Superintendencia de Educación

MPV/MFA/XBG/CNN/ PCC/LOZ/HCJ/PSC/PSY

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°2201, DE FECHA 25 DE NOVIEMBRE DE 2016, DE LA SUPERINTENDENCIA DE EDUCACIÓN Y APRUEBA POLÍTICA PARA EL USO DE INTERNET Y CORREO ELECTRÓNICO INSTITUCIONAL VERSIÓN N°3, EN EL MARCO DE LA SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0826

Santiago, 01 DIC 2017

VISTO:

Lo dispuesto en el DFL N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en el Decreto con Fuerza Ley N° 29, de 2004, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en la Ley N° 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 N° 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 N° 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°2201, de esta Superintendencia que aprobó la Política para el uso de internet y correo electrónico institucional 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 para el uso de internet y correo electrónico institucional versión n°2, aprobada mediante Resolución Exenta N°2201 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° 2201, de 2016 de la Superintendencia de Educación.

2. **APRUÉBASE,** la Política para el uso de internet y correo electrónico institucional 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 PARA EL USO DE INTERNET Y CORREO ELECTRÓNICO INSTITUCIONAL

VERSIÓN 3.0

CONTROL ISO27002:2013

A.8.1.3

A.13.2.3

ÍNDICE

1. Objetivo 5
2. Alcance 5
3. Roles y Responsabilidades 5
4. Definiciones 6
5. Documentos relacionados 6
6. Política 7
6.1. Uso correcto de Internet 7
6.1.1. Gestión de perfiles de Usuario: 7
6.1.2. Uso de Internet: 7
6.2. Restricciones al Uso de Internet 7
6.3. Cuentas de Usuario y contraseñas 8
6.4. Correo Electrónico Institucional 8
6.4.1. Estructura de la dirección de correo 8
6.4.2. Uso del correo electrónico 9
6.4.3. Mensajes masivos 10
6.4.4. Acceso al correo electrónico 11
6.4.5. Restricciones al uso y contenido del correo electrónico 11
6.4.6. Privacidad de los mensajes electrónicos 11
6.5. Uso del correo electrónico en el caso de desvinculaciones, renuncias y otros 12
7. Publicación y comunicación de esta política 12
8. Aceptación de la política 12
9. Revisión de la política 12
10. Sanciones aplicables 12
11. Control de versiones 13
12. Responsabilidades de elaboración y aprobación del documento: 13
13. Anexos 14
ANEXO A: Protocolo de uso de redes sociales 14
ANEXO B: Protocolo para encriptar archivos, utilizando WinZip con WinRar. 15
ANEXO C: Instructivo para solicitar acceso a recursos restringidos de Internet: 17

1. Objetivo

El propósito de esta política es regular en la Superintendencia de Educación (SUPEREDUC) la navegación hacia Internet, definiendo categorías generales y específicas, las cuales otorgaran el acceso o bloqueo de los diferentes sitios en Internet y asegurar la continuidad de los servicios de correo electrónico institucional, minimizando los eventuales daños a las operaciones, garantizando el cumplimiento de los objetivos de la SUPEREDUC, regulando su uso, confidencialidad e integridad y almacenamiento de correos electrónicos.

1.1. Objetivos específicos:

a) Ofrecer a los Usuarios una guía sobre los requerimientos mínimos que deben ser cumplidos respecto del uso del correo electrónico institucional que provee el Servicio, como también las implicancias del mal uso.

b) Garantizar la disponibilidad de las redes para el correcto uso y funcionamiento de los sistemas de información institucionales (SIPA, SIFE, CRM, SIGPER, SIGFE, entre otros).

c) Evitar congestión en las redes provocando lentitud en el servicio.

d) Evitar problemas jurídicos tanto nacionales como internacionales, debido al incorrecto uso de los recursos.

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 y otros trabajadores, incluyendo visitas y empresas que presten servicios a la SUPEREDUC.

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

- A.08.01.03 Se deberían identificar, documentar e implementar las reglas para el uso aceptable de la información de los activos asociados a la información y a las instalaciones de procesamiento de información.
- A.13.02.03 Mensajería electrónica.

