

**RESOLUCIÓN EXENTA N°
VALLENAR,**

VISTOS:

1. Lo dispuesto en la Ley N° 21.040, que crea el Sistema de Educación Pública; en la Ley N°19.553, el Artículo 7° que Concede Asignación de Modernización y Otros que Indica; en la Ley N°19.882, que regula nueva política de personal a los funcionarios públicos que indica; en la Ley N°19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; la Ley N°18.575, orgánica constitucional de bases generales de la Administración del Estado; la Resolución N°2 de fecha 10 de junio de 2024 que exime de toma de razón y somete a registro los actos administrativos que se indican; Que, la resolución Exenta N°8317 del Ministerio de Educación de fecha 30-06-2025, que aprueba el convenio de desempeño de gestión educacional del director ejecutivo del servicio local de educación pública de Huasco"; Resolución 36 que fija normas sobre exención del trámite de toma de razón contraloría general de la república; en el Decreto Supremo N°56 de 21-04-2025, del Ministerio de Educación, que designa al Director Ejecutivo del Servicio Local de Educación Pública de Huasco; en el Decreto Exento N°1737, de 18 de diciembre de 2019, del MINEDUC, que modifica el Decreto N°970, y establece el nuevo orden de subrogación para el Servicio Local de Educación Pública de Huasco (Planificación y Control de Gestión, Apoyo Técnico Pedagógico y Administración y Finanzas), el Decreto Supremo N° 83 del Ministerio Secretaría General de la Presidencia de 2005 que Aprueba Norma Técnica para los Organismo de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; la Política Nacional de Ciberseguridad de junio de 2023; El Decreto Supremo N° 1 del 2015 del ministerio Secretaría General de la Presidencia que aprueba norma técnica sobre sistemas y sitios web de los órganos de la Administración del Estado, La Ley Marco de Ciberseguridad N° 21.663, y;

CONSIDERANDO:

2. Que, la Ley N°21.040, que crea el Nuevo Sistema de Educación; crea a su vez los Servicios Locales de Educación, que le asigna y otorga potestades y facultades a su Director Ejecutivo, consagradas en el art. 22 de la citada ley y demás normas legales; Las funciones y atribuciones que posee el Servicio Local de Educación Pública; específicamente lo dispuesto en el art. 18 letra b) que le permite "Administrar los recursos humanos, financieros y materiales del servicio y los establecimientos educacionales de su dependencia, para lo cual podrá adquirir toda clase de bienes muebles e inmuebles para el cumplimiento de sus fines", y letra O) de la ley 21.040, que permite "celebrar convenios o acuerdos con organismos públicos o privados para abordar asuntos de interés común".

3. Que, la Ley N°21.040, que crea el Nuevo Sistema de Educación; Artículo 18.- Funciones y atribuciones. Los Servicios Locales tendrán las siguientes funciones y atribuciones, las cuales se entienden sin perjuicio de aquellas que corresponden a los sostenedores de establecimientos educacionales:

b) Administrar los recursos humanos, financieros y materiales del servicio y los establecimientos educacionales de su dependencia, para lo cual podrá adquirir toda clase de bienes muebles e inmuebles para el cumplimiento de sus fines.

m) Elaborar y proponer a la Dirección de Educación Pública, u otros organismos públicos a través de ella, proyectos de inversión en equipamiento e infraestructura educacional u otros



ítems relacionados con su objeto y fines para desarrollar en el territorio de su competencia, de conformidad a la ley.

t) Ejercer las demás funciones y atribuciones que establezcan las leyes.

4. Que, la Ley N°21.040, que crea el Nuevo Sistema de Educación; Artículo 19.- 8. Velar por la existencia y mantención de una adecuada infraestructura y equipamiento educativo, en el marco de la normativa vigente.

11. Coordinar y organizar la ejecución de las políticas, planes, programas o prestaciones realizadas por otros órganos de la Administración del Estado respecto del establecimiento educacional de su dependencia o sus estudiantes, sin perjuicio de las competencias específicas de dichos órganos.

