AGENCIA DE CALIDAD DE LA EDUCACION
28 SEP 2021
DOCUMENTO TOTALMENTE TRAMITADO

APRUEBA ACTUALIZACIÓN Y CREACIÓN DE LOS MANUALES Y PROCEDIMIENTOS ASOCIADOS AL PRINCIPIO DE GESTIÓN DE ACTIVOS Y TRANSFERENCIA DE INFORMACIÓN

RESOLUCIÓN EXENTA N° 587

SANTIAGO, 28 SEP 2021

VISTOS:

Lo dispuesto en el DFL N° 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N°19.880, que establece las Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado; en la Ley N°20.529, sobre Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización; en la Ley N°20.285, sobre Acceso a la Información Pública; en la Ley N°19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firmas; en la Ley N°19.628, sobre Protección a la Vida Privada; en el Decreto Supremo N°83, de 2005, 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; en la norma chilena NCh-ISO 27001; en los Memorandum N°58 y N°83, de 2019, del Secretario Ejecutivo de la Agencia de Calidad de la Educación; en la Resolución Exenta N°1527, de 2019, que aprobó la Política de Gestión de Activos de la Agencia de Calidad de la Educación; en la Resolución Exenta N°1611, de 2019, que aprobó la Política para Transferencia y Manejo de Información; en la Resolución Exenta N°583, de 2021, que aprueba la actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación; en la Resolución Exenta N°584, de 2021, que aprueba la Política de Protección de Datos Personales; en la Resolución Exenta N°585, de 2021, que aprueba la actualización del Procedimiento de Respuesta ante Incidentes; en la Resolución Exenta N°218, de 2021 que aprueba medidas y procedimientos de datos personales; en la Resolución Nº7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del Trámite de Toma de Razón, y

CONSIDERANDO:

Que, el artículo 9° de la Ley N°20.529, sobre Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización, crea la Agencia de Calidad de la Educación, servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, cuyo objeto es evaluar y orientar al sistema educativo para que éste propenda al mejoramiento de la calidad y equidad de las oportunidades educativas, considerando las particularidades de los distintos niveles y modalidades educativas.

Que, de acuerdo al Decreto Supremo N°83, de 2005, del Ministerio Secretaría General de la Presidencia, la norma chilena NCh-ISO 27001, y otras normativas presentes en el Sistema de Gestión de Seguridad de la Información, las exigencias y recomendaciones que se proveen, presentan desafíos en cuanto a la necesidad de garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información.

Que, mediante Resolución Exenta N°583, de 28 de septiembre de 2021, se aprobó la actualización de la Política de Seguridad de la Información de la Agencia, definiendo roles y responsabilidades, y estableciendo los pilares institucionales sobre la misma, lo que ha derivado en la necesidad de actualizar y/o dictar nuevas políticas o procedimientos asociados a estas materias.

Que, en este sentido, dentro de las regulaciones que se dejan sin efecto, se encuentran: Resolución Exenta N°1527, de 2019, del Servicio, se aprobó la Política de Gestión de

Activos de la Agencia de Calidad de la Educación y Resolución Exenta N°1611, de 2019, del Servicio, se aprobó la Política para Transferencia y Manejo de Información.

Que, por su parte, mediante Resolución Exenta N°583, de 28 de septiembre de 2021, se aprobó la actualización de política de Seguridad de la Información de la Agencia, definiendo roles y responsabilidades, y estableciendo los pilares institucionales sobre la materia, motivando ello la necesidad de actualizar y/o dictar nuevas políticas o procedimientos.

Que, teniendo en cuenta lo expuesto, corresponde aprobar el presente acto, por medio de cual se aprueba las distintas materias asociadas al principio de gestión de activos y transferencia de información, dejando sin efecto las regulaciones vigentes.

RESUELVO:

PRIMERO: APRUEBASE, el Manual para Administración de Medios Removibles de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Evitar la revelación, modificación, eliminación o destrucción no autorizada de información almacenada en medios de almacenamiento extraíble.

2. ALCANCE

Los lineamientos de este manual extienden su aplicación a todos los medios extraíbles que almacenen y/o transporten fuera de las instalaciones de la Agencia, activos de información críticos según lo estipulado en el Procedimiento de Actualización del Inventario de Activos de Información (SSI-PRO-3.1). Así mismo, el cumplimiento de esta Manual deberá ser aplicado por todo el personal de planta, contrata u honorarios, así como por proveedores externos de la Agencia que por motivo del cumplimiento de su ámbito de responsabilidades deban manipular este tipo de medios.

En relación con la norma ISO/IEC 27.001:2013, este procedimiento considera dentro de su alcance los siguientes controles:

a) ISO/IEC 27.001:2013, Control A.08.03.01 – Administración de medios removibles.

b) ISO/IEC 27.001:2013, Control A.08.03.03 – Transferencia física de medios.

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.2 relativo al principio de gestión de activos y transferencia de información.

b) Resolución Exenta N°584, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Política de Protección de Datos Personales.

c) Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.

4. TÉRMINOS Y DEFINICIONES

Los términos y definiciones que aplican a este y todos los documentos del SSI de la Agencia se encuentran en el Anexo I de la Resolución Exenta N°583 de 2021 de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación. (SSI-POL-01).

5. ROLES Y RESPONSABILIDADES

a) **Jefaturas de División:** como propietarios de los activos de información, serán los responsables de velar por la correcta aplicación dentro de su División, de las medidas dispuestas en este documento.

b) **Jefaturas de Departamento:** ejecutar de forma correcta los lineamientos entregados por este documento, y velar por su ejecución por parte de sus proveedores.

c) **Líder(es) Interno(s) del SSI:** responsable de liderar la adopción de los lineamientos dispuestos en este manual al interior de su División, así como de canalizar las necesidades de mejora que este requiera.

d) **Encargada de Seguridad de Información y Encargada de Ciberseguridad:** ejercer como rol asesor a nivel administrativo y operativo, respectivamente, para la aplicación y mejora continua de este Manual.

Para mejorar el entendimiento de los roles y responsabilidades sobre la aplicación de este manual, se presenta la siguiente matriz RACIE:

Rol	JEFATURA DIVISIÓN	JEFATURA DPTO.	ENC. SI / CIBERSEGURIDAD	LÍDER SSI
RESPONSABLE	X			
EJECUTOR		X		
CONSULTADO			X	
INFORMADO				X

6. LINEAMIENTOS DEL MANUAL

Para establecer una protección adecuada sobre los activos de información críticos de la Agencia, se deben considerar los medios de almacenamiento extraíbles como, por ejemplo, discos duros, dispositivos USB, DVD y CDs. De esta forma, el presente manual considera los siguientes tipos de lineamientos:

a) **Lineamientos de seguridad para medios extraíbles en reposo:** Corresponde a aquellos lineamientos aplicables cuando los medios extraíbles son utilizados netamente para el almacenamiento de información y datos críticos de la Agencia.

b) **Lineamientos de seguridad para medios extraíbles en tránsito:** Corresponde a los lineamientos aplicables cuando los medios extraíbles son utilizados para transferir y/o transportar información y datos críticos desde la Agencia hacia el exterior de ésta, considerando necesariamente la participación de terceros externos a la institución como proveedores.

c) **Lineamientos de seguridad para eliminación y reutilización de medios extraíbles:** Corresponde a los lineamientos aplicables al momento de dar de baja o reutilizar los medios de almacenamiento extraíbles.

6.1. Seguridad para medios extraíbles en reposo

Se debe considerar la aplicación de los siguientes lineamientos, según lo indica el Checklist de Seguridad para Medios Extraíbles que se muestra en el Anexo 1 de este documento:

a) Los medios de almacenamiento extraíble que sean utilizados para almacenar activos de información críticos de la Agencia deben ser fácilmente identificables, mediante su etiquetado.

b) Los medios de almacenamiento extraíble utilizados para almacenar activos de información críticos deberán ser ubicados en instalaciones que cuenten con los mecanismos de control contra amenazas físicas y del medio ambiente, de forma de evitar la indisponibilidad de la información ahí contenida por dichas causas. Para lo anterior se deben considerar los principios de control de acceso físico establecidos en la Política General de Seguridad de Información (SSI-POL-01)[1].

c) Los medios de almacenamiento extraíble utilizados para almacenar activos de información críticos deberán contar con mecanismos de cifrado que impidan el acceso a la información por parte de terceros no autorizados. Para lo anterior se deben considerar los principios para uso de controles criptográficos[2] y responsabilidades en el acceso a la información[3] establecidos en la Política General de Seguridad de Información (SSI-POL-01) en lo que se refiere a la aplicación de mecanismos de cifrado y generación de las contraseñas robustas que permitan cifrar de forma segura los medios de almacenamiento extraíble, derivadas de la aplicación de estos principios.

