JAL/FTO/ AAM/PBC/DLR

Superintendencia de Educación
TOTALMENTE TRAMITADO

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°0727 DE 2017 Y APRUEBA POLÍTICA DEVOLUCIÓN DE ACTIVOS VERSIÓN N°2, EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 0797

Santiago, 30 DIC 2019

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 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; en 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; en las Resoluciones Exentas N°s 674 y 723, ambas de 2019, de la Superintendencia de Educación; en el Oficio Gab. Pres. N° 008, de 23 de octubre de 2018, del Presidente de la República, por el cual imparte instrucciones en materia de ciberseguridad y Oficio Gab. Pres. N°001 de 2019, de Presidencia, que proporciona lineamientos para la transformación digital de la Administración del Estado, y en las Resoluciones N°s 6 y 7, 2019, 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, con fecha 23 de octubre de 2018, el Presidente de la Republica dicta el Instructivo Presidencial N°008 que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

3. Que, con fecha 20 de octubre de 2017, se dicta Resolución Exenta N° 0727, que aprueba versión 1.0 de la política de devolución de activos de la Superintendencia de Educación.

4. Que, mediante Resolución Exenta N° 0698, de fecha 10 de diciembre de 2019 se nombró al Comité de Seguridad de la Información Institucional, para que, en función del marco legal y tecnológico, proponga a este Jefe de Servicio, un Sistema de Seguridad de la Información y Ciberseguridad lo mantenga y mejore en el tiempo.

5. Que, debido a una serie de cambios institucionales y a la revisión efectuada por la Encargado/a de Seguridad de la Información y Ciberseguridad, se ha estimado procedente reestructurar, ajustar y actualizar el contenido del procedimiento revisión de los requisitos de legislación.

RESUELVO:

1. **DÉJASE,** sin efecto, a contar de la total tramitación del presente acto administrativo la Resolución Exenta N° 0727, de 2017 de la Superintendencia de Educación.

2. **APRUÉBASE,** la versión N°2 de la Política de devolución de activos de información en la Superintendencia de Educación, cuyo texto es el siguiente:

Política devolución de activos de información

Tabla de Contenidos

ELABORADO POR	REVISADO POR	APROBADO POR
Daniela Llano Recabal **Encargada de Seguridad de la Información y Ciberseguridad**	**Angie Aracena Medina** **Comité Operativo Seguridad de la Información**	**José Manuel Astorga** **Comité Directivo Seguridad de la Información (s)**

1. Objetivo

En el marco del Sistema de Gestión de Seguridad de la Información se deben definir las directrices y requisitos para la devolución de activos organizacionales, tanto físicos y electrónicos, previamente entregados a los funcionarios que trabajan o presten servicios en la Superintendencia de Educación, cuando estos finalizan su empleo, contrato o acuerdo con la institución.

2. Alcance

Esta política se aplica a todas las áreas de SUPEREDUC y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 1de Definiciones Estratégicas. Como también a todos los usuarios de la SUPEREDUC, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presente servicios a la SUPEREDC, que en virtud de las responsabilidades que establece su cargo o funciones, la institución le ha hecho entrega de activos tanto físicos y electrónicos para el desarrollo adecuado de sus funciones.

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

- A.08.01.04 Devolución de activos.

3. Referencias normativas

- Política General de Seguridad de la Información de la Superintendencia de Educación vigente.
- Ley N° 19.880, Establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del estado, Ministerio Secretaria General de la Presidencia.
- Política eliminación o reutilización segura de equipos de la Superintendencia de Educación vigente.
- Política de uso de medios removibles y dispositivos móviles de la Superintendencia de Educación vigente.
- Procedimiento de creación, modificación, eliminación de cuentas e información y egreso de personas vigente de la Superintendencia de Educación vigente
- Política de respaldo de la Superintendencia de Educación vigente.

4. Definiciones

Concepto	Descripción
Estaciones de trabajo y otros equipos	Conjunto de elementos tecnológicos de hardware y software que lo componen. - **A nivel de Hardware:** incluyen pantalla, teclado, mouse, parlantes, unidad central (CPU), disquetera, unidad de CD (externa o interna), impresoras, proyector, tv, scanner, teléfonos (IP y móvil), fax, Banda ancha móvil, notebooks, docking, candados y cables. - **A nivel de Software:** incluyen todos los programas, sistemas de información o aplicaciones, sistemas operativos y rutinas de comunicación o de uso general.
Activo de Información	Recursos del sistema de información, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Una organización incluye diferentes tipos de activos: - Activos relacionados con el entorno (edificios, instalaciones, equipamientos) y personal. - Activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones). - Activos relacionados con la información (datos, metadatos y soportes). - Activos relacionados con las funcionalidades de la organización (productos, servicios). Activos intangibles (credibilidad, conocimiento acumulado).