5. Que, la resolución Exenta N°8317 del Ministerio de Educación de fecha 30-06-2025, que aprueba el convenio de desempeño de gestión educacional del director ejecutivo del servicio local de educación pública de Huasco”

6. Que, por medio del Decreto Supremo N° 83 del Ministerio Secretaría General de la Presidencia con fecha 12 de enero del 2005, Aprueba Norma Técnica para los Organismo de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

7. Que, por medio del Decreto Supremo N° 1 del 2015 del ministerio Secretaría General de la Presidencia, Aprueba norma técnica sobre sistemas y sitios web de los órganos de la Administración del Estado.

8. Que, por medio de la Política Nacional de Ciberseguridad de junio de 2023.

9. Que, por medio de la Política General de Seguridad de la Información y Ciberseguridad aprobada por resolución exenta número 1010 del año 2024.

RESUELVO:

1. APRUÉBESE, la “Política Específica de Respaldo de Información Digital”, cuyo contenido es el siguiente:



Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.

Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:

<https://doc.digital.gob.cl/validador/EJELDE-780>



POLÍTICA ESPECÍFICA DE RESPALDO DE INFORMACIÓN DIGITAL



Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.

Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:

<https://doc.digital.gob.cl/validador/EJELDE-780>

Control De Modificaciones				
Número de modificaciones	Número de pagina	Número de sección	Fecha de modificación	Responsable

	Nombre	Cargo	Firma
Realizado	Hugo Cruz Guerrero	Profesional de Seguridad de la Información	
Revisado	Luis Milla Yáñez	Jefe del Departamento Jurídico (s)	
Aprobado	Javier Obanos Sandoval	Director Ejecutivo	



Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.

Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:

<https://doc.digital.gob.cl/validador/EJELDE-780>

Introducción

La Resiliencia Digital del Servicio Público en un Mundo Interconectado

En la era de la transformación digital, la información se ha convertido en un pilar fundamental para la operación de cualquier institución. Para el Servicio Local de Educación Pública de Huasco, desde ahora SLEPH, la información es un activo crucial para la gestión administrativa, financiera y de recursos humanos, pues permite entregar el soporte multidisciplinario que necesitan los más de 60 establecimientos educacionales del territorio. Este entorno digital interconectado que facilita la innovación y la eficiencia también presenta riesgos significativos debido al aumento exponencial de las amenazas, que van desde pérdida de información hasta filtraciones de datos masivas. Estos incidentes pueden comprometer la triada de la información; confidencialidad, integridad y disponibilidad y lo que es más importante, pueden paralizar operaciones y afectar la calidad del servicio que entregamos a la comunidad.

En este contexto global, Chile no es una excepción. Si bien nuestro país ha experimentado un avance en la digitalización de sus servicios, esta dependencia tecnológica nos hace igualmente vulnerables. Hemos sido testigos de incidentes de ciberseguridad que han afectado a instituciones públicas y privadas, lo que ha evidenciado la necesidad imperante de fortalecer nuestra infraestructura de protección de datos. En el ámbito público, una robusta política de respaldo de información no es solo una buena práctica de gestión, sino una responsabilidad fundamental para garantizar la continuidad del servicio y la confianza de nuestra comunidad.

El marco legal y regulatorio chileno está evolucionando para hacer frente a estos desafíos. La promulgación de la Ley Marco de Ciberseguridad establece un conjunto de principios y obligaciones para proteger la infraestructura crítica y los datos personales, obligando a las organizaciones a adoptar medidas de seguridad adecuadas. Esta normativa, subraya la obligación legal de las instituciones de resguardar la información sensible y demuestra que la ciberseguridad ha pasado de ser una consideración técnica a una exigencia de gobernanza pública.

En respuesta a este panorama, la presente Política de Respaldo de Información Digital se establece como un pilar fundamental de nuestra estrategia de ciberseguridad y resiliencia organizacional integrando el conjunto de políticas específicas, las cuales estarán al alero de la Política general de Seguridad de la Información y Ciberseguridad.