6.2. Seguridad para medios extraíbles en tránsito

Se debe considerar la aplicación de los lineamientos dispuestos en el punto anterior, para ser complementados por los siguientes:

a) Identificación de las personas externas que manipularán el o los medios de almacenamiento extraíbles y en qué contexto. Estas personas deben ser designadas por el o los proveedores involucrados y notificados a la Agencia previo a su manipulación.

b) Se deben establecer mecanismos de seguimiento y auditoría sobre la manipulación de los medios de almacenamiento extraíbles por parte del proveedor o tercero externo a la Agencia, de forma de validar que solo se han manipulado los medios según lo estipulado en el contrato o relación con la Agencia. Para lo anterior, se debe considerar como mínimo la información que se lista a continuación, plasmada en la Ficha de Transferencia Física de Medios Extraíbles que se presenta en el Anexo 2 de este documento:

   i. Fechas y horas de recepción / entrega de los medios.
   ii. Nombre y apellido de las personas que participaron en cada entrega y recepción de estos medios como parte de las actividades de manipulación que efectúa el proveedor.
   iii. Entidad a la que pertenece la persona que participa en la manipulación del medio extraíble.
   iv. Propósito de la manipulación, que puede abarcar más no se limita a la entrega, recepción o almacenamiento del medio extraíble.
   v. Observaciones de interés para la seguridad del medio extraíble y la trazabilidad durante su manipulación.

6.3. Seguridad para eliminación o reutilización de medios extraíbles

---

[1] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra b) sobre el control de acceso físico.
[2] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.4), letra a), punto ii) sobre la aplicación de controles criptográficos.
[3] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra a), punto iv) sobre las responsabilidades del usuario en el acceso a la información.

Finalmente, se debe considerar la aplicación de la seguridad al momento de dar de baja o reutilizar este tipo de dispositivos. Para lo anterior, se deben considerar los siguientes lineamientos, que al momento de ejecutarlos deben ser incluidos en el Checklist de Seguridad para Medios Extraíbles del Anexo 1:

a) Para la eliminación o reutilización de los medios de almacenamiento extraíbles que sean utilizados para almacenar información crítica se debe aplicar un borrado seguro que impida la recuperación parcial o total de éstos por parte de terceros no autorizados. Para lo anterior se debe considerar el principio de eliminación y reutilización del equipamiento dispuesto en la Política General de Seguridad de Información (SSI-POL-01)[4].

7. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-3.1— Checklist de seguridad para medios extraíbles
MANUAL / PROCEDIMEINTO	Administración de medios removibles
CONTROLES ISO 27.001	• ISO/IEC 27.001:2013, Control A.08.03.01 – Administración de medios removibles.
RESPONSABLE	Jefaturas de División o quien ésta designe
DESCRIPCIÓN	Corresponde a la validación de la inclusión de las medidas de seguridad dispuestas en este manual al momento de utilizar medios extraíbles para almacenar información o datos críticos de la Agencia.
FRECUENCIA	En función de la necesidad de utilizar medios extraíbles en el contexto que indica este manual.
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-3.1— Ficha de transferencia física de medios extraíbles
MANUAL / PROCEDIMEINTO	Administración de medios removibles
CONTROLES ISO 27.001	• ISO/IEC 27.001:2013, Control A.08.03.03 – Transferencia física de medios.
RESPONSABLE	Jefaturas de División o quien esta designe
DESCRIPCIÓN	Corresponde a la evidencia de manipulación sobre los medios extraíbles por parte de terceros externos a la Agencia, cuando estos son utilizados para transferir o transportar información o datos críticos de la Agencia.
FRECUENCIA	En función de la necesidad de utilizar medios extraíbles en el contexto que indica este manual.
ALMACENAMIENTO	Digital – Google Drive del responsable

8. NO CONFORMIDADES E INCUMPLIMIENTO

Los riesgos y no conformidades derivadas del incumplimiento o necesidad de mejora de los lineamientos establecidos en este documento deberán ser comunicados directamente tanto al Propietario y/o Custodio de los activos de información involucrados, como a las

[4] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra b), punto i) sobre la eliminación y reutilización del equipamiento.

Encargadas de Seguridad de Información y Ciberseguridad, de forma de establecer e implementar las acciones correctivas necesarias.

Así mismo, cualquier evento o incidente de seguridad de la información, deberá ser canalizado según lo estipulado en el Procedimiento de Respuesta ante Incidentes de Seguridad (SSI-PRO-5.1).

1. ANEXOS.

1.1. Anexo 1: Checklist de seguridad para medios extraíbles

Agencia de Calidad de la Educación	**Checklist de Seguridad para Medios Extraíbles**			
	Nivel de Confidencialidad	*Medio Uso Interno*	Páginas	**1 de 1**
			Versión	**0**
	Fecha versión del documento	**TBD**	Código	**SSI-RO-MAN-3.1**
	Checklist de Seguridad para Medios Extraíbles			

Se declara que se han implementado los siguientes controles de seguridad según lo dispuesto en el Manual para la Administración de Medios Removibles (SSI-MAN-3.1) del Sistema de Seguridad de Información de la Agencia:

1. Checklist para medios removibles en reposo:

   ☐ Etiquetado del medio extraíble que indique claramente que la información contenida en éste es de carácter crítico.

   ☐ Ubicación cuenta con protección contra amenazas físicas y del ambiente.

   ☐ Cifrado

2. Checklist para medios removibles en tránsito:

   ☐ Ficha de transferencia física de medios (aplica solo si el medio extraíble ha sido manipulado por terceros externos a la Agencia).

3. Checklist para la eliminación o reutilización física de medios:

El medio extraíble fue:

☐ Eliminado o dado de baja. ☐ Disponibilizado para su reutilización

☐ Se aplica borrado seguro al momento de eliminar o disponibilizar para su reutilización el medio extraíble.

Comentarios:

_____
_____
_____
_____

1.1.Anexo 2: Ficha de transferencia física de medios extraíbles

	Ficha de Transferencia Física de Medios Extraíbles			
	Nivel de Confidencialidad	*Medio Uso Interno*	Páginas	1 de 2
			Versión	0
	Fecha versión del documento	TBD	Código	SSI-RO-MAN-3.1
	Ficha de Transferencia Física de Medios Extraíbles			

Se declara que sobre el o los medios extraíbles _____ se han ejecutado las siguientes acciones:

FECHA	HORA	NOMBRE Y APELLIDO	ENTIDAD	PROPÓSITO DE MANIPULACIÓN	OBSERVACIONES

Comentarios:

_____

_____

SEGUNDO: APRUEBASE, el Procedimiento de Elaboración y Actualización del Inventario de Activos de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Asegurar que se genera y mantiene actualizado el inventario de activos de información e inventario de sistemas productivos de la Agencia.

2. ALCANCE

Este procedimiento debe ser ejecutado por todas las Divisiones de la Agencia, así como por la Unidad de TIC, dependiente de la División de Administración General (DAG).

En relación con la norma ISO/IEC 27.001:2013, este procedimiento considera dentro de su alcance los siguientes controles:

a) ISO/IEC 27.001:2013, Control A.8.1.1 – Inventario de activos.

b) ISO/IEC 27.001:2013, Control A.8.1.2 – Propiedad de los activos.

c) ISO/IEC 27.001:2013, Control A.8.2.1 – Clasificación de la información.

d) Asegurar que se genera y mantiene actualizado el inventario de activos de información e inventario de sistemas productivos de la Agencia.

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.2 relativo al principio de gestión de activos y transferencia de información.

b) Resolución Exenta N°584, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Política de Protección de Datos Personales.

c) Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.

4. TÉRMINOS Y DEFINICIONES

Los términos y definiciones que aplican a este y todos los documentos del SSI de la Agencia se encuentran en el Anexo I de la Resolución Exenta N°583 de 2021 de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación. (SSI-POL-01).

5. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades se encuentran definidos en la sección Modo de Operación, para cada uno de los procedimientos que conforman este documento.