Concepto	Descripción
Derecho de acceso	Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recurso.
Restringir el acceso	Delimitar el acceso de los funcionarios/as, servidores públicos a honorarios y terceras partes a determinados recursos.
Sistema Informático	Uno o más computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
Usuario	Persona que utiliza un sistema informático y recibe un servicio, tales como: correo electrónico o red de conectividad proporcionado o administrado por la SUPEREDUC, ya sea que lo utilice en virtud de un empleo, de una función o de cualquier prestación de servicio, sin importar la naturaleza jurídica de ésta o del estatuto que lo rija.
Directorio Activo	Active Directory (AD) o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos

5. Roles y Responsabilidades

Rol	Responsabilidades
Mesa de Servicio	
Unidad Gestión de Personas	a) Con la anticipación debida y mediante solicitud proveer a la Mesa de Servicios TI los antecedentes de ingresos, egresos, cambio de funciones o traslado de funcionarios planta, contrata u honorarios que presten servicios a la Superintendencia de Educación aportando todos los antecedentes requeridos para facilitar el cumplimiento de esta política.
Departamento de Tecnologías y Procesos	a) Velar por el cumplimiento de la política, estándares y procedimientos establecidos para la gestión del hardware y accesos en la SUPEREDUC. b) Registrar, clasificar y dar respuesta a los requerimientos reportados por la alta y baja de los activos electrónicos de la SUPEREDUC. c) Elaborar y mantener el catastro del Hardware en la SUPEREDUC. d) Supervisar y administrar los accesos a los recursos informáticos de la SUPEREDUC. e) Mantener un registro de los accesos otorgados a los usuarios de la SUPEREDUC. f) Gestionar y administrar la información de autenticación de usuarios de la SUPEREDUC. g) Propone, define e implementa las medidas de seguridad a implementar, para resguardar las cuentas de usuarios y sus respectivas contraseñas. h) Punto de contacto para orientar, asesorar, actualizar y restaurar problemas relacionados con las contraseñas de los usuario de la Superintendencia.
Usuarios	a) Administrar la información contenida en su computador de la SUPEREDUC, cumpliendo con las definiciones establecidas en esta política. b) Utilizar de manera permanente y proteger los medios de seguridad física, provistos por el Departamento de Tecnologías y Procesos de Información para el uso de los dispositivos móviles (ejemplo: candados de seguridad). c) Reportar cualquier falla o deterioro del equipo o componente, a través de los canales formalmente establecidos.
Jefaturas de la SUPEREDUC	a) Validar y aprobar los accesos a los sistemas de información a su cargo, cuidando de mantener una adecuada segregación de funciones. b) Informar el ingreso o baja de un usuario que sea contratado por la Superintendencia de Educación. c) Las jefaturas de las Divisiones, Intendencia, Direcciones Regionales, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política, así como las políticas específicas, manuales y procedimientos asociados al SGSI
Encargado/a de Seguridad de la información y Ciberseguridad	d) Velar por la difusión y cumplimiento de esta política. e) Monitorear el correcto funcionamiento y operación respecto la entrega y utilización de contraseñas, entrega y baja de activos, así como evaluar circunstancias particulares al uso de estas y en caso de ser identificarse eventos

	de seguridad, activar el protocolo de incidentes de seguridad de la información vigente en la SUPEREDUC. f) Velar por la correcta aplicación de la política y apoyar en las unidades técnicas responsable de la administración y gestión de usuarios y contraseñas. g) Actualizar la política, con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.

6. Directrices

6.1. Asignación de activos a nuevos usuarios:

La Jefatura de la Unidad, Departamento o División es responsable de solicitar los accesos básicos para los nuevos funcionarios mediante el "Formulario de solicitud de creación/eliminación de accesos" (Ver Anexo N°1) vigente, el cual debe venir firmado y entregado al Departamento de Tecnología y Procesos mediante la Mesa de Servicio.

El área de Operaciones del Departamento de Tecnologías y Procesos es responsable de la creación de los accesos básicos de ingreso que incluye:

- Creación de cuenta de correo electrónico.
- Creación de usuario en Active Directory.
- Habilitación de estación de trabajo (computador, notebook, mouse, entre otros).
- Entrega de dispositivos móviles (celular, banda ancha móvil, entre otros).

El área de gestión y desarrollo de personas es responsable de habilitar los accesos físicos en el nivel central de la subsecretaría de educación, con la entrega de tarjetas de identificación para accesos a las dependencias.

