



**SERVICIO LOCAL DE EDUCACIÓN PÚBLICA
HUASCO**

**APRUEBA MODIFICACIÓN A LA "POLÍTICA
DE SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD" DEL SERVICIO LOCAL
DE EDUCACIÓN PÚBLICA DE HUASCO**

**RESOLUCIÓN EXENTA Nº
VALLENAR,**

VISTOS: La ley Nº21.040/2017, que crea el Sistema de Educación Pública; el Decreto con Fuerza de Ley Nº1 de 07 Marzo del 2018 del Ministerio de Educación que fija la Planta de personal del Servicio Local de Educación Pública de la Provincia del Huasco que comprende las comunas de Alto del Carmen, Vallenar, Freirina y Huasco; Las potestades y facultades que posee el Director Ejecutivo, consagradas en el art. 22 de la citada ley y demás normas legales que sean pertinentes; el Decreto Nº379/2017, del Ministerio de Educación, la que fija la denominación, ámbito de competencia territorial, domicilio y calendario de instalación con las fechas en que iniciarán funciones los Servicios Locales de Educación Pública que indica; Art. 6º y 7º de la Constitución Política de la República; Decreto con fuerza de ley Nº1/19.653, que fija el texto refundido coordinado y sistematizado de la ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; ley Nº19.880, que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; D.F.L. No 1 de 1996 que fija texto refundido coordinado y sistematizado de la Ley 19.070 y las leyes que complementan y modifican; Decreto Nº453 del Ministerio de Educación del año 1991, que aprueba Reglamento de la ley Nº19.070, Estatuto de los Docentes de la Educación; ley de presupuesto para el sector público vigente; la Resolución Nº2 de fecha 10 de junio de 2024 que exime de toma de razón y somete a registro los actos administrativos que se indican; Resolución 36 que fija normas sobre exención del trámite de toma de razón contraloría general de la república; Decreto Supremo Nº146 del 22 de abril del 2019 DEL Ministerio De Educación, el que designa al Director Ejecutivo del Servicio Local de Educación Pública de Huasco; Decreto Exento Nº1737, de 18 de diciembre de 2019, del MINEDUC, que modifica el Decreto Nº970, 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); y:

CONSIDERANDO:

1. Que, la Ley Nº21.040, 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".

2. Que, la Ley Nº21.040, que crea el Nuevo Sistema de Educación; Artículo 19.- Responsabilidades del Servicio Local respecto de los establecimientos educacionales de su dependencia. Corresponderá especialmente a los Servicios Locales, respecto de los establecimientos educacionales de su dependencia, entre otros: 8. Velar por la existencia y mantención de una adecuada infraestructura y equipamiento educativo, en el marco de la normativa vigente.

3. Que, por medio del Decreto Supremo Nº 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.

4. Que, por medio del Decreto Supremo Nº 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.

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



6. Que, por tratarse de un servicio público de reciente creación y como medida de buena administración, resulta necesario establecer procedimientos claros y expeditos, estableciendo directrices a saber y los responsables de ejecutar cada una de las fases establecidas.

7. Que, en resolución exenta N°844 de fecha 13 de agosto de 2024, se designa como Encargado Titular de CIBERSEGURIDAD del Servicio Local de Educación Pública de Huasco a don HUGOCRUZ GUERRERO, cédula de identidad N°15.033.637 4 Profesional de Seguridad de la Información y como Encargado Suplente a don CRISTIAN CHAPARRO HUIRICAN, cédula de Identidad N°15.022.073-4, Profesional de Mantenimiento y Gestión de Proyectos de Infraestructura, contrata grado 14°.

8. Que, en resolución exenta n°1010 de fecha 23 de septiembre de 2024, se aprueba la Política de Seguridad de la Información y Ciberseguridad.

9. Que, en virtud de lo señalado precedentemente, y en uso de las facultades normativas y reglamentarias vigentes que se me otorgan.