6. LINEAMIENTOS DEL PROCEDIMIENTO

Para dar cumplimiento al objetivo de este procedimiento, cada inventario de activos de información deberá considerar:

a) La División a la que pertenecen los activos de información.
b) Proceso y subproceso al cual están asociados los activos de información.
c) Identificador único de los activos de información.
d) Nombre de los activos de información, considerando que esta debe ser pensada para su mantención en el tiempo, por ende, debe estar relacionado lo más posible con el nombre que se le da a diario en la operación del proceso y subproceso asociado.
e) Descripción funcional de los activos de información, la que debe facilitar el entendimiento sobre la función y relevancia que cumplen cada uno de éstos para el proceso y subproceso asociado.
f) Asociación de los activos de información con la tecnología en donde se gestionan, estableciendo el medio tecnológico sobre el cual es almacenado o tratado cada activo de información. Para lo anterior se deben considerar, más no limitar a herramientas o sistemas web, carpetas compartidas, repositorios de almacenamiento de información, medios removibles, servidores, entre otros a fin.
g) Niveles de criticidad de los activos de información para los ámbitos de Confidencialidad, Disponibilidad, Integridad y Privacidad.

Así mismo, el inventario de sistemas deberá considerar, más no limitarse a:

a) Nombre del sistema, considerando que debe coincidir con los sistemas definidos en el inventario de activos de información.
b) URL mediante la cual se accede al sistema. Aplica solo para aquellos de tipo web.
c) División a la cual presta servicios el sistema.

d) Proceso de la división a la cual presta servicios el sistema.
e) Unidad o Departamento que administra el sistema.
f) Nombre y rol de la persona responsable de la administración del sistema.
g) Descripción funcional del sistema, la que debe facilitar el entendimiento sobre la función y relevancia que cumplen cada uno de éstos para el proceso / subproceso asociado.
h) Período de operación del sistema, que permitirá identificar si existen sistemas que se mantienen en producción durante períodos específicos.
i) Fecha de última actualización.
j) Estado

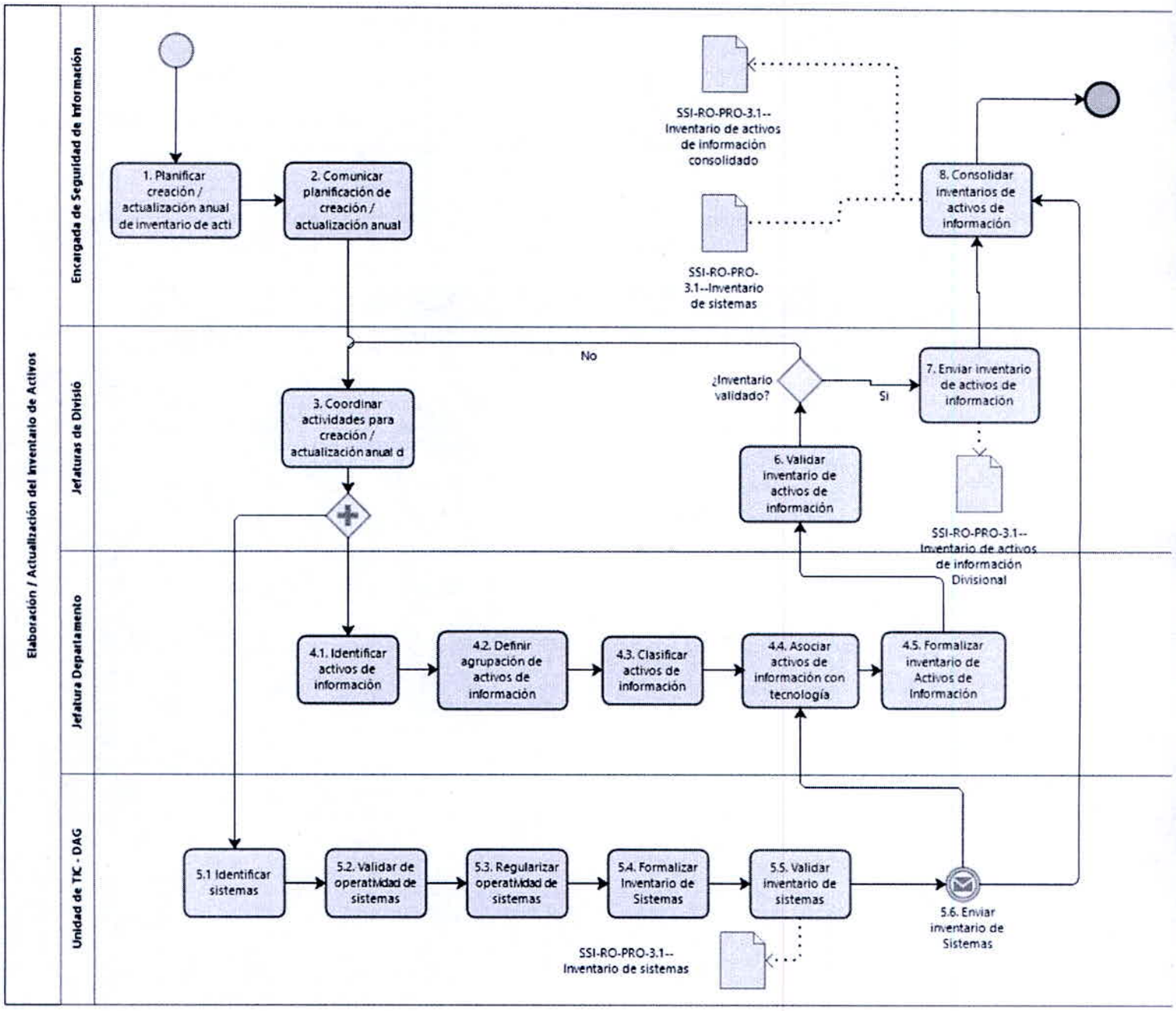
6.1. Criterios de clasificación de activos

DIMENSIÓN	Descripción	NIVEL DE CRITICIDAD	DESCRIPCIÓN
Conf.	Definir confidencialidad de activos.	Alto	Información que sólo puede ser accedida por ciertos miembros de la institución. Su divulgación al público puede provocar daños considerables en términos legales y reputacionales.
		Medio	Información disponible para todos los miembros de la Agencia (uso interno). Su divulgación puede causar daños reputacionales moderados a la institución.
		Bajo	Toda información cuya publicación sea aplicable por la ley de transparencia.
Disp.	Definir disponibilidad de activos.	Alto	La indisponibilidad del activo implica la detención total o parcial de uno o más procesos críticos de la Agencia, así como un incumplimiento de la ley de transparencia.
		Medio	La indisponibilidad del activo conlleva la ralentización o detención de uno o más procesos de la agencia.
		Bajo	La indisponibilidad del activo no implica consecuencias asociadas a la ralentización o detención de procesos internos de la institución.
Int.	Definir integridad de activos.	Alto	La modificación no autorizada del activo implica consecuencias considerables de tipo legal, monetario, y/o reputacional para la Agencia.
		Bajo	La modificación no autorizada del activo no implica consecuencias significativas para la institución.
Priv.	Definir privacidad de activos	Alto	El activo cuenta con información individualizable, y su divulgación se encuentra penada por al ley 19.628 de protección de datos personales.
		Bajo	El activo no posee información de carácter personal o individualizable.

7. MODO DE OPERACIÓN

A continuación, se especifican a nivel de diagrama, descripción de actividades y matriz de responsabilidades, los flujos procedimentales asociados a este documento.