Las contraseñas de acceso facilitadas al usuario son temporales de ingreso, el usuario debe modificar dicha clave y se realizarán de acuerdo con el "Procedimiento de creación, modificación, eliminación de cuentas e información de egreso de personas" vigente en la Superintendencia de Educación. Además, se informará al nuevo usuario sus responsabilidades implicadas en el uso de los sistemas informáticos y los activos de información de la SUPEREDUC (correo electrónico, CRM, bases de datos, entre otros). Las condiciones de uso incluyen:

- Mantener confidenciales las contraseñas de acceso a los sistemas informáticos y a la red de la SUEPREDUC.
- Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Seguridad de la Información, vigentes en la SUPEREDUC y en todo lo que sea de su competencia.
- No divulgar ningún tipo de información perteneciente a SUPEREDUC.
- Comprender la responsabilidad funcionara, aun fuera de las dependencias de trabajo y fuera de horario normal de trabajo.

6.2. Registro de usuarios en los sistemas de información de la SUPEREDUC.

La Jefatura de la Unidad, Departamento o División es responsable de solicitar los accesos básicos para los nuevos funcionarios mediante el "Formulario de solicitud de creación/eliminación de accesos" (Ver Anexo N°1) firmado y entregado al Departamento de Tecnología y Procesos mediante la Mesa de Servicio

El Departamento de Tecnología y Procesos es responsable de chequear que el nivel de acceso solicitado es apropiado para el propósito institucional y que sea consistente con las Políticas de Seguridad de la Información vigente en la Superintendencia de Educación.

6.3. Revisión de los derechos de acceso del usuario.

La administración de los perfiles de usuario radica en los Usuarios líderes de los sistemas de información y las Jefaturas de División correspondientes. Para administrar los accesos a los sistemas de información de la Superintendencia de Educación se definirán perfiles de acceso asignables a grupos de usuarios que, por su responsabilidad en la organización, presenten necesidades de acceso equivalentes.

El Encargado de Seguridad de la Información y Ciberseguridad es responsable de que se efectúe la revisión de los derechos de accesos por el Departamento de Tecnología y Procesos, de acuerdo a los siguientes lineamientos:

- Se debe revisar los derechos de acceso de los usuarios cada 6 meses.
- Las autorizaciones para derechos de acceso con privilegios especiales se deben revisar a intervalos de 3 meses.
- Se debe chequear la asignación de privilegios para asegurar que no se hayan obtenidos privilegios no autorizados.
- Chequeo de IDs de usuarios y cuentas redundantes.
- Los accesos de cuentas con mayores privilegios, deben ser revisados al menos 2 veces al año.

Los Usuarios Lideres de los sistemas, deben revisar en forma periódica los perfiles de usuarios del personal vigente y solicitar al Departamento de Tecnologías y Procesos, la actualización de estos cada vez que ocurra un cambio en la definición de funciones. Principalmente solicitar los cambios de acceso cuando existe algún cambio como; ascenso, remoción o terminación del contrato del funcionario

6.4. Devolución de activos en la finalización laboral.

Todo funcionario/a es responsable de devolver todos los activos pertenecientes a SUPEREDUC que estén en su poder, en mismas condiciones que fueron asignados, como consecuencia de la finalización de su relación laboral, contrato o acuerdo con la Superintendencia de Educación.
Si un funcionario/a posee conocimiento que es importante para las operaciones en curso, es su responsabilidad documentar dicha información y transferirla a su Unidad o Departamento dependiente.

6.5. Recuperación de activos y revocación de derechos de acceso

La Jefatura o el Coordinar Administrativo del área involucrada es responsable de informar cualquier desvinculación de funcionarios mediante el "Formulario de solicitud para creación/eliminación de accesos" (Ver Anexo N°1) esta notificación debe ser enviada simultáneamente a:

- Departamento Gestión de Personas.
- Departamento de Administración.
- Departamento de Tecnologías de Información.

Ante el informe de desvinculación de algún funcionario/a, el Departamento de Administración es responsable de gestionar la recuperación de los activos asignados al funcionario/a. entre otros, se encuentran:

- Documentos corporativos.
- Equipamiento.
- Teléfonos Móviles.
- Tarjetas de acceso.

Los activos recuperados deben ser registrados en el Sistema de Inventario.

El Departamento de Tecnología y Procesos, es responsable de eliminar los derechos de acceso a los sistemas de información de la Superintendencia de Educación, recuperar el/los equipos informáticos asignados al funcionario, junto con los activos de información asignados al funcionario, entre otros se encuentran:

- Software.
- Licencias.
- Manuales.
- Cuentas VPN.
- Cualquier información almacenada en medios electrónicos.

Una vez que es recuperado el activo tecnológico, se realiza un respaldo del perfil completo del usuario según "procedimiento de respaldo usuarios y servidores" vigente. Dado que posteriormente se realizado un borrado seguro de toda la información existente en el equipo mediante el "procedimiento de creación, modificación, eliminación de cuentas e información de egreso de personas" vigente en la SUPEREDUC.

