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

APRUEBA ACTUALIZACIÓN Y CREACIÓN DE LOS MANUALES Y PROCEDIMEINTOS ASOCIADOS AL PRINCIPIO DE SEGURIDAD DE LA GESTIÓN DE TECNPLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC)

RESOLUCIÓN EXENTA N° 588

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; Resolución Exenta N°1026, de 14 de agosto de 2019, del Servicio, se aprobó la Política de Ubicación y Protección de Equipamiento de la Agencia de Calidad de la Educación; Resolución Exenta N°1613, de 13 de diciembre de 2019, del Servicio, se aprobó la Política de controles de Red; en la Resolución Exenta N°1616, de 13 de diciembre de 2019, del Servicio, que aprobó la Política de Protección contra Código Malicioso; Resolución Exenta N°1547, de 05 de diciembre de 2019, del Servicio, se aprobó la Política de Desarrollo Seguro Control; y Resolución Exenta N°1548, de 05 de diciembre de 2019, del Servicio, se aprobó la Política de Gestión de Controles Criptográficos y Contraseñas; en los Memorándum N°58 y N°83, de 2019, del Secretario Ejecutivo; 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 sobre Protección de Datos Personales; en la Resolución Exenta N°585, de 2021, que aprueba la actualización del Procedimiento de Respuesta ante Incidentes de la Agencia de Calidad de la Educación; en la Resolución Exenta N°218, de 2021 que aprueba medidas y procedimientos de datos personales; en la Resolución N°7, 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°1026, de 14 de agosto de 2019, del Servicio, se aprobó la Política de Ubicación y Protección de Equipamiento de la Agencia de Calidad de la Educación; Resolución Exenta N°1613, de 13 de diciembre de 2019, del Servicio, se aprobó la Política de controles de Red; en la Resolución Exenta N°1616, de 13 de diciembre de 2019, del Servicio, que aprobó la Política de Protección contra Código Malicioso; Resolución Exenta N°1547, de 05 de diciembre de 2019, del Servicio, se aprobó la Política de Desarrollo Seguro Control; y Resolución Exenta N°1548, de 05 de diciembre de 2019, del Servicio, se aprobó la Política de Gestión de Controles Criptográficos y Contraseñas.

Que, teniendo en cuenta lo expuesto, corresponde aprobar el presente acto, por medio de cual se aprueba las distintas materias asociadas al principio de seguridad en la gestión de tecnologías de información y comunicación (TIC), dejando sin efecto las regulaciones vigentes.

RESUELVO:

PRIMERO: **APRUEBASE,** el Manual para la Seguridad en Operaciones TIC de Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Establecer los lineamientos base para la seguridad en las operaciones tecnológicas de la Agencia.

2. ALCANCE

Estos lineamientos deben ser aplicados para toda la infraestructura TIC de la Agencia, incluyendo el equipamiento físico, software, redes y sistemas.

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.11.02.01 – Ubicación y protección del equipamiento.
b) ISO/IEC 27001:2013, Control A.11.02.08 – Equipo de usuario desatendido.
c) ISO/IEC 27001:2013, Control A.12.01.04 – Segregación de ambientes de desarrollo, pruebas y operación.
d) ISO/IEC 27001:2013, Control A.12.04.01 – Registro de eventos.
e) ISO/IEC 27001:2013, Control A.12.04.02 – Protección de la información de registro.
f) ISO/IEC 27001:2013, Control A.12.04.03 – Registros del administrador y del operador.
g) ISO/IEC 27001:2013, Control A.13.01.01 – Controles de red.
h) ISO/IEC 27001:2013, Control A.13.01.02 – Seguridad de los servicios de red.
i) ISO/IEC 27001:2013, Control A.13.01.03 – Segregación de redes

3. NORMAS Y REFERENCIAS

a) 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 de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

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 los manuales y procedimientos relativos al principio de control de acceso físico y lógico.

e) Resolución Exenta N°1612, de 2019, de la Agencia de Calidad de la Educación, que aprueba la Política de Seguridad de Información para Relación con Proveedores de la Agencia de Calidad de la Educación.