7.1. Flujo de Procedimiento para la Elaboración/Actualización de Inventarios de Activos de Información



7.2. Matriz de Procedimiento para la Elaboración/Actualización de Inventarios de Activos de Información

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Planificar creación / actualización anual de inventario de activos.	Elaborar una planificación del proceso de creación/actualización del inventario de activos de información de la Agencia. Esta planificación debe realizarse al menos una vez al año calendario,	Encargada(o) de Seguridad de la Información	2

		y debe incluir a todas las Divisiones de la Agencia.		
2	Comunicar planificación de creación / actualización anual de inventario de activos.	La planificación anual de creación / actualización del inventario de activos, debe ser enviada a los Propietarios / Dueños de los activos de información de la Agencia y a la Unidad de TIC como custodio de la tecnología y sistemas en la Agencia.	Encargada(o) de Seguridad de la Información	3
3	Coordinar actividades para creación / actualización anual de inventario de activos.	Coordinar los equipos internamente para la creación / actualización del inventario de activos de cada División, y el inventario de sistemas de la Agencia.	Jefaturas de División	4.1 y 5.1
4.1	Identificar activos de información.	Identificar los activos de información de cada División, de la forma más detallada posible, estableciendo la relación con los procesos y subprocesos de la División en los que éste influye. **NOTA:** Si ya existe un listado de activos de información, esta actividad tendrá carácter de actualización.	Jefaturas de Departamento	4.2
4.2	Definir agrupación de activos de información.	De ser posible, y, en caso de que la lista de activos de información identificados en la actividad anterior resultase muy extensa, se podrá definir una agrupación de éstos, centrando la atención en aquellos que tengan similar gestión y/o criticidad para el proceso, subproceso o División a la que pertenecen.	Jefaturas de Departamento	4.3
4.3	Clasificar activos de información.	Se debe establecer la clasificación de criticidad de los activos de información según los lineamientos entregados anteriormente en este documento.	Jefaturas de Departamento	4.4
4.4	Asociar activos de información con tecnología.	Se debe establecer qué sistemas de la Agencia son utilizados para la operación sobre los activos de información, o la agrupación de éstos.	Jefaturas de Departamento	4.5
4.5	Formalizar inventario de activos de información	Una vez identificados, agrupados, clasificados y asociados con la tecnología, se debe, plasmar la información en una planilla excel para ser validada por la Jefatura de División, la cual debe considerar los lineamientos entregados previamente en este documento.	Jefaturas de Departamento	6
5.1	Identificar sistemas	Se deben identificar los sistemas que apalancan la operación de los procesos críticos de cada División.	Unidad de TIC - DAG	5.2

5.2	Validar operatividad de sistemas.	Se debe validar si los sistemas identificados en la actividad (5.1) se encuentran todos en producción, con la finalidad de identificar sistemas que deban ser dados de baja por haber cumplido su período de operación.	Unidad de TIC - DAG	5.3
5.3	Regularizar operatividad de sistemas	En función de los resultados de la actividad (5.2), se debe actualizar la lista de sistemas para dejar en ésta solo aquellos que se encuentran operativos y soportan la operación de los procesos críticos de las Divisiones.	Unidad de TIC - DAG	5.4
5.4	Fomralizar inventario de sistemas	Una vez regularizada la identificación de los sistemas operacionales críticos de la Agencia, se deben plasmar en una planilla excel que considere los lineamientos entregados previamente en este documento, para ser validado por la Jefatura TIC - DAG.	Unidad de TIC - DAG	5.5
5.5	Validar inventario de sistemas	Se debe validar el inventario de sistemas para ser enviada a las Divisiones como insumo para completar sus inventarios de activos de información. A modo informativo, se debe compartir también el inventario de sistemas con la Encargada de Seguridad de Información y Encargada de Ciberseguridad.	Jefatura Unidad TIC	5.6
5.6	Enviar inventario de sistemas	Se debe enviar el inventario a las Divisiones y a la Encargada de Seguridad de Información.	Unidad de TIC - DAG	4.4 y 8
6	Validar inventario de activos de información	Se debe validar el inventario de activos de información, considerando que éste es el principal input para la definición del alcance del SSI y ejecución del análisis de riesgos de seguridad de información de la institución. Se pueden dar las siguientes opciones: - El inventario es validado (7). - El inventario no es validado (3).	Jefaturas de División	3 o 7
7	Enviar inventario de activos de información.	Se debe hacer envío a la Encargada de Seguridad de Información, con copia a la Encargada de Ciberseguridad, del inventario de activos de información e inventario de sistemas por parte de los responsables de éstos.	Jefaturas de División	8

8	Consolidar inventario de activos de información.	Se debe consolidar en un solo inventario de carácter institucional, todos los inventarios de activos de información e inventario de sistemas proporcionados por las Divisiones.	Encargada(o) de Seguridad de la Información	FIN

7.3 Matriz de Responsabilidades

A continuación, se presenta la matriz RECIE del procedimiento bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

ID	ACTIVIDAD	ENCARGADA SI	JEFATURA DIVISIÓN	JEFATURA DPTO.	UNIDAD TIC - DAG	JEFATURA DAG	LÍDERES INTERNOS SSI
1	**Planificar creación / actualización anual de inventario de activos.**	R/E	C	-	-		-
2	**Comunicar planificación de creación / actualización anual de inventario de activos.**	R/E	I	-	I		I
3	**Coordinar actividades para creación / actualización anual de inventario de activos.**	C	R/E	C/I	C/I		C/I
4.1	**Identificar activos de información.**	C	R	E	-		C
4.2	**Definir agrupación de activos de información.**	C	R	E	-		C
4.3	**Clasificar activos de información.**	C	R	E	-		C
4.4	**Asociar activos de información con tecnología.**	C	R	E	C		C
4.5	**Formalizar inventario de activos de información**	I	R	E	I		I
5.1	**Identificar sistemas**	C	I	C	E	R	C
5.2	**Validar operatividad de sistemas.**	C	I	C	E	R	C
5.3	**Regularizar operatividad de sistemas**	C	I	C	E	R	C
5.4	**Formalizar Inventario de Sistemas**	C	I	C	E	R	C
5.5	**Validar inventario de sistemas**	C	I	C	E	R	C
5.6	**Enviar inventario de sistemas**	C	I	C	E	R	C

6	**Validar inventario de activos de información**	C	R	C	C		C
7	**Enviar inventario de activos de información.**	I	R	E	-		I
8	**Consolidar inventario de activos de información.**	R	I	-	-		-

8. REGISTRO DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-3.1—Inventario de activos de información consolidado
MANUAL / PROCEDIMIENTO	Creación y actualización de inventario de activos de información.
CONTROLES ISO 27.001	• A.8.1.1 – Inventario de activos. • A.8.1.2 – Propiedad de los activos. • A.8.2.1 – Clasificación de la información.
RESPONSABLE	Encargada de Seguridad de Información
DESCRIPCIÓN	Corresponde a la planilla con el consolidado de todos los inventarios de activos de información Divisionales.
FRECUENCIA	Anual
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-3.1—Inventario de activos de información Divisional
MANUAL / PROCEDIMIENTO	Creación y actualización de inventario de activos de información.
CONTROLES ISO 27.001	• A.8.1.1 – Inventario de activos. • A.8.1.2 – Propiedad de los activos. • A.8.2.1 – Clasificación de la información.
RESPONSABLE	Jefaturas de División, o a quienes éstas designen
DESCRIPCIÓN	Corresponde a la planilla con los activos de información de la División, clasificados según su criticidad.
FRECUENCIA	Anual
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-3.1—Inventario de Sistemas
MANUAL / PROCEDIMIENTO	Creación y actualización de inventario de activos de información.
CONTROLES ISO 27.001	• A.8.1.1 – Inventario de activos. • A.8.1.2 – Propiedad de los activos. • A.8.2.1 – Clasificación de la información.
RESPONSABLE	Jefaturas Unidad de TIC - DAG
DESCRIPCIÓN	Corresponde a la planilla con los sistemas productivos de la Agencia según los lineamientos de este procedimiento.
FRECUENCIA	Anual
ALMACENAMIENTO	Digital – Google Drive del responsable

9. NO CONFORMIDADES E INCUMPLIMIENTOS

Los riesgos y no conformidades derivadas del incumplimiento o necesidad de mejora de los lineamientos establecidos en este documento deberán ser comunicados directamente tanto al Propietario y/o Custodio de los activos de información involucrados, como a las Encargadas de Seguridad de Información y Ciberseguridad, de forma de establecer e implementar las acciones correctivas necesarias.

Así mismo, cualquier evento o incidente de seguridad de la información, deberá ser canalizado según lo estipulado en el Procedimiento de Respuesta ante Incidentes de Seguridad (SSI-PRO-5.1).