3. Roles y Responsabilidades

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

[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

- **Departamento de Tecnologías de Información:**
  - Mantener la seguridad y disponibilidad de los sistemas de información.
  - Administrar y dar soporte a los servicios de Internet, red y correo electrónico.
  - Mantener a los Usuarios informados sobre nuevas amenazas y cuidados con respecto al resguardo de la comunicación.
  - Aplicar las medidas necesarias para monitorear el cumplimiento de esta política.
  - **Gestor de Servicios TI:**
    - Registrar, clasificar y dar respuesta a los requerimientos reportados.
- **Encargado de Seguridad de la Información**:
  - Velar por el cumplimiento de esta política.
  - Difundir esta política.
- **Usuarios**
  - Cumplir con lo establecido en esta política.
  - Ser responsable del acceso permitido para el uso de Internet.

4. Definiciones

a) **Activo de Información**: Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

b) **Uso aceptable de internet**: Uso aceptable para el cometido de las funciones o aplicaciones siempre y cuando no contravenga alguna normativa o restricción de esta política.

c) **Cuentas Genéricas**: Son cuentas o alias de correo electrónico que son utilizados por un equipo o grupo de personas para una determinada función y no se utilizan para la comunicación personal, se designa uno o varios Usuarios para la administración de la cuenta.

d) **OneDrive:** Almacenamiento en la nube institucional que permite guardar archivos o documentos en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet con la cuenta de usuario.

5. Documentos relacionados

a) Política de Uso de Contraseñas.

b) Ley N° 17.336 de 02 de octubre de 1970, sobre Propiedad Intelectual y Derechos de Autor.

c) Ley N° 19.628 de 28 de agosto de1999 sobre Protección Datos Personales.

d) Ley N° 20.285 de 20 de agosto de 2008 sobre Acceso a la Información Pública.

e) Anexo A: Protocolo de uso de redes sociales.

f) Anexo B: Protocolo para encriptar archivos, utilizando winzip.

g) Anexo C: Instructivo para solicitar acceso a recursos restringidos de Internet.

6. Política

6.1. Uso correcto de Internet

Para garantizar el nivel de servicio de navegación a Internet se mantendrá un monitoreo permanente, priorizando las comunicaciones que la SUPEREDUC requiere mantener con otras entidades gubernamentales y privadas necesarias para el funcionamiento de los sistemas del negocio.

6.1.1. Gestión de perfiles de Usuario:

a) El uso de la red se encuentra disponible para todos los Usuarios, pero los permisos para el uso de Internet, estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada Usuario.

b) La asignación de perfiles de Usuario es realizada por cada jefe de área de acuerdo al perfil de cargo de cada funcionario/a (cuya descripción se encuentra a cargo de la encargada de reclutamiento en el área de gestión de personas), este perfil de Usuario es informado a soporte, quien realizará la asignación de privilegios de acuerdo a lo indicado por cada jefe de área.

6.1.2. Uso de Internet:

a) Los Usuarios de la red de SUPEREDUC deben utilizar, como primera opción para conectarse a Internet, los medios dispuestos por la institución. De existir problemas con la conexión principal, los Usuarios pueden acceder a través de otros canales de proveedores de servicios de Internet externos. Cuando se use la opción alternativa, ésta debe ser resguardada con medidas de seguridad tales como firewall entre la institución y la salida a Internet, equipos de escritorio actualizados en cuanto a antivirus, firewall del equipo, antimalware y parches de seguridad.

b) Las soluciones inalámbricas deben contar con portales cautivos para que los invitados que necesiten conexión a Internet sólo puedan usar de manera controlada este medio, además de asegurar que la red de trabajo de la institución se mantenga aislada de los mismos.

c) Toda información entrante y saliente a Internet, es monitoreada y registrada.

d) Los Usuarios no deben almacenar contraseñas en los navegadores.

6.2. Restricciones al Uso de Internet

a) Se prohíbe descargar desde Internet, material que infrinja el Ordenamiento Jurídico Nacional o en la normativa interna establecida en la SUPEREDUC.

b) No está permitido almacenar información institucional en sitios o nubes de almacenamiento virtual provisto por terceros (dropbox, google drive, etc.), la

institución provee de recursos específicos para ello (almacenamiento en OneDrive[2] de Office 365).