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) **Jefatura División de Administración General (DAG):** 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) **Jefatura de la Unidad de TIC – DAG:** ejecutar y dar 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.

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

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

ROL	JEFATURA DAG	UNIDAD TIC - DAG	ENC. SI / CIBERSEGURIDAD
RESPONSABLE	X		
EJECUTOR		X	
CONSULTADO			X
INFORMADO			

6. LINEAMIENTO DEL MANUAL

Para incluir la seguridad de la información y datos críticos de la Agencia dentro de la operación TIC, se consideran los siguientes ámbitos:

a) **Aseguramiento de la operación correcta y segura de las instalaciones de procesamiento de información:** corresponde a los lineamientos de seguridad que abordan aspectos físicos para la seguridad de la operación TIC, como la seguridad del equipamiento físico y de las instalaciones críticas de procesamiento de información que administra la Unidad de TIC.

b) **Registro de eventos y monitoreo operacional:** corresponde a los lineamientos de seguridad que abordan el monitoreo de los componentes lógicos de la infraestructura tecnológica de la Agencia, como el uso de recursos de servidores, y acciones de los usuarios sobre los sistemas y software operacional de la institución.

c) **Seguridad en las redes:** corresponde a los lineamientos de seguridad que abordan las redes de comunicación de la Agencia, sean estas internas o con conexión hacia internet.

6.1. Lineamientos para la seguridad en instalaciones críticas de procesamiento de información

Las instalaciones críticas de procesamiento de información administradas por la Unidad de TIC – DAG se encuentran definidas en el Manual para Seguridad Física (SSI-MAN-4.1)[1], así como los lineamientos asociados a su protección contra amenazas físicas y del ambiente. Dentro de estas instalaciones (Centro de Datos, oficinas y bodegas de la Unidad de TIC), adicional a lo anterior, se deben considerar las siguientes directrices:

a) Los equipos en bodega deberán situarse de forma que se minimicen los accesos no autorizados y los accesos innecesarios en estas instalaciones.

b) Los equipos de la Unidad de TIC que manipulan el equipamiento que se ubica en estas instalaciones deberían instalarse de tal forma que se minimice el riesgo de que la información sea vista durante su uso por personas no autorizadas.

c) Sobre los equipos disponibilizados a los usuarios de la Agencia, se deben establecer configuraciones de seguridad que terminen las sesiones activas después de cinco (5) minutos de inactividad, bloqueando el equipo para que el usuario deba autenticarse al requerir utilizarlo nuevamente.

6.2. Lineamientos para el registro de eventos y monitoreo operacional

Se deben implementar los siguientes lineamientos asociados al monitoreo y registro de eventos en sistemas y software operacionales de la Agencia.

a) Todos los sistemas y software operativos de servidores operacionales de la Agencia deben contar con un registro de eventos (log) asociados al comportamiento de los usuarios sobre éstos. La información para monitorear debe incluir, más no limitarse a:

   i. Identificador (ID) de los usuarios.
   ii. Actividades del sistema.
   iii. Fechas, tiempos y detalles de eventos clave, por ejemplo, conexión (log-on) y desconexión (log-off).
   iv. Identidad o localización del dispositivo, si es posible e identidad del sistema.
   v. Registro de intentos de acceso a los sistemas exitosos y fallidos.
   vi. Registro de intentos de acceso a los recursos y a los datos exitosos y fallidos.

[1] Resolución Exenta N°586, de 2021, de la Agencia de Calidad de la Educación, que aprueba los manuales y procedimientos relativos al principio de control de acceso físico y lógico.

vii. Cambios en la configuración de los sistemas y software.
viii. Uso de privilegios.
ix. Uso de utilidades y aplicaciones del sistema.
x. Ficheros a los que se ha accedido y el tipo de acceso.
xi. Direcciones y protocolos de red.
xii. Activación y desactivación de los sistemas de protección, tales como antimalware o detección de intrusos.
xiii. Transacciones ejecutadas por usuarios en las aplicaciones, sólo si éstas son de tipo transaccional.