El objetivo de esta política, aplicada a la administración central del SLEPH, es garantizar la confidencialidad, integridad y disponibilidad de la información ante cualquier incidente de seguridad, ya sea un ataque cibernético, una falla técnica, un desastre natural o un error humano. Al implementar esta política, el SLEPH se compromete a asegurar la continuidad de nuestras operaciones, a cumplir con nuestras obligaciones legales y regulatorias, y a proteger el valor incalculable de nuestra información, sentando las bases para una operación segura y confiable en el presente y en el futuro.



Contenido

1. DEFINICIONES ESTRATÉGICAS INSTITUCIONALES	8
1.1. Declaración	8
1.2. Objetivo general.....	8
1.3. Objetivos específicos.....	9
1.4. Alcance.....	9
1.5. Marco referencial.....	9
1.6. Vigencia y actualización	10
1.7. Difusión	10
2. DEFINICIONES.....	10
3. PRINCIPIOS Y RESPONSABILIDADES	11
3.1. Principios	11
3.2. Responsabilidades	12
4. ESTRATEGIA DE RESPALDO	13
5. PROCESO DE RESTAURACIÓN	13
6. DIFUSIÓN	14
6.1. Obligación de conocimiento y cumplimiento.	14
6.2. Publicidad y fomento de su cumplimiento.	14
7. SANCIONES.....	15





1. DEFINICIONES ESTRATÉGICAS INSTITUCIONALES

El Servicio Local de Educación Pública de Huasco, presenta en este documento los alcances, responsabilidades y funciones operacionales para la protección ante pérdida del acceso a los activos de información a fin de garantizar la continuidad operacional y la seguridad de éstos.

Un activo de información en el contexto de la norma internacional ISO/IEC 27001 es: “algo que una empresa valora y por lo tanto debe proteger”.

La resiliencia, en el ámbito de la ciberseguridad, se refiere a la capacidad de una organización para anticipar, resistir, recuperarse y adaptarse a incidentes cibernéticos, manteniendo la continuidad del servicio y protegiendo la integridad y confidencialidad de la información. En esencia, es la habilidad para minimizar el impacto de los ataques y asegurar que las operaciones puedan continuar, incluso frente a la adversidad. Es en función de esta definición que el SLEPH se hace cargo con este documento a fin de garantizar resiliencia ante un incidente de ciberseguridad.

1.1. Declaración

El Servicio se compromete a todo nivel, a implementar medidas de seguridad para proteger los activos de información del impacto de incidentes que afecten la confidencialidad, integridad y/o disponibilidad de éstos. Los resultados de la aplicación de las medidas de seguridad serán evaluados bajo la perspectiva de la mejora continua, asegurando el cumplimiento de los requisitos legales y aplicando una estrategia de seguridad basada en las mejores prácticas y control sobre los activos de información.

El SLEPH se compromete a disponer para todos los equipos de trabajo que forman parte de éste de las herramientas y soporte necesarios para la protección de la información a través de su respaldo periódico definido por procedimiento(s) formalizado(s).

El SLEPH se compromete a colaborar con el ecosistema digital en materia de ciberseguridad, tanto en sus aspectos técnicos como jurídicos.

El SLEPH se compromete a establecer e incorporar en su diario quehacer los requisitos para el respaldo periódico de la información y así asegurar su continuidad operacional y de la administración de la seguridad de la información ante situaciones adversas.

1.2. Objetivo general

Asegurar la continuidad operacional y minimizar la pérdida de datos ante cualquier incidente, falla tecnológica, desastre natural, error humano o ataque cibernético. Para ello, esta política establece las directrices y responsabilidades para el respaldo, restauración y protección de la información del Servicio Local de Educación Pública de Huasco.