c) No está permitido utilizar los equipos computacionales entregados por la SUPEREDUC para actividades no relacionadas con las asignadas a su rol profesional. El cumplimiento de estas restricciones, se regulará de acuerdo al perfil de cada Usuario, en particular se debe evitar:
   i. Descargar sistemas de audio/video vía Internet (Youtube, radios online, Spotify, entre otros). Se excluyen los medios de prensa.
   ii. Cargar y/o descargar archivos de música.
   iii. Cargar y/o descargar archivos de imágenes y videos.
   iv. Cargar y/o descargar juegos o jugar juegos online.
   v. Instalar sistemas de telecomunicaciones ajenos a los corporativos.
   vi. Construcción y/o hosting de sitios web personales o ajenos a la institución.
   vii. Transferencia de archivos a través de protocolo SFTP, FTP, u otros no autorizados bajo convenios de interoperabilidad.
   viii. Está prohibido ingresar a páginas con contenidos pornográficos, pedófilos y otros relacionados.
d) Cuando el Usuario requiera el acceso a un sitio que se encuentre bloqueado, solo será permitido con la debida autorización formal de su Jefatura, Jefe Departamento de Tecnología Información y Encargado de Seguridad.
e) Se recomienda leer y considerar para el uso de redes sociales, el Anexo A: *"Protocolo de uso de redes sociales"* de la SUPEREDUC.

6.3. Cuentas de Usuario y contraseñas

a) El Usuario es responsable del mantenimiento de la seguridad tanto de su propia información como de sus cuentas asignadas y contraseñas. El cambio y uso de contraseñas debe ser de acuerdo a la *"Política Uso de Contraseñas"*.
b) Las cuentas y contraseñas son asignadas a Usuarios individuales y no pueden ser compartidas con otras personas. Los Usuarios son responsables también por el tráfico y el contenido de la información de las cuentas asignadas.

6.4. Correo Electrónico Institucional

6.4.1. Estructura de la dirección de correo

a) El formato de una cuenta de correo electrónico para los alias del dominio "supereduc.cl" es:<alias_del_Usuario>@supereduc.cl

[2] Almacenamiento online (One Drive de Office 365) que se compenetra perfectamente con las herramientas que usa a diario para crear, comunicarse y colaborar desde su equipo PC o Mac o su dispositivo iOS®, Android™ o Windows

El alias del Usuario estará formado por el primer nombre del funcionario/a punto el primer apellido completo. Si el alias elegido ya está en uso, se podrá utilizar la combinación que Gestión de Personas, a través de la encargada de reclutamiento, indique al Departamento de Tecnologías de Información, con un mínimo de 48 horas de aviso para gestionarla.

b) La creación de cuentas genéricas, se gestionarán a través de la jefatura del área solicitante, quien la solicitará vía correo electrónico al Departamento de Tecnología de Información, mesadeservicio@supereduc.cl, o al anexo 55555, con un mínimo de 48 horas de aviso para gestionarla. Las cuentas genéricas no reemplazan a ningún correo electrónico de funcionario/a, sólo se utilizan como listas de distribución.

6.4.2. Uso del correo electrónico

a) Los correos electrónicos proveen de una comunicación rápida y eficiente tanto dentro como fuera de la institución. Está prohibido el uso de correos personales para fines laborales, sólo se debe utilizar las herramientas provistas por SUPEREDUC para la comunicación electrónica.

b) Los correos electrónicos enviados y recibidos están almacenados en los equipos informáticos de SUPEREDUC y serán retenidos por el tiempo que la institución estime necesario de acuerdo a criterios legales y administrativos.

c) Ocasionalmente los funcionarios/as utilizan los sistemas de correo electrónico para propósitos personales. Esto está permitido siempre que no afecte el trabajo para el cual fue contratado ni su contenido pueda afectar negativamente a los intereses y/o lineamientos generales de la institución. Es importante que se tenga en cuenta que este tipo de comunicación se genera bajo el nombre de SUPEREDUC y esto puede afectar la imagen de la institución.

d) El uso de correos electrónicos es un recurso compartido, por lo tanto, los mensajes y archivos personales deben manejarse en el rango mínimo de almacenamiento de espacio.

e) Correos personales no deben estar archivados en el sistema por más tiempo del estrictamente necesario.

f) Toda casilla de correo electrónico institucional está directamente vinculada al funcionario/a y él es responsable del contenido y de los archivos adjuntos a cada mensaje.

g) El resguardo de las claves de acceso al correo electrónico es de exclusiva responsabilidad del Usuario, no se deben divulgar, compartir ni anotarlas en lugares visibles y/o de fácil acceso.

h) Como regla general, toda información de la SUPEREDUC no debe ser compartida con terceros sin la debida autorización de la respectiva Jefatura. Siempre se debe tener en cuenta que existe un alto riesgo de intercepción de la información, por esta razón

se recomienda no enunciar el contenido de información confidencial o sensible en el título de un correo electrónico.

i) Cualquier información que contenga datos personales o información sensible, debe ser encriptada con una contraseña para su envío, la que se entregará por parte del remitente vía telefónica, sin dejar registro escrito de ella en el correo electrónico. (Ver Anexo B)

j) Si bien la SUPEREDUC cuenta con sistema de gestión de seguridad de la información, no es posible garantizar la totalidad de ésta. Si los Usuarios tienen dudas respecto a la información que enviará, debe consultar con su jefatura o con el Encargado de Seguridad de la Información.