b) La definición de qué información adicional se debe considerar en los registros de actividad de los usuarios debe tener concordancia con las necesidades de monitoreo de seguridad, sin que este punto inhabilite la responsabilidad de monitoreo específico de la operación TIC.

c) La definición de información y actividad a considerar debe contemplar los lineamientos de la Política de Protección de Datos Personales (SSI-POL-06)[2].

d) Cuando sea posible, los usuarios administradores no deben tener el privilegio de borrar sus propios registros.

e) La información de registro de eventos (log) debe contar con las protecciones que minimicen el riesgo asociado a la alteración o borrado de la información registrada o de los directorios que las contienen.

f) Se deben disponer los controles necesarios para que la recolección de información de registro de los sistemas y software no supere la capacidad de almacenamiento de los servidores asociados, evitando así la indisponibilidad de estos por falta de capacidad.

g) Se debe ejercer una revisión constante y periódica de los registros asociados a la actividad de usuarios, incluyendo de usuarios con privilegios de administración.

6.3. Lineamientos para la seguridad en las redes

Para incluir la seguridad en las redes de comunicación de la Agencia y así proteger la información en los sistemas, se deben implementar las siguientes directrices:

a) Cuando sea posible, la responsabilidad en la administración de las redes debe estar separada de la administración de los sistemas y aplicaciones productivos.

b) integridad de la información que es transmitida a través de las redes de comunicación, para lo cual deben considerarse los lineamientos que establecen los principios de gestión de controles criptográficos[3] y transferencia de información[4] establecidos en la Política General de Seguridad de Información de la Agencia (SSI-POL-01).

c) Se debe implementar un registro de eventos y su monitoreo para permitir la detección y detención de acciones que pueden afectar la seguridad de información.

d) Los sistemas de red deben ser autenticados.

---

[2] Resolución Exenta N°584, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Política de Protección de Datos Personales.
[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 6.2.4), letra a), punto ii) sobre la gestión de controles criptográficos.
[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 a), punto ii) sobre la transferencia y confidencialidad de información.

e) La conexión de los sistemas de red debe ser restringida.

f) Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en redes distintas.

g) En lo respectivo a los servicios de red provistos por proveedores, se debe considerar la identificación de los mecanismos de seguridad, niveles de servicio y requisitos de gestión para incluirlos en cualquier acuerdo con proveedor como lo indica la Política para relación con proveedores (SSI-POL-08)[5].

7. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-7.2—Configuración para cierre de sesión automático en equipos, sistemas y software.
MANUAL / PROCEDIMIENTO	Seguridad en Operaciones TIC
CONTROLES ISO 27.001	• A.11.02.01 – Ubicación y protección del equipamiento. A.11.02.08 – Equipo de usuario desatendido.
RESPONSABLE	Jefe Unidad TIC - DAG
DESCRIPCIÓN	Corresponde a la captura de pantalla que evidencia la configuración para el bloqueo de equipos y cierre de sesiones en sistemas y software después de cinco (5) y diez (10) minutos de inactividad respectivamente.
FRECUENCIA	En función de los cambios definidos en las configuraciones de equipos, sistemas y software.
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-7.2—Separación de redes.
MANUAL / PROCEDIMIENTO	Seguridad en Operaciones TIC
CONTROLES ISO 27.001	• A.12.01.04 – Segregación de ambientes de desarrollo, pruebas y operación. • A.13.01.01 – Controles de red. • A.13.01.02 – Seguridad de los servicios de red. • A.13.01.03 – Segregación de redes.
RESPONSABLE	Jefe Unidad TIC - DAG
DESCRIPCIÓN	Corresponde a la captura de pantalla que evidencia la separación de las redes de servicios de información, usuarios y sistemas de información, así como la separación de las redes asociadas a ambientes productivos, prueba y desarrollo.
FRECUENCIA	En función de los cambios en las redes de la Agencia.
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-7.2—Registro de eventos.
MANUAL / PROCEDIMIENTO	Seguridad en Operaciones TIC
CONTROLES ISO 27.001	• A.12.04.01 – Registro de eventos.