1.3. Objetivos específicos

- a. Garantizar que los sistemas y datos de la administración central del SLEPH puedan ser restaurados en un plazo razonable tras un incidente, minimizando el impacto en las operaciones y en la calidad del servicio entregado.
- b. Resguardar toda la información, asegurando que no se pierda o sea comprometida.
- c. Cumplir con el marco legal, mantener la política y los procedimientos de respaldo alineados con las obligaciones de la Ley Marco de Ciberseguridad (Ley N° 21.643) y la NCh ISO 27001:2013
- d. Verificar la viabilidad y la integridad de los respaldos de datos, asegurando que puedan ser restaurados correctamente cuando sea necesario.
- e. Asignar los roles y las responsabilidades para la ejecución, monitoreo y gestión de los respaldos, promoviendo una cultura de seguridad de la información entre funcionarios(as).
- f. Crear y documentar procedimiento(s) claro(s) para la restauración de datos, permitiendo una respuesta rápida y eficaz ante cualquier incidente.

1.4. Alcance

Esta política aplica a toda la información digital almacenada en los equipos computacionales institucionales, independientemente de su ubicación física. Incluye, pero no se limita a, documentos administrativos, financieros, académicos, datos personales de estudiantes y funcionarios y bases de datos.

Esta política rige independientemente del lugar en que el personal realiza sus tareas e indistintamente de la modalidad de trabajo ya sea presencial, a distancia, teletrabajo u otra, en las condiciones que establezca la legislación vigente.

1.5. Marco referencial

Los contenidos y controles esenciales de carácter legal que se consideraran en la política son:

- a) Política General de Seguridad de la Información y Ciberseguridad del Servicio Local de Educación Pública de Huasco.
- b) Ley N° 21.663, Ley Marco de Ciberseguridad.
- c) NCh-ISO 27001/27002 - Tecnología de la Información – Código de prácticas para la gestión de seguridad de la información - INN Chile.
- d) Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- e) Ley N°19.628: sobre Protección de la vida privada.



f) Ley N° 19.223: sobre Delitos informáticos.

1.6. Vigencia y actualización

La Política se considera vigente desde la fecha de su aprobación por parte del director ejecutivo del SLEPH, documento que será revisado y/o actualizado anualmente o cuando se determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente en el SLEPH.

La Política deberá ser revisada permanentemente y se generarán las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del conjunto de controles de seguridad.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

- Cambios en el marco normativo nacional que afecte al SLEPH.
- Incorporación o modificaciones relevantes de procesos o actividades críticas del SLEPH.
- Cambios significativos al soporte tecnológico.
- Modificaciones en la estructura de la organización.
- Cambios significativos en los niveles de riesgo a que se expone la información.
- Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a esta política deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

1.7. Difusión

El mecanismo de difusión de la Política será a través de correos electrónicos masivos o cualquier otro medio que se estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

2. DEFINICIONES

Para los propósitos de esta política, se entenderá por:

Activos de la información: todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución, cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten. Por ejemplo: dispositivos móviles, software, equipamiento computacional, infraestructura tecnológica y física.

Confidencialidad: la información debe estar protegida de accesos no autorizados. Por lo tanto, se debe asegurar que la información es accedida únicamente por las personas autorizadas.

Disponibilidad: certeza del acceso a la información cuando es requerida por los usuarios autorizados.



Respaldo: copia de seguridad de la información almacenada en un medio diferente al original, con el propósito de poder restaurarla en caso de pérdida o corrupción de los datos originales.

Restauración: proceso de restaurar la información desde un respaldo a su estado original o a un nuevo medio.

Incidente de Seguridad: cualquier evento o situación que comprometa la disponibilidad, integridad y confidencialidad de la información, o bien afecte a la infraestructura tecnológica, proceso y aplicativos que la contienen, impidiendo acceder a ésta en forma oportuna.

Integridad: la información debe estar completa, actualizada y ser veraz, sin modificaciones o alteraciones no autorizadas o corruptas.

Riesgo : es la contingencia de un daño a un activo de información. A su vez, contingencia significa que el daño puede materializarse en cualquier momento o no suceder nunca.