6.4.3. Mensajes masivos

a) Se prohíbe el envío, mediante correo electrónico institucional, de ofertas de compra o venta, así como también cualquier tipo de cartas en cadena, pirámides o Phishing, o enviar un correo electrónico solicitando donaciones caritativas, peticiones o cualquier material relacionado.

b) Se prohíbe el envío de mensajes masivos que comprometan el prestigio o nombre de la SUPEREDUC o de alguno de sus miembros, de acuerdo a lo establecido en el artículo 25 letra i), del decreto Supremo N° 83 del año 2004, del Ministerio Secretaria General de la Presidencia.

c) El envío masivo de información se gestionará a través de la jefatura del área solicitante, quien la solicitará vía correo electrónico al Departamento de Tecnología de Información, mesadeservicio@supereduc.cl, al anexo 55555 con un mínimo de 24 horas de aviso para gestionarla.

d) Se debe utilizar el pie de firma institucional, la cual será creada por el Departamento de Tecnología de Información de acuerdo a los estándares definidos en la Superintendencia.

e) Se prohíbe falsificar encabezados de correos electrónicos, es decir utilizar nombres de dominio que sean inválidos o inexistentes u otras formas engañosas de enviar correo electrónico.

f) Se prohíbe personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal, es decir, tomar el nombre de Usuario de otra persona y hacerse pasar por ella, para enviar un correo electrónico.

g) Si un Usuario se ausenta de sus labores por un tiempo considerable (vacaciones, licencias médicas, comisión de servicio, etc.), debe dejar su correo electrónico con respuesta automática, donde comunique que estará ausente por un período de tiempo, especificando las fechas e indicando el nombre y correo electrónico del funcionario/a que lo reemplazará.

6.4.4. Acceso al correo electrónico

Se prohíbe el intento de obtener acceso a los mensajes de correo electrónico de otro Usuario, sin su expreso permiso.

6.4.5. Restricciones al uso y contenido del correo electrónico

a) El Usuario interno o externo que utilice el correo electrónico institucional podrá enviar mensajes con un tamaño de hasta 10 MB, y recibirlos con un tamaño de hasta 10 MB, sin prejuicio que esta definición pueda cambiar de acuerdo a las necesidades, roles y funciones de cada uno de los Usuarios.

b) Se prohíbe el envío de publicidad o cualquier información de tipo comercial por correo institucional.

c) Los mensajes contenidos en el correo institucional, no podrán ser contrarios a las disposiciones del orden público y al respeto de los derechos fundamentales de las personas.

d) No se debe enviar por correo institucional, contenidos que no tengan relación con el trabajo o que excedan al tamaño asignado tales como videos, imágenes, archivos de audio (mp3), etc., a fin de no sobrecargar la red institucional.

e) Se prohíbe utilizar la cuenta de correo electrónico institucional para emitir opiniones personales en foros de discusión externas a la institución, listas temáticas u otras instancias de naturaleza polémica, que pueda crear conflictos al interior de la institución.

f) El Usuario de correo electrónico institucional debe evitar la instalación y ejecución de archivos adjuntos que sean desconocidos, cualquier duda que tenga respecto de la seguridad de algún adjunto, debe consultarla al Encargado de Seguridad.

g) El Usuario de correo electrónico debe tener cuidado con archivos adjuntos que descargue a su equipo, escanear con antivirus en caso de dudas u origen desconocido (formato imagen: jpg o gif, archivos en formato Word:doc o docx o archivos en formato pdf).