[5] 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.

	• A.12.04.02 – Protección de la información de registro. • A.12.04.03 – Registros del administrador y del operador.
RESPONSABLE	Jefe Unidad TIC - DAG
DESCRIPCIÓN	Corresponde a la captura de pantalla que evidencia la realización de un registro de eventos de la actividad sobre los sistemas y software de la Agencia.
FRECUENCIA	En función de la implementación de este control sobre los sistemas y software de la Agencia.
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)[6].

SEGUNDO: APRUEBASE, el Procedimiento de Control de Cambios TIC de Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Establecer los lineamientos para incluir la seguridad en la ejecución de cambios sobre la infraestructura tecnológica productiva de la Agencia.

2. ALCANCE

Este procedimiento debe aplicarse ante cualquier cambio significativo sobre la infraestructura tecnológica productiva que pueda afectar la operación 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 27.001:2013, Control A.12.01.02 – Control de cambios.
b) ISO/IEC 27.001:2013, Control A.12.01.03 – Gestión de la capacidad.
c) ISO/IEC 27.001:2013, Control A.12.04.04 – Sincronización de relojes.
d) ISO/IEC 27.001:2013, Control A.12.05.01 – Instalación de software en sistemas operacionales.
e) ISO/IEC 27.001:2013, Control A.14.02.01 – Revisión de las aplicaciones después de los cambios en la plataforma de operación.
f) ISO/IEC 27.001:2013, Control A.14.02.01 – Revisión de las aplicaciones después de los cambios en la plataforma de operación.

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 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

[6] Resolución Exenta N°584 de 2021 de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización del Procedimiento de Respuesta ante Incidentes de Ciberseguridad.

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

Los cambios sobre la infraestructura TIC y software de la Agencia, deben ser controlados e involucrar a todos los roles, tanto técnicos como del negocio cuyos procesos se puedan ver afectados por dichos cambios. Para lo anterior, se deben tener en cuenta las siguientes directrices:

a) Se entenderá como cambio significativo, toda modificación, nueva configuración, actualización, instalación de parche o similares, cuya implementación tenga un impacto potencial directo en la operación de uno o varios procesos de la Agencia o en la seguridad de información de uno o varios activos críticos, y por ende requiere de la coordinación con todos los roles involucrados.

b) Al momento de definir el requerimiento de un cambio sobre la infraestructura TIC o softwares de la Agencia, se debe realizar una evaluación de los impactos potenciales considerando los impactos en la seguridad de la información.

c) Se debe dejar un registro de los cambios significativos, así como planificarlos y probarlos previo a su implementación total en producción.

d) Los cambios significativos deben ser aprobados formalmente por el Dueño Funcional de los sistemas y el Propietario o Custodio de los Activos de Información involucrados.

e) Los cambios significativos deben ser comunicados en detalle a todas las partes respectivas.

f) Los cambios significativos deben aplicarse en primera instancia sobre un ambiente de pruebas separado del ambiente productivo como indica el principio de seguridad en la gestión de tecnologías de información y comunicación de la Política General de Seguridad de Información (SSI-POL-01)[7].

g) Se debe supervisar y ajustar la utilización de recursos tecnológicos como memoria, disco y capacidad de procesamiento en general, así como realizar proyecciones de los requisitos futuros de capacidad para garantizar el rendimiento y disponibilidad de la infraestructura TIC y el software. Para esto, se debe considerar lo siguiente:

[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 6.2.4), letra a), punto i) sobre la seguridad en las operaciones TIC.

i. Borrado de datos obsoletos.
ii. Desmantelamiento de bases de datos, aplicaciones y sistemas cuando éstos no requieren estar en operación.
iii. Optimización lógica de las aplicaciones y las consultas a la base de datos.
iv. Denegación o restricción del ancho de banda para servicios consumidores de muchos recursos, en función de su criticidad para la organización.