Seguridad de la Información: proceso encargado de asegurar y proteger los recursos de un sistema de información para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.

Trabajo a distancia: aquel en el que el trabajador o funcionario presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos o instalaciones del servicio.

Usuario: persona que utiliza el sistema informático o los medios del servicio con independencia de su calidad contractual y la modalidad de trabajo (presencial, teletrabajo o trabajo a distancia).

3. PRINCIPIOS Y RESPONSABILIDADES

3.1. Principios

- a) **Totalidad de la Información:** la información debe ser respaldada sin excepción.
- b) **Automatización:** se priorizarán los sistemas de respaldo automatizados para reducir el error humano y asegurar la regularidad.
- c) **Integridad y Confidencialidad:** los respaldos deben garantizar la integridad de los datos (no alterados) y su confidencialidad (acceso solo a personal autorizado).
- d) **Verificación Regular:** los respaldos deben ser verificados periódicamente para asegurar su viabilidad y la capacidad de restauración.



- e) Pruebas de Recuperación: se realizarán pruebas regulares de restauración para validar la efectividad del proceso de respaldo.
- f) Almacenamiento Seguro: los respaldos deben almacenarse de forma segura, protegiéndolos contra accesos no autorizados, corrupción o desastres.

3.2. Responsabilidades

a) Dirección Ejecutiva:

- Revisar, aprobar y asegurar los recursos necesarios para la implementación y mantención de la política de respaldo de información.
- Promocionar objetivos, importancia y alcance de la política.

b) Profesional de Seguridad de la Información:

- Diseñar y supervisar la política y el o los procedimientos de respaldo.
- Coordinar las pruebas de restauración de datos.
- Asegurar la capacitación del personal en aspectos de respaldo de información según herramientas y técnicas utilizadas.
- Evaluar y recomendar tecnologías y prácticas de respaldo desde la perspectiva de seguridad.
- Velar por el cumplimiento de la política y los estándares de seguridad en los respaldos.

c) Encargado del Área de TI:

- Implementar y mantener la infraestructura tecnológica necesaria para los sistemas de respaldo.
- Gestionar, monitorear y optimizar los sistemas de respaldo en operación.
- Ejecutar los procedimientos de respaldo y restauración de datos según lo establecido.
- Proveer soporte técnico a los usuarios en relación con los sistemas de respaldo.
- Asegurar la disponibilidad y el correcto funcionamiento de las herramientas de respaldo.

d) Jefes(as) y Encargados(as) de Unidades o Áreas:

- Asegurar que su personal cumpla con los procedimientos de respaldo.
- Reportar incidentes que puedan afectar la información o los respaldos.

e) Funcionarios y funcionarias en su totalidad:

- Almacenar la información en las ubicaciones definidas para respaldo automático.
- Informar de inmediato cualquier anomalía o problema relacionado con la información o su respaldo.
- Cumplir con los procedimientos de respaldo establecidos.



4. ESTRATEGIA DE RESPALDO

El SLEP Huasco implementará una estrategia de respaldo que incluirá el uso de herramientas de sincronización y respaldo en la nube y/o herramientas de almacenamiento local para la información almacenada en los equipos institucionales.

Frecuencia: los respaldos mediante sincronización serán continuos o programados según la configuración de la herramienta utilizada para las carpetas designadas.

Tipos de Respaldo: se empleará la sincronización completa de carpetas designadas y otros métodos de respaldo según la criticidad de la información.

Ubicación de los Datos: es mandatorio que toda la información se almacene en las ubicaciones designadas para respaldo automático.

Cifrado y Seguridad: en el caso de herramientas de respaldo en la nube, los datos respaldados se beneficiarán del cifrado en tránsito y en reposo ofrecido por la solución de respaldo. Los funcionarios/as deben asegurar el uso de contraseñas robustas para sus cuentas y activar la autenticación de dos factores (2FA) cuando sea aplicable. El Área de TI y el Profesional de Seguridad de la Información velarán por la implementación de medidas de seguridad adicionales si fueran necesarias.