6.4.6. Privacidad de los mensajes electrónicos

El resguardo de información clasificada como confidencial secreta o reservada, de acuerdo a lo establecido en el artículo N° 21 de la Ley N° 20.285 del año 2008 (publicado en la Página Web de la Superintendencia link www.gobta.supereduc.cl, requiere medidas apropiadas. Si las necesidades de la institución obligan al envío de información mediante el sistema de correo, los Usuarios deben enviarlo únicamente a las personas que lo requieren. Es importante considerar que un mensaje de correo electrónico, puede ser impreso o reenviado a personas no autorizadas. En la confección y envío de mensajes confidenciales por e-mail, los Usuarios deben tomar las mismas precauciones a las

empleadas a los documentos confidenciales impresos. Se reitera que el manejo de la información confidencial debe ser encriptada.

6.5. Uso del correo electrónico en el caso de desvinculaciones, renuncias y otros.

a) El área de gestión de personas de la SUPEREDUC, informará mediante correo electrónico institucional al Departamento de Tecnologías de Información, cuando un funcionario/a sea desvinculado. Se procederá a respaldar y deshabilitar la cuenta de correo electrónico institucional e informará a través de respuesta automática que el Usuario ya no pertenece a la institución, acompañado de los datos de contacto de la persona que lo reemplace.

b) La deshabilitación de la cuenta de correo electrónico, será por un período de 6 meses, al término de este período, la cuenta será cerrada.

c) Se respaldará el correo igual que cualquier otro que esté en uso. El contenido del correo institucional será resguardado como información institucional.

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, pudiéndose utilizarse los canales de difusión establecidos por la SUPEREDUC (Intranet, Email, circulares, etc).

8. Aceptación de la política

Todos los Usuarios/as 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 y los controles de la norma Nch:27.001 desarrollados en esta política. - Puntos 6.4.1, 6.4.3, se modifica email de contacto y 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 SI	Comité Operativo de SSI	Comité Directivo SSI

13. Anexos

ANEXO A:

Protocolo de uso de redes sociales

El siguiente protocolo está compuesto por las reglas y conductas que deben seguir los Usuarios autorizados de la Superintendencia de Educación, con respecto a las Redes Sociales institucionales.

En este documento se incluye a:

Facebook: Facebook.com/supereducCL

Twitter: @supereduc_cl

Youtube: www.youtube.com/user/SuperintendenciaEE

1) No está permitido:

a) Responder preguntas a Usuarios con respecto al funcionamiento o cualquier asunto de la Superintendencia de Educación.

b) Realizar preguntas y comentarios con respecto al funcionamiento interno de la SUPEREDUC.

c) Usar las Redes Sociales de la SUPEREDUC como un canal de comunicación entre Usuarios.

d) Hablar en nombre de la SUPEREDUC en el muro y las publicaciones de las Redes Sociales.

e) Entregar cualquier tipo de información sobre la SUPEREDUC en las Redes Sociales de la misma.

f) Realizar comentarios negativos en Redes Sociales de la SUPEREDUC.

g) Realizar comentarios negativos sobre Usuarios y autoridades de la SUPEREDUC.

2) Está permitido

a) Hacer Me Gusta, comentar mensajes positivos y compartir contenido.

b) Ser parte de la comunidad de Superintendencia de Educación en Redes Sociales, es decir, ser fan en Facebook, seguidor en Twitter y estar suscrito al canal de Youtube.

c) Hacer Retweet en Twitter a la información entregada por Superintendencia de Educación.

d) Invitar a sus amigos a ser parte de las Redes Sociales de Superintendencia de Educación.

e) Compartir material de Youtube la SUPEREDUC entre amigos y contactos.

ANEXO B:

Protocolo para encriptar archivos, utilizando WinZip con WinRar

WinZip y WinRar son programas de compresión de archivos para Windows. Normalmente crea archivos *.zip o *.rar que cualquier persona puede abrir y extraer.