10. ANEXO

Anexo 1. Inventarios de Activos de Información

DIVISIÓ	CATEGORÍA	PROCESO	SUBPROCESO	AI-ID	ACTIVO	TECNOLOGÍA ASOCIADA	DESCRIPCIÓN	CONF	DISP	PRIV	INT
DELA	Instrumentos de aplicación	Construcción de Instrumentos	Elaboración de Instrumentos de Aplicación Experimental	DELA-01	Instrumentos de Aplicación	Drive de Unidad de Pruebas Simce. Equipos de profesionales de Unidad de Pruebas Simce. Proveedor de prueba. Respaldos en CDC - DVD Unidad de Pruebas Simce.	Conjunto de ítems agrupados en una prueba o cuestionario a ser aplicada.	ALTA	ALTA	ALTA	ALTA
DELA	Instrumentos de aplicación	Construcción de Instrumentos	Elaboración de Instrumentos de Aplicación Definitivos	DELA-02	Instrumentos de Aplicación (Digital e impreso)	Drive de Unidad de Pruebas Simce y Depto. De Operaciones de Campo. Equipos de profesionales de Unidad de Pruebas Simce y Depto. De Operaciones de Campo. Proveedores de los servicios de diagramación, impresión, aplicación y capturo.	Conjunto de Pruebas y cuestionarios en su versión definitiva, para su impresión y aplicación.	ALTA	ALTA	ALTA	ALTA
DELA	Instrumentos de aplicación	Operaciones de Campo y Logística	Aplicación en terreno	DELA-03	Instrumentos de Aplicación Impresos con respuestas	Proveedores de los servicios de aplicación y captura.	Conjunto de Pruebas y cuestionarios aplicados para los distintos evaluaciones.	ALTA	ALTA	ALTA	ALTA
DELA	Bases de datos y digitalización de imágenes	Todos los Macroprocesos DELA	Todos los Macroprocesos DELA	DELA-04	Matriz de productos DELA	Drive DELA	Archivo con especificaciones técnicas como: cantidad y tipo de prueba, cantidad de formas, áreas a aplicar, cantidad estimada de preguntas y páginas, colores de impresión, entre otros; de los productos que levantará y aplicará la División durante el año.	ALTA	ALTA	ALTA	ALTA
DELA	Bases de datos y digitalización de imágenes	Operaciones de Campo y Logística	Empadronamiento, Impresión y distribución del material de aplicación	DELA-05	Base de Datos de empadronamiento, Impresión y Marcaje de base de aplicación.	Servidores Agencia Proveedores del servicio de impresión, aplicación y captura.	Bases de datos asociadas a los resultados del proceso de empadronamiento para rendir la aplicación y, Base de Datos de impresión y marcaje con información correspondiente a: curso, nombres, código de barra, entre otros, además, la base de aplicación que se entrega a los proveedores	ALTA	ALTA	ALTA	ALTA
DELA	Bases de datos y digitalización de imágenes	Procesamiento y Análisis de Datos	Captura	DELA-06	Imágenes Digitalizadas	Proveedor del servicio de captura y servicio de corrección. Discos duro externo administrado por asistente de Gestión de Datos. Servidores Agencia. Software de corrección de preguntas abiertas.	Conjunto de imágenes digitalizadas correspondientes a los distintos instrumentos de aplicación.	ALTA	ALTA	ALTA	ALTA

TERCERO: **APRUEBASE,** el Manual para la Transferencia y Manejo de Información de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Mantener la seguridad de la información y datos durante la manipulación o transferencia de los mismos, ya sea dentro de la Agencia, así como con cualquier entidad externa.

2. ALCANCE

Estos lineamientos deben ser aplicados por el personal de planta, contrata y honorarios de la Agencia, así como por los proveedores que por cumplimiento del servicio acordado deba tener acceso a los sistemas o activos de información de la Agencia.

En relación con la norma ISO/IEC 27.001:2013, este procedimiento considera dentro de su alcance los siguientes controles:

a) ISO/IEC 27001:2013, Control A.08.02.02 – Etiquetado de información.

b) ISO/IEC 27001:2013, Control A.13.02.01 – Políticas y procedimientos de transferencia de información.

c) ISO/IEC 27001:2013, Control A.13.02.02 – Acuerdos sobre transferencia de información.

d) ISO/IEC 27001:2013, Control A.13.02.02 – Mensajería electrónica

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la

Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.2 relativo al principio de gestión de activos y transferencia de información.

b) Resolución Exenta N°584, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Política de Protección de Datos Personales.

c) Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.

4. TÉRMINOS Y DEFINICIONES

Los términos y definiciones que aplican a este y todos los documentos del SSI de la Agencia se encuentran en el Anexo I de la Resolución Exenta N°583 de 2021 de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación. (SSI-POL-01).

5. ROLES Y RESPONSABILIDADES

a) Jefaturas de División: responsable de velar por el cumplimiento y correcta aplicación de lo estipulado en este manual, así como de facilitar la implementación de las medidas necesarias para cumplir con su objetivo y alcance.

b) Líder(es) Interno(s) del SSI: liderar la adopción de lo dispuesto en este manual al interior de su División, así como canalizar cualquier necesidad de mejora u optimización operacional que éste requiera.

c) Jefaturas de Departamento: responsable de la correcta ejecución de los lineamientos de este manual por parte del personal que compone su Departamento.

d) Encargada de Seguridad de Información y Encargada de Ciberseguridad: ejercer como rol asesor desde un nivel administrativo y operativo, respectivamente, para la aplicación y mejora continua de este Manual.

Para mejorar el entendimiento de los roles y responsabilidades sobre la aplicación de este manual, se presenta la siguiente matriz RACIE:

Rol	JEFATURA DIVISIÓN	JEFATURA DPTO.	ENC. SI / CIBERSEGURIDAD	LÍDER SSI
RESPONSABLE	X			
EJECUTOR		X		
CONSULTADO			X	
INFORMADO				X

6. LINEAMIENTOS DEL MANUAL

Para proteger el intercambio de información mediante el uso de todo tipo de recursos de comunicación, ya sea al interior de la Agencia y/o con terceras partes, se deben considerar los siguientes lineamientos:

a) Las responsabilidades asociadas a la seguridad de los activos de información se establecen según la Política General (SSI-POL-01)[5].

b) Los activos que contengan información y/o datos críticos de la Agencia deben ser fácilmente identificables, para lo cual se debe considerar su etiquetado en base a su nivel de criticidad según los principios de gestión de activos y transferencia de información descritos en la Política General de Seguridad de Información (SSI-POL-01)[6]. Para el etiquetado, se debe considerar lo siguiente:

   i. Cuando el activo de información se genera digitalmente, se debe indicar su nivel de confidencialidad ya sea en su encabezado o utilizando marca de agua.

   ii. Cuando el activo de información es gestionado de forma física y no cuenta con un etiquetado de su nivel de confidencialidad como se describe en el punto anterior, se deberá indicar utilizando mecanismos físicos como timbres y sellos.

   iii. Para optimizar la operación del etiquetado de activos de información, se puede etiquetar el soporte o equipamiento mediante el cual se almacena, procesa, transfiere o transporta el o los activos de información críticos. Para el caso de la utilización de medios de almacenamiento extraíbles se debe complementar este lineamiento según el principio de gestión de activos y transferencia de información dispuesto en la política general de seguridad (SSI-POL-01)[7].

c) La copia o reproducción de aquellos activos de información críticos se debe realizar con la debida autorización de su propietario, o en su defecto de su custodio.

d) Se debe tener la precaución de no dejar activos de información críticos en impresoras o dispositivos periféricos similares, de forma de protegerlos de accesos no autorizados.

e) Las Divisiones de segunda línea de defensa, deberán ser conscientes al momento de manipular activos de información críticos de la primera línea, de forma de alinearse a las definiciones de seguridad que éstos requieren. Para identificar los activos de información críticos de la Agencia se deben utilizar los principios de gestión de activos y transferencia de información descritos en la Política General de Seguridad de Información (SSI-POL-01)[8].

f) Se deben establecer los mecanismos necesarios para garantizar la trazabilidad y no repudio sobre los activos de información críticos.

g) Los propietarios o custodios de los activos de información de la primera línea deben definir la pertinencia de otorgar acceso a sus activos de información críticos cuando estos deben ser transferidos o manipulados por roles de las Divisiones de la segunda línea de defensa.

---

[5] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.3) sobre la estructura funcional del SSI.
[6] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra a), punto i) sobre la elaboración y actualización del inventario de activos de información.
[7] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra b), punto iii) sobre la administración de medios removibles.
[8] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra a), punto i) sobre la elaboración y actualización del inventario de activos de información.

h) Para el uso de medios de almacenamiento extraíbles, serán los propietarios y custodios de los activos de información los responsables de hacer efectivos los controles asociados y definidos en el principio de gestión de activos y transferencia de información dispuesto en la política general de seguridad (SSI-POL-01) [9].

i) Para la transferencia de activos de información que contengan datos privados, se deben considerar los lineamientos establecidos en la Política de protección de datos privados (SSI-POL-06)[10].

j) En caso de que un tercero deba acceder o manipular activos de información de la Agencia, será responsabilidad de su propietario y custodio que éstos incorporen los lineamientos de seguridad necesarios durante la prestación de su servicio.

k) Las diferentes Divisiones, podrán establecer convenios para transferencia de información con terceras partes, para lo cual deben considerar los lineamientos de seguridad dispuestos en general por el SSI. Estos convenios o acuerdos de transferencia de información deben estar formalmente establecidos.