5. PROCESO DE RESTAURACIÓN

Para asegurar que los objetivos de disponibilidad y resiliencia de esta política se cumplan de manera efectiva, se establece la necesidad de un Procedimiento de Restauración de Datos separado y debidamente documentado.

Este procedimiento técnico detallará los pasos a seguir para restaurar la información a partir de los respaldos en caso de un incidente que comprometa los datos del Servicio Local de Educación Pública de Huasco. Su objetivo es garantizar una respuesta rápida y coordinada que permita la restauración de los sistemas y la continuidad de las operaciones del SLEPH en el menor tiempo posible.

El Procedimiento de Restauración debe abordar, como mínimo, los siguientes puntos:

- Identificación de la información a restaurar.
- Roles y responsabilidades: asignación clara de quién lidera y ejecuta la restauración.
- Pasos del proceso: guía detallada y secuencial para la restauración de la información.
- Verificación y validación: confirmar la integridad y funcionalidad de los datos restaurados.
- Documentación del incidente: requisitos para el registro del evento y las lecciones aprendidas.
- Determinación de la fuente del respaldo.



El profesional de seguridad de la información es el responsable de mantener este procedimiento actualizado y de asegurar que el personal técnico tenga el conocimiento y los recursos para ejecutarlo eficazmente. La efectividad de este procedimiento se validará a través de pruebas de restauración periódicas, cuyos resultados serán documentados y revisados.

6. DIFUSIÓN

6.1. Obligación de conocimiento y cumplimiento.

El personal o terceras partes que usen los recursos informáticos de almacenamiento de información del servicio, deberán conocer y dar cumplimiento a esta política.

6.2. Publicidad y fomento de su cumplimiento.

Se deberá mantener informado al personal a través de canales digitales u otros respecto de las normas de uso establecidas en el presente reglamento. A la vez se difundirá con la frecuencia que la dirección ejecutiva y/o el Comité de Seguridad de la Información determine o que los actores internos relacionados impulsen, a través de correo masivo invitando a conocerlas, cada vez que sean modificadas tanto esta política como otras relacionadas y las respectivas guías, procedimientos y protocolos atinentes, que hayan sido aprobadas, incorporando en lo posible estrategias comunicacionales que simplifiquen educativamente los contenidos para hacerlos fácilmente comprensibles, interpretables, asimilables y adoptables por todo el personal.

Asimismo, el Profesional de Seguridad de la Información favorecerá acciones destinadas a sensibilizar, entrenar, capacitar y educar a los usuarios para operar los servicios y sistemas informáticos en conformidad a dichas normas y políticas.

Se considera un aspecto clave para el éxito de esta política hacer llegar el conocimiento a los diferentes niveles jerárquicos, razón por la que el plan de capacitación y de difusión de estas materias debe contemplar las diferentes necesidades del público objetivo, adecuando los niveles de profundidad del material a entregar y seleccionando las tecnologías óptimas que permitan una entrega eficiente y eficaz de los conocimientos.



7. SANCIONES

El no cumplimiento de la Política de Respaldo de Información será sancionad en conformidad a las disposiciones administrativas internas. Lo anterior, sin perjuicio de la responsabilidad civil o penal que corresponda.

ANÓTESE PUBLÍQUESE Y COMUNÍQUESE

Distribución:

- Jefe Unidad de Planificación y Control de Gestión SLEP Huasco.
- Jefe Unidad de Administración y Finanzas SLEP Huasco.
- Jefe Unidad de Apoyo Técnico Pedagógico SLEP Huasco.
- Auditoría Interna SLEP Huasco.
- Encargado Área Jurídica SLEP Huasco.
- Secretaría Dirección SLEP Huasco.
- Oficina de Partes SLEP Huasco.
- Encargado Área de TI



Firmado por:
Javier Francisco Obanos Sandoval
Director Ejecutivo
Fecha: 07-10-2025 17:42 CLT
Servicio Local de Educación Pública
de Huasco