RESUELVO:

1. **APRUÉBESE**, la modificación a la “**Política de Seguridad de la Información y Ciberseguridad**”, cuyo contenido es el siguiente:



**POLÍTICA DE SEGURIDAD
DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

Septiembre de 2024



Control De Modificaciones				
Número de modificaciones	Número de pagina	Número de sección	Fecha de modificación	Responsable
1	7	2.2.6	10-03-2025	Hugo Cruz Guerrero

	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	

Política de Seguridad de la Información y Ciberseguridad



Introducción

En el entorno actual, donde la digitalización y la conectividad son elementos clave para el funcionamiento de los servicios públicos y privados, la protección de la información y la ciberseguridad se han convertido en prioridades fundamentales. La información es uno de los activos más valiosos para cualquier entidad, y su integridad, confidencialidad y disponibilidad deben ser resguardadas frente a amenazas y riesgos en constante evolución.

Este documento establece la Política de Seguridad de la Información y Ciberseguridad, desde ahora Política, del Servicio Local de Educación Pública de Huasco, desde ahora Servicio, con el objetivo de proporcionar un marco claro y coherente para la gestión de la seguridad de la información en todos los niveles de la organización. La política está diseñada para proteger los activos de información, reducir los riesgos asociados con la ciberseguridad y garantizar el cumplimiento del marco normativo nacional, conformado, entre otras, por la ley N° 20.285, sobre acceso a la información pública; la ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; la ley N° 21.180, sobre transformación digital del Estado; decreto supremo N° 83 del 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos; etc.

La Política de Seguridad de la Información y Ciberseguridad aborda los principios y procedimientos que guiarán al Servicio Local de Educación Pública de Huasco en la protección de su información y sistemas contra accesos no autorizados, alteraciones y pérdidas. Este documento también establece las responsabilidades de funcionarios(as) y los aspectos que son parte del funcionamiento diario del Servicio que deben estar bajo controles de seguridad.

Es imperativo que todo el personal de la institución comprenda y cumpla con esta política para garantizar un entorno seguro y resiliente. La protección de la información es una responsabilidad compartida y, por lo tanto, requiere el compromiso y la colaboración de todos los colaboradores de la institución.

Política de Seguridad de la Información y Ciberseguridad



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/VEXN4O-313>

Contenido

1.	DEFINICIONES ESTRATÉGICAS INSTITUCIONALES.....	1
1.1.	Declaración.....	1
1.2.	Objetivo general.....	2
1.3.	Objetivos específicos.....	2
1.4.	Alcance	3
1.5.	Revisión Independiente de la Seguridad de la Información	3
1.6.	Marco referencial.....	3
1.7.	Vigencia y actualización.....	4
1.8.	Roles y responsabilidades	4
1.9.	Difusión.....	5
2.	PRINCIPIOS Y RESPONSABILIDADES TRANSVERSALES	5
2.1.	Principios generales	5
2.2.	Principios específicos.....	5
3.	DIFUSIÓN	8
3.1.	Obligación de conocimiento y cumplimiento.	8
3.2.	Incorporación de la norma a los actos administrativos y contratos.	8
3.3.	Publicidad y fomento de su cumplimiento.	8
4.	SANCIONES.....	9
5.	GLOSARIO DE TÉRMINOS.....	9

Política de Seguridad de la Información y Ciberseguridad



1. DEFINICIONES ESTRATÉGICAS INSTITUCIONALES

El Servicio presenta en este documento las características, responsabilidades y consideraciones operacionales mínimas obligatorias para la administración de los activos de información de interés a fin de garantizar la continuidad operacional y la seguridad de la información en lo que se refiere a su confidencialidad, integridad y disponibilidad.

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 gestión de activos de información es una tarea de gestión de la información que involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes del negocio.

1.1. Declaración

El Servicio se compromete a todo nivel, a implementar controles de seguridad para proteger los activos de información de los procesos que hacen posible su existencia, estableciendo una adecuada gestión del riesgo, aplicando y monitoreando controles para la mitigación del riesgo detectado para llevarlo a niveles compatibles con el riesgo residual tolerable o definido por la Dirección Ejecutiva. Los resultados de la aplicación de los controles 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 Servicio se compromete a disponer y utilizar adecuadamente plataformas electrónicas cumpliendo con estándares de seguridad, interoperabilidad, interconexión y ciberseguridad, así como las condiciones de accesibilidad, seguridad, funcionamiento, calidad, protección y conservación de los documentos, definidas en los estándares técnicos establecidos por los reguladores, la ley vigente y las propias definiciones estratégicas.