6.1. Uso de medios electrónicos para transferencia de información

Al momento de utilizar medios electrónicos para la transferencia y manejo de información crítica se deben considerar los siguientes lineamientos:

a) Queda prohibida la transferencia o manejo de información crítica a través de medios electrónicos diferentes a los provistos por la suite de Google Workspace.

b) Al momento de utilizar el correo electrónico para la transferencia de información crítica, se debe tener en consideración:

   i. Que el o los activos de información a transferir se encuentren etiquetados según lo definido por este manual.

   ii. Que no se encuentren en copia usuarios que no posean el privilegio de acceso a estos activos.

   iii. Utilizar el modo confidencial de Gmail cuando sea necesario.

c) Al momento de utilizar Google Drive para la transferencia y manejo de información crítica, se debe tener en consideración:

   i. Velar por la correcta aplicación de los permisos de acceso y privilegios de manipulación de los activos según lo establecido en el principio de control de acceso físico y lógico de la Política General de Seguridad (POL-01)[11].

7. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN

[9] Resolución Exenta N°583 de 2021 de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra a), punto i) sobre la elaboración y actualización del inventario de activos de información.
[10] Resolución Exenta N°584, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Política de Protección de Datos Personales.
[11] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra a) sobre el control de acceso lógico.

NOMBRE	SSI-RO-MAN-3.2— Lista de convenios de transferencia de información
MANUAL / PROCEDIMEINTO	Transferencia y manejo de información
Controles	• A.08.02.02 – Etiquetado de información. • A.13.02.01 – Políticas y procedimientos de transferencia de información. • A.13.02.02 – Acuerdos sobre transferencia de información. • A.13.02.02 – Mensajería electrónica.
RESPONSABLE	Jefaturas de División o quien ésta designe
DESCRIPCIÓN	Corresponde al listado donde se identifican tanto las áreas internas como las instituciones externas con las cuales existe transferencia de activos de información críticos.
FRECUENCIA	En función de la necesidad de transferencias de información crítica de la División.
ALMACENAMIENTO	Digital – Google Drive del responsable

8. NO CONFORMIDADES E INCUMPLIMIENTOS

Los riesgos y no conformidades derivadas del incumplimiento o necesidad de mejora de los lineamientos establecidos en este documento deberán ser comunicados directamente tanto al Propietario y/o Custodio de los activos de información involucrados, como a las Encargadas de Seguridad de Información y Ciberseguridad, de forma de establecer e implementar las acciones correctivas necesarias.

Así mismo, cualquier evento o incidente de seguridad de la información, deberá ser canalizado según lo estipulado en el Procedimiento de Respuesta ante Incidentes de Seguridad (SSI-PRO-5.1).

9. ANEXO

Anexo I: Listado de convenios de transferencia de información

Agencia de Calidad de la Educación	Listado de convenios de transferencia de información			
	Nivel de Confidencialidad	*Medio Uso Interno*	Páginas	1 de 2
			Versión	0
	Fecha versión del documento	TBD	Código	SSI-RO-MAN-3.2
Gobierno de Chile	Listado de convenios de transferencia de información			

El siguiente listado corresponde a las áreas internas e instituciones externas con las cuales la División ______________________ transfiere y/o intercambia activos de información críticos:

ÁREA / INSTITUCIÓN	MOTIVO DE LA TRANSFERENCIA DE INFORMACIÓN	ACTIVOS DE INFORMACIÓN TRANSFERIDOS	OBSERVACIONES

CUARTO: APRUEBASE, el Manual para la Asignación y Devolución de Recursos de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Establecer una gestión de los recursos y equipamiento tecnológicos utilizados por el personal de la Agencia.

2. ALCANCE

Los lineamientos de este manual se deben aplicar para todo el equipamiento tecnológico disponibilizado para el cumplimiento de las responsabilidades del personal de la Agencia, independiente de la naturaleza de su relación contractual.

En relación con la norma ISO/IEC 27.001:2013, este procedimiento considera dentro de su alcance los siguientes controles:

a) ISO/IEC 27.001:2013, Control A.08.01.04 - Devolución de activos.

b) ISO/IEC 27.001:2013, Control A.09.04.04 - Uso de programas utilitarios privilegiados.

c) ISO/IEC 27.001:2013, Control A.16.06.02 – Restricciones sobre instalación de software.

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.2 relativo al principio de gestión de activos y transferencia de información.

b) Resolución Exenta N°584, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Política de Protección de Datos Personales.

c) Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.

d) Resolución Exenta N°586, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización y Creación de los manuales y procedimientos asociados al principio de Control de Acceso Físico y Lógico.

4. TÉRMINOS Y DEFINICIONES

Los términos y definiciones que aplican a este y todos los documentos del SSI de la Agencia se encuentran en el Anexo I de la Resolución Exenta N°583 de 2021 de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación. (SSI-POL-01).

5. ROLES Y RESPONSABILIDADES

a) Jefaturas de División: responsable de la correcta ejecución y cumplimiento de este manual en lo que respecta a la devolución de los recursos o equipamiento asignados al personal de su División. Deberá canalizar y facilitar las gestiones para la mejora continua y optimización del manual.

b) Jefatura de Unidad de TIC - DAG: ejecutar y cumplir este manual en lo que respecta a la entrega y recepción del equipamiento. Deberá canalizar y facilitar las gestiones para la mejora continua y optimización del manual.

c) Líder(es) Interno(s) del SSI: Serán los responsables de liderar la adopción de estos lineamientos al interior de sus Divisiones.

d) Jefaturas de Departamento: ejecutar las acciones técnicas necesarias para garantizar la correcta devolución del equipamiento asignado al personal de su Departamento. Deberán proponer mejoras y optimizaciones operacionales para el procedimiento.

e) Encargada de Seguridad de Información y Encargada de Ciberseguridad: ejercer como rol asesor a nivel administrativo y operativo, respectivamente, para la aplicación y mejora continua de este Manual.

Para mejorar el entendimiento de los roles y responsabilidades sobre la aplicación de este manual, se presenta la siguiente matriz RACIE:

Rol	JEFATURA DIVISIÓN	JEFATURA DPTO.	JEFATURA UNIDAD TIC - DAG	ENC. SI / CIBERSEGURIDAD	Líder SSI
RESPONSABLE	X				
EJECUTOR		X	X		

CONSULTADO				X	
INFORMADO					X

6. LINEAMIENTOS DEL MANUAL

Para establecer una gestión segura de los recursos y equipamiento tecnológico de la Agencia se deben considerar los lineamientos de:

a) **Acondicionamiento de equipos para asignación:** Corresponde a los controles de seguridad aplicables durante la preparación del equipamiento previa a su entrega a los usuarios.

b) **Devolución de equipamiento:** Corresponde a los controles de seguridad aplicables una vez entregado el equipamiento por parte los usuarios a la Unidad de TIC.

6.1. Lineamientos para el Acondicionamiento de los Equipos

Previo a la entrega del equipamiento a los usuarios de la Agencia, se debe establecer una configuración base que considere los siguientes aspectos:

a) Creación de usuario en el Controlador de Dominio con los privilegios respectivos como se definen en el Procedimiento de Gestión de Cuentas y Accesos (SSI-PRO-4.1)[12].

b) Instalación de sistema operativo Windows 10 Pro 64 bits, versión 20H1 o 20H2.

c) Instalación de los softwares por defecto:

   i. Office 2016, versión KB3115276.

   ii. PDF Viewer, última versión disponible al momento del acondicionamiento del equipo.

   iii. Winrar, última versión disponible al momento del acondicionamiento del equipo.

   iv. VLC, última versión disponible al momento del acondicionamiento del equipo.

   v. Google Drive File Stream vinculado a la cuenta corporativa de correo electrónico.

   vi. Google Chrome, última versión disponible al momento del acondicionamiento del equipo.

   vii. Sistema VPN.

   viii. TeamViewer Corporate.

d) Instalación y configuración de herramientas de seguridad, incluyendo la configuración mínima de seguridad para los equipos:

   i. Sistema antimalware Sophos.

   ii. Configuration Manager

[12] Resolución Exenta N°586, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización y Creación de los manuales y procedimientos asociados al principio de Control de Acceso Físico y Lógico.

iii. Establecer permisos limitados para la instalación de software aplicables solo a personal con perfil administrador.

iv. Se debe impedir lo más posible la libertad de los usuarios para utilizar programas utilitarios que puedan afectar la operación de las herramientas de seguridad.

v. Se debe establecer cifrado de disco duro para todo el equipamiento que sea utilizado fuera de las instalaciones de la Agencia, con énfasis en aquellos disponibilizados a los usuarios evaluadores de establecimientos.

7. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-4.1—Registro de asignaciones actualizado en CMDB
MANUAL / PROCEDIMIENTO	Asignación y devolución de recursos
CONTROLES ISO 27.001	• A.08.01.04 – Devolución de activos. • A.09.04.04 – Uso de programas utilitarios privilegiados. • A.16.06.02 – Restricciones sobre instalación de software
RESPONSABLE	Jefatura Unidad de TIC – DAG
DESCRIPCIÓN	Corresponde a la captura de pantalla de la CMDB institucional, donde el estado de asignación de los equipos coincide con las altas y bajas de usuario.
FRECUENCIA	Dependerá de la frecuencia de la asignación y devolución de recursos.
ALMACENAMIENTO	Digital – Google Drive del responsable

8. NO CONFORMIDADES E INCUMPLIMIENTO

Los riesgos y no conformidades derivadas del incumplimiento o necesidad de mejora de los lineamientos establecidos en este documento deberán ser comunicados directamente tanto al Propietario y/o Custodio de los activos de información involucrados, como a las Encargadas de Seguridad de Información y Ciberseguridad, de forma de establecer e implementar las acciones correctivas necesarias.

Así mismo, cualquier evento o incidente de seguridad de la información, deberá ser canalizado según lo estipulado en el Procedimiento de Respuesta ante Incidentes de Seguridad (SSI-PRO-5.1).

QUINTO: APRUEBASE, el Procedimiento de Eliminación o Reutilización de Equipamiento de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Evitar el acceso, modificación, eliminación o destrucción no autorizada de la información, equipos y medios removibles.

2. ALCANCE

Todos los equipos y soportes institucionales utilizados para el acceso, administración o almacenamiento de datos e información crítica de la Agencia, y que por cumplimiento de su ciclo de uso o de su vida útil deba ser eliminado o reutilizado.

En relación con la norma ISO/IEC 27.001:2013, este procedimiento considera dentro de su alcance los siguientes controles:

a) ISO/IEC 27.001:2013, Control A.8.3.2 – Eliminación de medios.
b) ISO/IEC 27.001:2013, Control A.11.2.7 – Seguridad en la reutilización o descarte de equipos.

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.2 relativo al principio de gestión de activos y transferencia de información.

b) Memorándum N°58, de 2019, del Secretario Ejecutivo de la Agencia de Calidad de la Educación.

c) Resolución Exenta N°584, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Política de Protección de Datos Personales.

d) Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.

4. TÉRMINOS Y DEFINICIONES

Los términos y definiciones que aplican a este y todos los documentos del SSI de la Agencia se encuentran en el Anexo I de la Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación. (SSI-POL-01).

5. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades se encuentran definidos en la sección Modo de Operación, para cada uno de los procedimientos que conforman este documento.

6. LINEAMIENTOS DEL PROCEDIMIENTO

Para ejercer una protección adecuada de la información crítica de la Agencia al momento de eliminar o reutilizar medios de almacenamiento y equipos, se deben seguir los siguientes lineamientos:

a) Se establece que ante todo evento que requiera de la aplicación de este procedimiento, se deberá aplicar el borrado de información seguro mediante el método de "wimping", minimizando así las probabilidades de recuperación de información sobre estos medios de almacenamiento y equipamiento.

b) Previo a la aplicación del método "wimping" de borrado seguro, se debe verificar que se ha hecho un respaldo preventivo de la información contenida en los medios de almacenamiento o equipos en cuestión, de forma de poder acceder a esta información en caso de ser requerida posteriormente. Lo

anterior debe considerar los principios de seguridad en la gestión TIC dispuestos en la Política de Seguridad de Información (SSI-POL-01)[13].

c) En caso de que un medio de almacenamiento extraíble deba ser eliminado o reutilizado, la información de éste se debe respaldar en la cuenta de Google Drive del custodio de los activos de información que éste contiene.
d) Se debe llevar registro y generar evidencia de la ejecución del borrado seguro del equipamiento.
e) Puede ser necesario para la eliminación de equipamiento, la contratación de proveedores especializados en esta labor, los que deben entregar evidencia de la ejecución de sus actividades, siguiendo los lineamientos establecidos en la Política de Seguridad en la Relación con Proveedores de la Agencia (SSI-POL-08)[14].

f) Al momento de dejar un equipo disponible para su reutilización, previa ejecución del borrado seguro se debe considerar el dejar el equipo en un estado "por defecto", es decir, con las configuraciones básicas para ser reutilizado.

   Estas configuraciones base incluyen, más no se limitan a:
   i. Inactivación de la herramienta antimalware de forma de que no ensucie los indicadores asociados al principio de seguridad en la gestión TIC relacionado con la protección contra código maliciosos, dispuesto en la Política General de Seguridad de Información (SSI-POL-01)[15].

   ii. Cambiar el nombre del equipo para que sea fácilmente identificable que no está asignado a ningún usuario de la organización.

   iii. Dejar instalado solo el software base por defecto definido en el principio de gestión de activos y transferencia de información de la Política de Seguridad de Información (SSI-PO-01)[16].

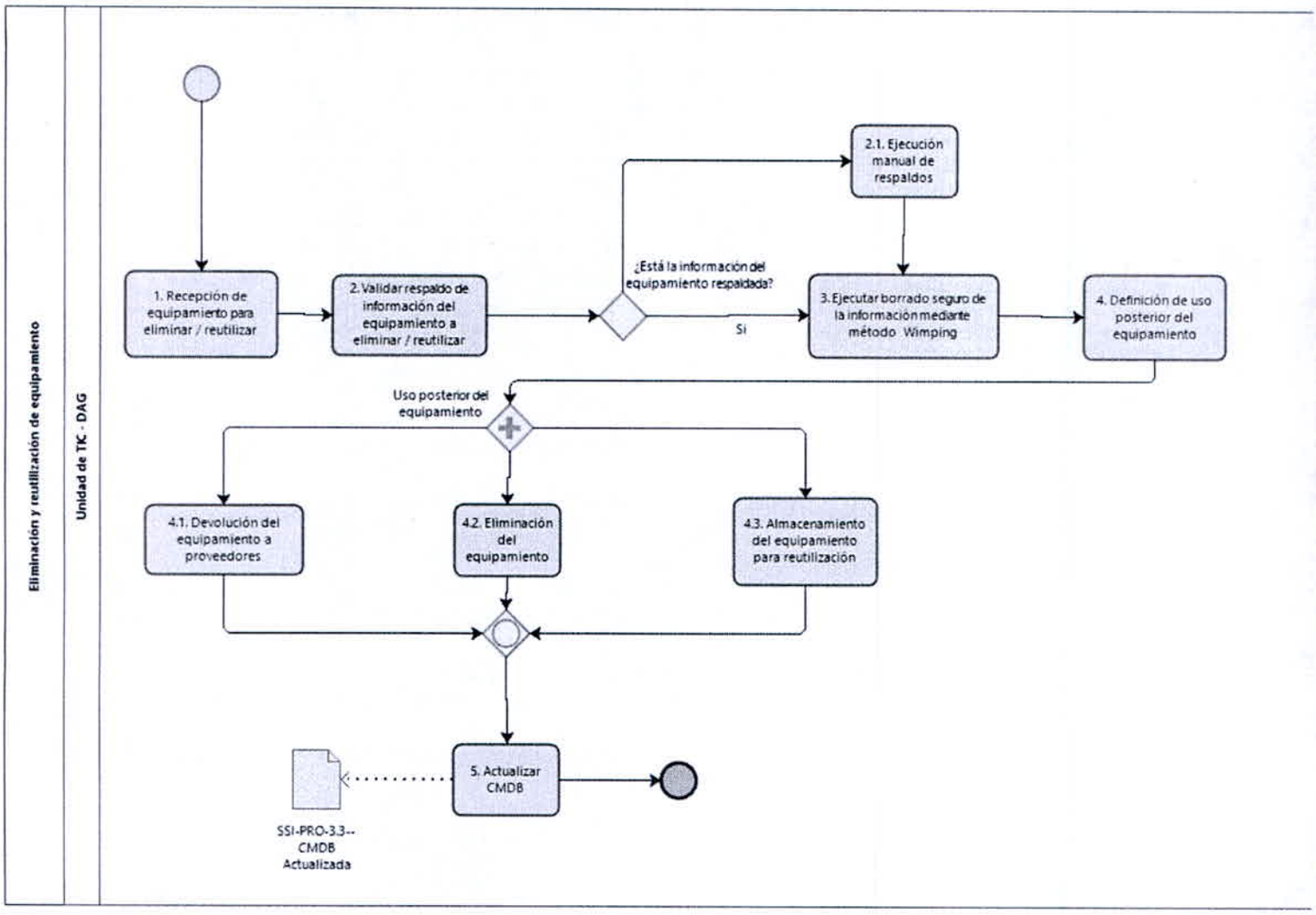
7. MODO DE OPERACIÓN

A continuación, se describen los flujos de actividades para los siguientes procedimientos de eliminación y reutilización del equipamiento:

a) Procedimiento de eliminación o reutilización del equipamiento.