En el caso que el usuario haya tenido cuentas de acceso a sistemas externos a la Superintendencia de Educación, tales como SIAPER (Contraloría General de la Republica), SIGFE (Dirección de Presupuesto), Mercado Publico, entre otros. La Jefatura o el Coordinar Administrativo del área involucrada, según corresponda, debe encargarse que sean eliminadas.

En el caso que se genere una baja funcionaria y no se entrega la totalidad del equipamiento asignado, o esté presente un siniestro atribuible a mal uso, se deberá solicitar que se instruya una investigación sumaria para definir posibles responsabilidades administrativas, lo que posteriormente podrían derivar en una eventual sanción.

El Jefe/a del Departamento de Tecnología y Procesos en los casos de usuarios administradores de plataformas de la SUPEREDUC, deberá deshabilitar el acceso al usuario y las contraseñas que utilizaba en función de su trabajo, beben ser reemplazadas por una nueva. Así como también revocar el acceso físico a las dependencias de equipamiento crítico, por ejemplo: acceso al Data Center.

Ninguna cuenta de acceso a los sistemas informáticos asignada al usuario, que abandone la institución se mantendrá activa. Al momento del cese de funciones se desactivará la cuenta y todos sus accesos.

7. Evaluación y Difusión

La presente política será evaluada por el Superintendente de Educación una vez al año, o bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.

Una vez que el documento entre en vigencia e/la Encargado/a de Seguridad de la Información y Ciberseguridad deberá difundir al personal y externos considerado en el alcance, mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrían ser página web institucional, intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

8. Revisión

Con una periodicidad concordante a la de la evaluación definida en el punto anterior, y a través de auditorías, ya sean internas o externas, y en tanto los recursos institucionales se encuentren disponibles para ello, se revisará el cumplimiento de la presente política con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento de la misma.

9. Aceptación

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, manuales y procedimientos vigentes de seguridad de la información y ciberseguridad 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.

10. Sanciones

El incumplimiento o violación a esta Política, de las Políticas específicas del Sistema, Procedimientos u otros documentos que se deriven de éstos, 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. Excepciones

La presente Política, y las Políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el/la Encargado/a de Seguridad de la Información y Ciberseguridad y debidamente autorizados por la Jefatura de Gabinete.

12. Revisiones de la política

REVISIONES DE LA POLITICA			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
1.0	Octubre 2017	Versión inicial	Versión inicial
2.0	Diciembre 2019	Actualización Política	Todas las Páginas.

13. Anexo N°1: Formulario de solicitud para creación/eliminación de accesos.

	FORMULARIO: **SOLICITUD PARA CREACIÓN/ELIMINACIÓN DE ACCESOS** **DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN** **DIVISIÓN DE ADMINISTRACIÓN GENERAL**	**FRM-CEA**
	Versión: 1.0	Fecha:

FORMULARIO DE SOLICITUD PARA CREACIÓN/ELIMINACIÓN DE ACCESOS

1. TIPO DE SOLICITUD

CREACIÓN DE USUARIO		FECHA DE SOLICITUD	
ACCESO A SISTEMA			
ELIMINACIÓN DE ACCESO			

2. JEFATURA QUE SOLICITA

NOMBRE COMPLETO	
UNIDAD, DEPARTAMENTO, DIVISIÓN	
EMAIL	
FONO-ANEXO	

3. IDENTIFICACIÓN DEL FUNCIONARIO

NOMBRE COMPLETO	
RUT	
CARGO	
UNIDAD, DEPARTAMENTO, DIVISIÓN	
CALIDAD JURIDICA	
FECHA DE INGRESO A LA INSTITUCION	

4. SISTEMA(S) A LOS QUE SE SOLICITA ACCESO/ELIMINACION

1	
2	
3	
4	
5	

FIRMA DE JEFATURA QUE SOLICITA

**Ingresar solo 1 funcionario por solicitud*

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

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

5. **REMÍTASE,** copia de la presente Resolución Exenta todas las Divisiones, Intendencia, Direcciones Regionales, Departamentos, Unidades y de la Superintendencia de Educación, de acuerdo con la distribución indicada en la presente resolución.

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

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

CRISTIÁN O'RYAN SQUELLA
SUPERINTENDENTE DE EDUCACIÓN

Distribución:

- Gabinete Superintendente.
- Jefes/as de División.
- Intendente/a de Educación Parvularia.
- Directores Regionales I a XVI región.
- Jefe/a Departamento de Finanzas.
- Jefe/a Departamento Gestión y Desarrollo de Personas.
- Jefe/a Departamento de Administración.
- Jefe/a Departamento de Tecnologías y Procesos.
- Departamento de Gestión Institucional.
- Departamento de Auditoria.
- Unidad de Transparencia.
- Encargada de Seguridad de la Información y Ciberseguridad.
- Oficina de Partes.