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



El Servicio se compromete a establecer e incorporar en su diario quehacer los requisitos para la seguridad de la información, la continuidad operacional del servicio y la continuidad de la administración de la seguridad de la información ante situaciones adversas, es decir, durante una crisis, desastre o Estado de Excepción Constitucional.

1.2. Objetivo general

Establecer las directrices generales en materia de seguridad de la información y ciberseguridad para administrar, mantener, sensibilizar, monitorear y revisar la gestión de la seguridad de la información acorde a las Definiciones Estratégicas, la misión/visión y objetivos estratégicos, asegurando la confidencialidad, integridad y disponibilidad de los activos de la información a través de su adecuada implementación, asignación de roles, funciones y responsabilidades.

1.3. Objetivos específicos

- a. Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información.
- b. Establecer los niveles de acceso apropiados a la información, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario(a).
- c. Apoyar la gestión de continuidad del servicio.
- d. Definir el ámbito de trabajo y responsabilidades corporativas e individuales respecto al uso de los recursos tecnológicos que provee la empresa y al manejo de la información.
- e. Implementar medidas en todos los niveles de operación que permitan generar conciencia en funcionarios(as), respecto del rol y responsabilidad de cada uno(a) en la gestión de la información del Servicio.



1.4. Alcance

La Política se aplica a todos los funcionarios, funcionarias y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información del Servicio. También se aplica a cualquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en que el personal presta sus servicios a la empresa, total o parcialmente, 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. Revisión Independiente de la Seguridad de la Información

Se podrá solicitar a un área interna u organismo auditor externo, la realización de auditorías o revisiones independientes sobre el cumplimiento de la Política, las políticas específicas, los procedimientos establecidos para operativizar las políticas y en general el funcionamiento y operación de los controles de seguridad de la información.

1.6. Marco referencial

Los contenidos y controles esenciales de carácter legal que se consideraran en las políticas del Servicio son:

- Ley N° 21.663, Ley Marco de Ciberseguridad.
- NCh-ISO 27001/27002 - Tecnología de la Información - Código de prácticas para la gestión de seguridad de la información - INN Chile.
- Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley N° 19.628: sobre Protección de la vida privada.
- Ley N° 19.223: sobre Delitos informáticos.
- Ley N° 17.336: sobre Propiedad Intelectual.



1.7. Vigencia y actualización

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

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 las leyes o reglamentos que afecten al Servicio.
- Incorporación o modificaciones relevantes de procesos o actividades críticas del Servicio.
- 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.
- Cambios relevantes en las Definiciones Estratégicas.
- Ajustes necesarios para proteger las infraestructuras críticas.

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

1.8. Roles y responsabilidades

El responsable institucional de seguridad de la información será el encargado de velar por la seguridad de la información y ciberseguridad dentro del órgano de la Administración del Estado respectivo, asegurar el desarrollo, cumplimiento y actualización de la Política y de gestionar la administración de la seguridad de la información y ciberseguridad.



1.9. 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. PRINCIPIOS Y RESPONSABILIDADES TRANSVERSALES

2.1. Principios generales

Esta política busca armonizar los controles necesarios con la debida funcionalidad de los procesos tanto de cara a los usuarios internos como externos y alineados con las diferentes normativas.

Esta política estará basada en enfrentar el riesgo sujeto a los recursos económicos, tecnológicos y humanos disponibles a través de su mitigación.

Se han de considerar los diferentes desafíos que afecten la ciberseguridad con criterios de priorización, privilegiando los procesos que permitan el cumplimiento de los objetivos estratégicos del Servicio y las regulaciones vigentes.

2.2. Principios específicos

2.2.1. Principio de constitucionalidad y legalidad: la Política, se deberá interpretar de manera tal que su aplicación se concilie con las normas constitucionales y legales vigentes, referidas a los derechos y libertades de las personas.

2.2.2. Principio de responsabilidad transversal: el incumplimiento de las obligaciones establecidas en la Política podrá constituir una transgresión que puede ser motivo de acciones administrativas internas. Lo anterior sin perjuicio de la responsabilidad civil o penal que corresponda.