[13] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.4), letra a), punto v) sobre el respaldo de sistemas, software y cuentas de usuario.
[14] Resolución Exenta N°1612, de 2019, de la Agencia de Calidad de la Educación, que aprueba la Política de Seguridad de la información para relación con proveedores.
[15] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.4), letra a), punto iii) sobre la protección contra código malicioso.
[16] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra b), punto ii) sobre asignación y devolución de equipamiento.

7.1. Flujo de Procedimiento para eliminación o reutilización del equipamiento



7.2. Matriz de Procedimiento para la eliminación o reutilización del equipamiento

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Recepción de equipamiento para eliminar / reutilizar	Se debe recibir el equipo y/o medios de almacenamiento por parte de la División / usuario a la cual fueron asignados. Esta recepción debe ser validada y concordante con el equipamiento entregado al usuario o usuarios en cuestión, según los registros de operación del Procedimiento de Asignación y Devolución de Equipamiento (SSI-PRO-3.2).	Unidad de TIC - DAG	2
2	Validar respaldo de información del equipamiento a eliminar / reutilizar	Previo a la aplicación del borrado seguro sobre el equipamiento a eliminar / reutilizar, se debe validar que la información que éste contiene se encuentre respaldada según los principios de respaldo de información establecidos en la Política General de	Unidad de TIC - DAG	2.1 o 3

		Seguridad (SSI-POL-01) [17]. Se pueden dar los siguientes escenarios: - La información del equipo o medio no se encuentra respaldada (2.1). - La información del equipo o medio se encuentra respaldada (3).		
2.1	Ejecución manual de respaldos	Se deben ejecutar los respaldos manuales según los principios de respaldo de información establecidos en la Política General de Seguridad (SSI-POL-01) [18].	Unidad de TIC - DAG	3
3	Ejecutar borrado seguro de la información mediante método Wimping	Se debe ejecutar el borrado seguro mediante método de "wimping".	Unidad de TIC - DAG	4
4	Definición de uso posterior del equipamiento	En función de la necesidad que haya gatillado de recepción del equipamiento, se debe determinar el uso posterior de éste, donde se pueden dar los siguientes escenarios: - El equipamiento debe ser devuelto al proveedor (4.1). - El equipamiento debe ser eliminado (4.2). - El equipamiento será reutilizado (4.3).	Unidad de TIC - DAG	4.1, 4.2, o 4.3
4.1	Devolución del equipamiento a proveedores	Se deben ejecutar las actividades necesarias para devolver el equipamiento al proveedor según los acuerdos estipulados en el contrato con éste. En esta actividad, si la relación con el proveedor es a través de un Departamento, éste debe formar parte activa de esta actividad.	Unidad de TIC - DAG	5
4.2	Eliminación del equipamiento	El equipamiento deberá ser eliminado de forma segura, ya sea de forma interna o externa. En esta actividad, si la relación con el proveedor es a través de un Departamento este debe formar parte activa de esta actividad.	Unidad de TIC - DAG	5
4.3	Almacenamiento del equipamiento para reutilización	El equipamiento deberá ser almacenado en una ubicación segura que cuente tanto con la protección ante amenazas físicas y del medio ambiente según el principio de seguridad física establecido en la Política General de Seguridad de Información (SSI-POL-01)[19], como con los lineamientos entregados en este documento.	Unidad de TIC - DAG	5

[17] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.4), letra a), punto v) sobre el respaldo de sistemas, software y cuentas de usuario.
[18] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.4), letra a), punto v) sobre el respaldo de sistemas, software y cuentas de usuario.
[19] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra b), punto i) sobre el control de acceso físico al equipamiento de procesamiento de información.

5	Actualizar CMDB[20]	Se debe actualizar la CMDB de la Agencia, siguiendo las siguientes directrices: - Equipo devuelto al proveedor o eliminado: Actualizar CMDB eliminado equipamiento. - Equipo es bodegado para reutilización: Actualizar CMDB dejando el equipamiento como "Disponible".	Unidad de TIC - DAG	FIN

7.3. Matriz de responsabilidades para Procedimiento para eliminación o reutilización del equipamiento

En este punto se presentan las matrices de responsabilidades tipo RACIE de los procedimientos anteriores, bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para el procedimiento de eliminación o reutilización del equipamiento:

ID	ACTIVIDAD	JEFATURA DAG	JEFATURA DPTO	JEFATURA UNIDAD TIC - DAG	ENC SI / CIBER
1	Recepción de equipamiento para eliminar / reutilizar	R	I/C	E	-
2	Validar respaldo de información del equipamiento a eliminar / reutilizar	R	I/C	E	C
2.1	Ejecución manual de respaldos	R	C	E	-
3	Ejecutar borrado seguro de la información mediante método Wimping	R	C	E	-
4	Definición de uso posterior del equipamiento	R	C	E	-
4.1	Devolución del equipamiento a proveedores	R	E	E	C/I
4.2	Eliminación del equipamiento	R	E	E	C/I
4.3	Almacenamiento del equipamiento para reutilización	R	-	E	-
5	Actualizar CMDB	R	-	E	-

8. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-3.3—CMDB Actualizada
PROCEDIMIENTO	Eliminación o reutilización del equipamiento
CONTROLES ISO 27.001	• A.8.3.2 – Eliminación de medios. • A.11.2.7 – Seguridad en la reutilización o descarte de equipos
RESPONSABLE	Jefatura de Unidad TIC - DAG
DESCRIPCIÓN	Corresponde a la actualización de la CMDB de la Unidad de TIC donde se da cuenta de los equipos que están en bodega una vez preparados para su reutilización o aquellos que fueron eliminados.

[20] Configuration Management Data Base.

FRECUENCIA	En función de la demanda de eliminación / reutilización de equipamiento
ALMACENAMIENTO	Digital – Google Drive del responsable

9. NO CONFORMIDADES E INCUMPLIMIENTO

Los riesgos y no conformidades derivadas del incumplimiento o necesidad de mejora de los lineamientos establecidos en este documento deberán ser comunicados directamente tanto al Propietario y/o Custodio de los activos de información involucrados, como a las Encargadas de Seguridad de Información y Ciberseguridad, de forma de establecer e implementar las acciones correctivas necesarias.

Así mismo, cualquier evento o incidente de seguridad de la información, deberá ser canalizado según lo estipulado en el Procedimiento de Respuesta ante Incidentes de Seguridad (SSI-PRO-5.1).

SEXTO: DÉJASE SIN EFECTO la Resolución Exenta N°s 1527 y 1611, ambas de 2019, de la Agencia de Calidad de la Educación.

SÉPTIMO: COMUNIQUESE por el Departamento de Gestión de Personas la presente resolución mediante correo electrónico a las jefaturas de las Divisiones y Macrozonas de la Agencia de Calidad de la Educación.

OCTAVO: **DIFUNDASE**, el presente procedimiento a todo el personal de la Agencia de Calidad de la Educación y a terceros que presten servicios para la misma.

PUBLÍQUESE la presente resolución en el Portal Transparencia.

REPUBLICA DE CHILE
Agencia de Calidad de la Educación
SECRETARIO EJECUTIVO

DANIEL RODRÍGUEZ MORALES
SECRETARIO EJECUTIVO
AGENCIA DE CALIDAD DE LA EDUCACIÓN

ASA/GCL/NJO/CBR

Distribución:
- Divisiones Agencia de Calidad de la Educación
- Macrozonas Agencia de Calidad de la Educación
- Archivo Secretaría Ejecutiva
- Unidad de Planificación
- Departamento de Auditoría
- Departamento Jurídico
- Oficina de Partes