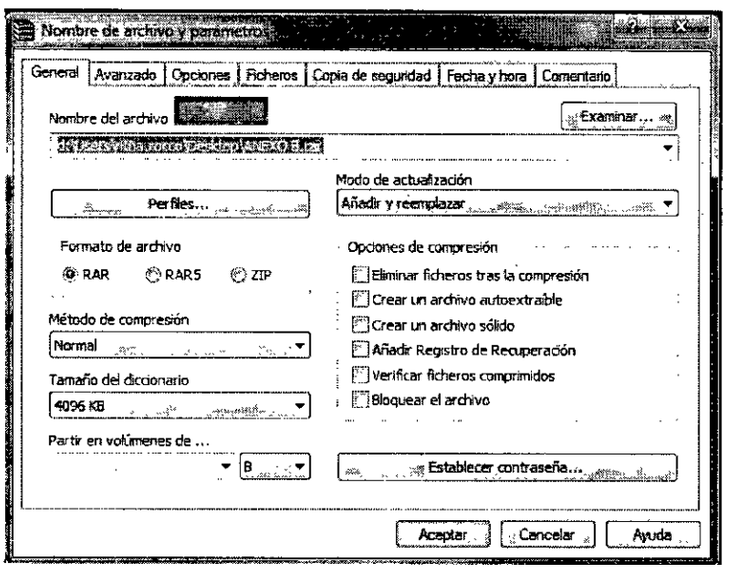
Para proporcionar seguridad, se agrega una contraseña a los archivos en formato WinZip o WinRar que puede cifrar los archivos dentro del archivo protegido por contraseña con un estándar de cifrado.

Los Usuarios que intenten abrir o extraer los archivos dentro del archivo zip necesitarán proporcionar la contraseña.

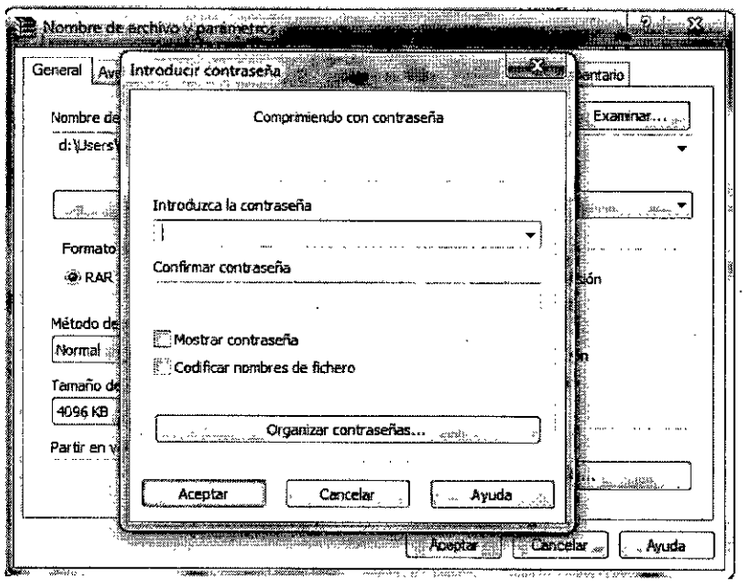
Instrucciones:

1. Abra el programa Winrar.
2. Seleccione la ubicación del archivo a encriptar en su equipo

   Haga clic en el botón "Examinar" cerca de la esquina superior izquierda de la ventana de Winrar o WinZip y una vez seleccionado, haga clic en "Aceptar".



3. Haga clic en la pestaña "Establecer contraseña " en el listón en la parte inferior de la ventana Winrar.



4. Escribe la contraseña en las cajas de "Introducir contraseña" y repita la contraseña en "Confirmar contraseña".
5. Haga clic "Aceptar".

Consejos y advertencias

Seleccione una contraseña fuerte con una combinación de letras, números y símbolos. Una simple contraseña como "contraseña" no proporciona mucha seguridad, incluso si es usada con una encriptación fuerte.

No se puede recobrar los contenidos del archivo zip (o rar) si olvidas tu contraseña.
La encriptación puede ser rota con una variedad de herramientas recuperadoras de contraseñas.

No proporcione en otro correo electrónico la contraseña de acceso, ya que, si alguien intercepta el archivo anterior, también podrá interceptar la contraseña, asegúrese de proporcionar sólo de manera telefónica la contraseña al receptor del mensaje.

ANEXO C:

Instructivo para solicitar acceso a recursos restringidos de Internet:

1) Cada vez que un Usuario que detecte la necesidad de acceder a recursos de Internet que han sido restringidos por la presente política, debe solicitar a su jefatura directa la tramitación de la debida habilitación del acceso.
2) Para ello el Usuario debe completar el Formulario de Solicitud de Acceso a Recursos Restringidos de Internet, publicado en la intranet de la SUPEREDUC, indicando el nombre su nombre, los servicios a los cuales solicita acceso y las fechas de inicio y de término que durará la habilitación.
3) Una vez autorizado por la jefatura, mediante la correspondiente firma del formulario, será recibido por el área de Coordinación de Tecnologías, la cual evaluará la solicitud notificando al Usuario y a la jefatura solicitante el resultado de esta.