- 2.2.3. Principio del buen uso de los recursos institucionales: el uso de los sistemas de comunicaciones electrónicas debe enmarcarse en el ámbito de competencia de la empresa, teniendo como finalidad el ejercicio de las funciones propias e inherentes para las cuales el usuario ha sido contratado o se ha convenido su prestación de servicios. Se promueve el buen uso de los sistemas de comunicaciones electrónicas, especialmente para aquellas prácticas que protejan a los sistemas de eventuales daños ocasionados por amenazas cibernéticas, entre las que se pueden mencionar: físicas, desastres naturales, por pérdida de servicios esenciales, por perturbación debido a radiación, por compromiso de información sensible, por fallas técnicas, por acciones no autorizadas, por compromiso de funciones, por acción de hacker, por acción de ciberdelincuentes, por acción terrorista, por espionaje industrial, por acción interna y otros.
- 2.2.4. Principio para obtención de prueba en Investigación Interna: con motivo de una investigación interna, la dirección ejecutiva podrá autorizar que el área de TI ejecute, en determinado sistema informático o en los servidores del área a cargo de la administración, procesos definidos tendientes a obtener la información necesaria, de tal forma que se garantice la menor afectación a la privacidad del trabajador.
- 2.2.5. Principio de responsabilidad por uso malicioso: la apertura de archivos adjuntos o la ejecución de programas que se reciban por medios electrónicos, constituyen acciones que pueden vulnerar la estabilidad, calidad o seguridad de las redes o del sistema informático. El personal no debe guardar, abrir o ejecutar en el equipo informático, programas o documentos electrónicos; si la fuente de éstos no es conocida; si no está autorizado por el propietario intelectual o industrial; como tampoco, si no se ha adquirido la licencia respectiva.



2.2.6. Principio de Acciones especiales de seguridad: el personal autorizado del área de TI podrá restringir, bloquear o cancelar el acceso de un usuario a los servicios tecnológicos o a otro servicio o sistema informático, siempre que dicha acción de seguridad sea indispensable en los siguientes casos:

- o Cuando existan requerimientos legales o judiciales, ante la presunta perpetración de algún ilícito.
- o Cuando existan antecedentes fundados, previa calificación de la dirección ejecutiva, que den cuenta de la violación grave de la normativa interna, o de la comisión de un ilícito.
- o Cuando por motivo del acceso, se cause o pueda causar un daño grave e inminente a la calidad o estabilidad del servicio informático o de las redes. Esta circunstancia deberá ser informada por el jefe o jefa del área de TI a la dirección ejecutiva, a más tardar dentro del día hábil siguiente desde que se inició la acción de seguridad.

El jefe o jefa del área de TI deberá informar al usuario afectado por la acción de seguridad, dentro del día hábil siguiente, salvo que la dirección ejecutiva disponga lo contrario.

2.2.7. Principio de confidencialidad e integridad de la información: se deberá garantizar y mantener la confidencialidad e integridad de toda la información y datos de los usuarios, que tenga acceso con ocasión de la administración del sistema informático y los servicios de redes.

2.2.8. Principio de Seguridad ante la navegación en Internet: el personal autorizado del área de TI podrá ejecutar sistemas de filtro, monitoreo y registro del tráfico de la navegación en la Internet, que se realice a través de las redes de la empresa, incluyendo las extranet (VPN), sólo para efectos de mantener protegida la seguridad y estabilidad del sistema informático, así como para procurar que su uso común y regular esté abocado a los fines establecidos.



3. DIFUSIÓN

3.1. Obligación de conocimiento y cumplimiento.

El personal o terceras partes que usen los recursos informáticos de la red de la empresa, deberán conocer y dar cumplimiento a esta Política General de Seguridad de la Información.

3.2. Incorporación de la norma a los actos administrativos y contratos.

Las normas y política expresadas en este documento, se considerarán parte integrante de los contratos de trabajo, y de cualquier otro contrato de servicio que signifique el uso de los medios informáticos proporcionados por la empresa.

3.3. 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 determine o que los actores internos relacionados impulsen, a través de correo masivo invitando a conocerlas, cada vez que sean modificadas tanto la Política General como otras 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.



