comunicación de esta política se efectuará de manera que los contenidos de la documentación sean accesibles y comprensibles para todos los usuarios, pudiendo utilizarse

---

[2] Solo para los casos en que el usuario no cuente con múltiples factores de autenticación.

[3] La autenticación de factores múltiples se puede lograr usando una combinación de los siguientes factores:
Algo que usted conoce: contraseña o número de identificación personal (PIN)
Algo que usted tiene: token, tarjeta inteligente, smartphone (autenticación de dos factores)
Algo que usted es: biometría, tal como una huella dactilar (autenticación de tres factores)

los canales de difusión establecidos por la SUPEREDUC (www.supereduc.cl, intranet, email, circulares, etc).

8. Aceptación de la política

Todos los usuarios de la SUPEREDUC, sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar ésta 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 y procedimientos vigentes de seguridad de la información 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.

9. Revisión de la política

La presente política será evaluada y revisada al menos una vez al año, o cuando SUPEREDUC lo requiera, para asegurar su continuidad e idoneidad, considerando cambios externos o internos que puedan afectarla.

10. Sanciones aplicables

El incumplimiento o violación a esta política, 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. Control de versiones:

Control de versiones		
Versión	**Resumen de cambios**	**Fecha**
1.0	- Versión inicial	Agosto 2015
2.0	- Actualización Política	Octubre 2016
3.0	- Punto 2.0, se incorpora al alcance las definiciones de Ficha A1. - Puntos 6.3, 6.4, se modifica el 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.	Noviembre 2017

12. Responsabilidades de elaboración y aprobación del documento:

Elaborado Por	Revisado Por	Aprobado Por
Encargado de Seguridad de la Información	Comité Operativo de SSI	Comité Directivo SSI

13. Anexos

ANEXO A:

Procedimiento de generación de contraseña segura

Introducción

Los nombres de las cuentas y los identificadores de los usuarios son fáciles de obtener por un atacante, lo cual tiene el camino abierto para vulnerar la red. Las contraseñas fáciles de adivinar, las contraseñas por defecto y las cuentas sin contraseñas constituyen un grave problema de seguridad.

Las contraseñas proveen un medio de validar la identidad de los usuarios y establecer los derechos de acceso a los servicios y activos de información, por esta razón es altamente necesario definir una política estricta en relación al uso y generación de las contraseñas de los usuarios. Al mantener una contraseña fuerte tu información y la del SUPEREDUC estará mejor protegida.

Recomendaciones para crear una Password Fuerte

1. Que contenga al menos 8 caracteres
2. Que no sea igual a su nombre, apellido, al de la empresa o a un nombre real. La contraseña no debe contener el nombre de usuario de la cuenta
3. Que no corresponda a una palabra completa del diccionario (que no tenga significado)
4. Que su significado sea absolutamente distinto a las password anteriores (password1, password2 ... estas no son buenas password)
5. Que contenga al menos un símbolo.
6. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" ó "98765")
7. Que contenga caracteres de cada uno de los grupos de la siguiente tabla:

Letras Mayúsculas	A, B, C
Letras Minúsculas	a, b, c
Números	0,1, 2, 3, 4, 5,6....
Símbolos del Teclado	¡ @ $ % & ( ) += { } ¿?

   Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.

8. Que NO contenga alguno de los caracteres de cada uno de los grupos de la siguiente tabla:

Símbolos del Teclado	# * ~~§
Letras Mayúsculas	Ñ
Letras Minúsculas	Ñ

9. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el RUN o número de teléfono.
10. No enviar nunca la contraseña por correo electrónico o en un SMS o whatsapp. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que le soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla. Casi con total seguridad se tratará de un fraude. La Superintendencia de Educación nunca le va a solicitar ese tipo de información.
11. No se deben almacenar las contraseñas en un lugar público y al alcance de los demás (encima de la mesa escrita en papel, etc...).
12. No utilizar la opción de "Guardar contraseña" que en ocasiones se ofrece, para evitar reintroducirla en cada conexión.
13. No debe contener la contraseña anterior (ni viceversa) y No debe coincidir con ninguna de las 4 contraseñas anteriores.