4. SANCIONES

El no cumplimiento de la Política de Seguridad de la información y Ciberseguridad y las Políticas Específicas será sancionado en conformidad a las disposiciones administrativas internas. Lo anterior, sin perjuicio de la responsabilidad civil o penal que corresponda.

5. GLOSARIO DE TÉRMINOS

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, tarjetas de accesos, software, equipamiento computacional, personal, edificios, infraestructura tecnológica y física.

Amenaza: Causa potencial de un incidente no-deseado por el cual puede resultar dañado o afectado un sistema u organización. Ejemplos: terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.

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.

Documento electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

Dueños de los datos : Se refiere a la Unidad de negocios que maneja datos institucionales, contenidos tanto en medios tradicionales como en sistemas informáticos a que pertenecen los usuarios que son funcionarios del Ministerio, en la calidad contractual que sea.



Estación de Trabajo: Equipo computacional conectado a una red de computadores que facilita a los usuarios el acceso a los servidores y periféricos de la red.

Evaluación del riesgo: Proceso consistente en la comparación de los niveles de riesgo encontrados contra los criterios de riesgo preestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre los beneficios potenciales y resultados adversos, para posteriormente ordenar y priorizar mediante un ranking los riesgos analizados.

Gestión del riesgo: Proceso definido para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización. Es un proceso iterativo que debe contribuir a la mejora organizacional a través del perfeccionamiento de los procesos.

Incidente de Seguridad: Cualquier evento o situación que comprometa la disponibilidad, integridad y confidencialidad de la información, o bien afecte a la plataforma tecnológica, proceso y aplicativos que la contienen, impidiendo acceder a ésta en forma oportuna. En general, es una transgresión de una política, estándar o procedimiento de seguridad, que no permite prestar los servicios institucionales por medios informáticos o tradicionales. Ejemplos de incidentes: Acceso no autorizado, robo de contraseñas, robo de información, denegación de servicio en internet, un malware actuando en los equipos institucionales o un phishing que ataca a los usuarios institucionales.

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

Política de Seguridad: Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.

Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.

Programa malicioso: Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora. También se denominan malware.



Restricción del acceso: Acción consistente en la delimitación de acceso de los funcionarios, servidores públicos a honorarios y terceras partes a determinados recursos físicos o lógicos.

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.

Sanción: Consecuencia jurídica de naturaleza administrativa, civil o penal derivada del incumplimiento de un deber.

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.

Sistema informático: Software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información o transferencia de información.

Sistema de comunicaciones electrónicas: Se refiere a todo medio o dispositivos que permite comunicarse. Entiéndase: correo electrónico, mensajería instantánea (WhatsApp, Instagram, Discord, WeChat, Facebook Messenger, Line, Viber, Snapchat, Skype u otros), Teleconferencia (Skype, Zoom, Microsoft Team, Webex, Jitsi u otros), Telefonía fija y móvil, u otros.

Teletrabajo: si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante estos medios. Válida mientras no exista una disposición legal que la sustituya o modifique en el contexto gubernamental.

Terceras partes: Persona u organismo ajeno a la relación directa establecida entre dos partes principales. Para estos efectos, se entenderá como terceras partes, entre otros a los proveedores de servicios y de red, los proveedores de productos de software y servicios de información, outsourcing de instalaciones y operaciones, servicios de asesoría de seguridad y auditores externos.



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, instalaciones o faenas de la empresa. Válida mientras no exista una disposición legal que la sustituya o modifique en el contexto gubernamental.

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



2. DÉJESE CONSTANCIA, que el documento podrá ser modificado, según lo convenga el Jefe/a superior del Servicio o, acorde las necesidades y/o lineamientos estratégicos del Servicio local de Educación Pública de Huasco.

3. TÓMESE debida nota por quien corresponda para los fines a que haya lugar.

ANÓTESE PUBLÍQUESE Y COMUNÍQUESE

DISTRIBUCIÓN

- Dirección
- Subdirección de ATP.
- Subdirección de Planificación y Control de Gestión
- Subdirección de Administración y Finanzas.
- Unidad de Tecnología de Información.
- Departamento Jurídico.
- Auditoria.



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/VEXN4O-313>