6.1. Sincronización de Relojes

Si bien la sincronización de relojes no se considera un cambio significativo dado su impacto potencial bajo para la operación, es de vital importancia su correcta ejecución ya que es un factor importante para la gestión y respuesta ante incidentes. Por esto, se deben tener en cuenta las siguientes directrices:

a) La fuente oficial de tiempo y hora precisas para efectuar la sincronización de relojes en la Agencia será el Servicio Hidrográfico y Oceánico de la Armada de Chile, el cual proporciona la fecha y hora exactos para Chile Continental, Chile Insular y la Región de Magallanes: http://www.horaoficial.cl/.

6.2. Instalación de Software en Sistemas Operacionales

Dentro del contexto del control de cambios, y, de forma de mantener la integridad del software en producción, se deberá controlar la instalación de software en estos sistemas teniendo en cuenta las siguientes directrices:

a) Todo cambio a nivel de software deberá incorporar requisitos de seguridad según el principio de seguridad en la gestión de tecnologías de información y comunicación de la Política General de Seguridad de Información (SSI-POL-01)[8].

b) La actualización de los sistemas y software operacional sólo deberán llevarse a cabo por roles administradores que forman parte de los Equipos internos de la Unidad de TIC - DAG.

c) Los sistemas operativos deben manejar códigos ejecutables aprobados, y no códigos de desarrollo o compiladores, de forma de complementar lo dispuesto por la Política General de Seguridad de Información en su principio sobre la seguridad en la gestión de las tecnologías de información y comunicación (SSI-POL-01)[9].

d) El software de las aplicaciones y de los sistemas operativos, solo deberá ser instalado tras haberse realizado pruebas de usabilidad, seguridad e impacto en otros componentes de la infraestructura TIC. Así mismo, si al momento de realizar estas evaluaciones se determina que el cambio es significativo, se debe contar con la autorización del Dueño Funcional del sistema y del Propietario o Custodio de los Activos de Información involucrados.

e) Ante todo cambio significativo se debe considerar una estrategia de vuelta atrás antes de implementar los cambios, conservando versiones anteriores del software como medida de contingencia.

---

[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 6.2.4), letra b), punto i) sobre requisitos de seguridad para el desarrollo y adquisición de software.
[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 6.2.4), letra a), punto iii) sobre la protección contra código malicioso.

f) En relación con el software adquirido a terceros, se debe considerar que éste entregue asistencia para la ejecución de cambios, así como considerar el riesgo de que el proveedor deje de entregar soporte al sistema.

g) En lo relacionado a la actualización e instalación de parches en sistemas operacionales, se deben tener en cuenta los requisitos del negocio para los cambios y la seguridad de la nueva versión, es decir, considerar los problemas de seguridad que puede tener la actualización o las nuevas funciones de ésta en este contexto. Sólo se deberán aplicar parches y actualizaciones cuando éstos signifiquen una reducción de los puntos débiles de seguridad.

h) Una vez realizados los cambios sobre los sistemas operativos y software crítico de la Agencia, se debe efectuar una revisión que valide y compruebe que no existen efectos adversos para la operación y la seguridad de información. Esta revisión debe considerar:

   i. La revisión de los procesos de control y de integridad de las aplicaciones para verificar que no ha habido compromisos dado un cambio en el sistema operativo.
   ii. La garantía de que los cambios están previstos en un plazo que permita realizar pruebas y revisiones antes de la implementación del cambio en producción.

i) Los cambios en los paquetes de software deben limitarse a los cambios estrictamente necesarios y deben considerar un control estricto que considere:

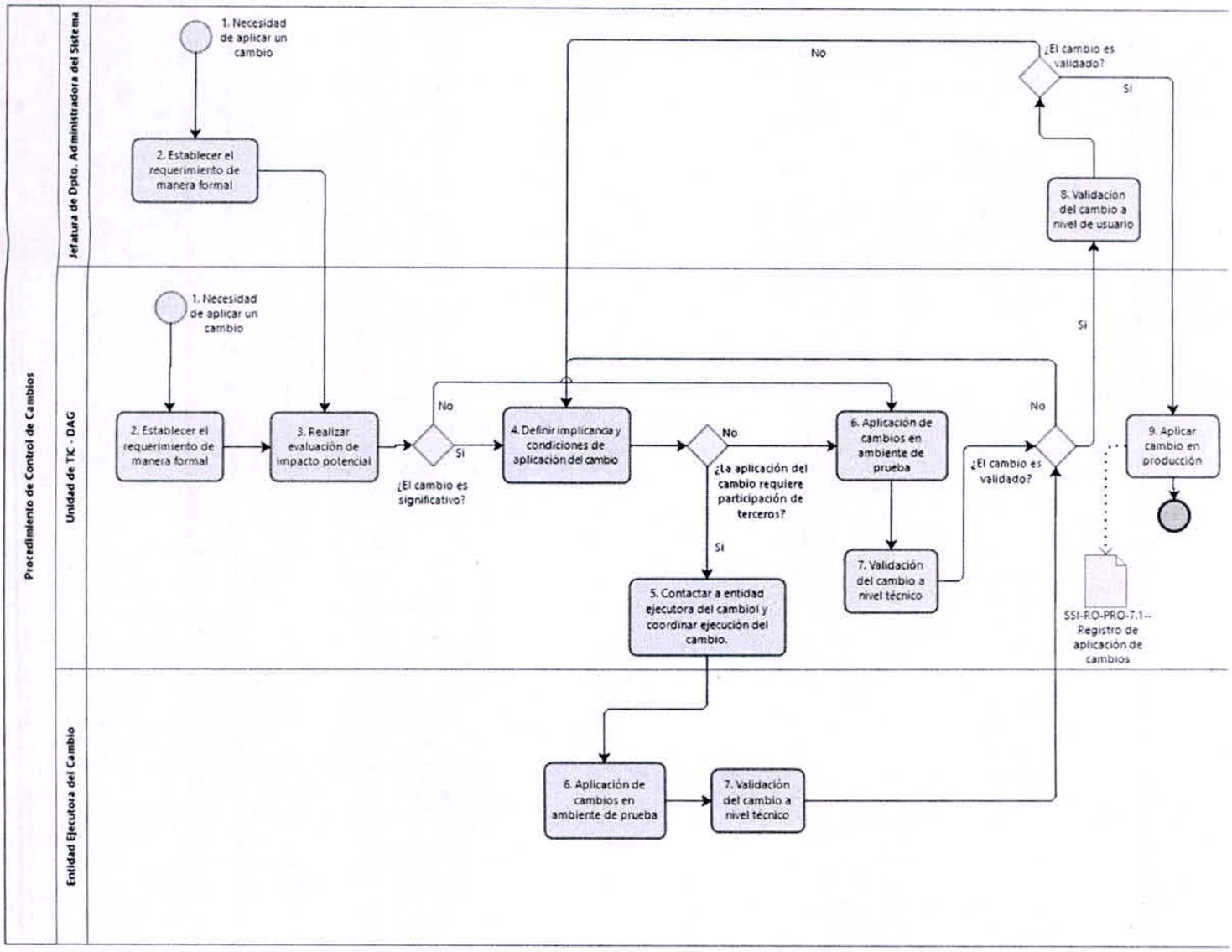
   i. El riesgo de que los controles y los procesos de integridad incorporados se vean afectados.
   ii. La necesidad de contar con la autorización del Dueño Funcional del sistema y del Propietario o Custodio de los Activos de Información involucrados. Si el sistema es de proveedor, se debe contar con su autorización, e idealmente que este realice el cambio.
   iii. La compatibilidad con otros softwares operacionales.

7. MODO DE OPERACIÓN

A continuación, se describen los flujos de actividades para los siguientes procedimientos de respaldo de información:

a) Procedimiento de control de cambios TIC.

7.1. Flujo de Procedimiento para Control de Cambios TIC.



(*) 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 6.3.1), sobre los roles y responsabilidades en el SSI.

7.2. Matriz de Procedimiento para Control de Cambios TIC.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Necesidad de aplicar un cambio	El proceso se inicia ante la necesidad de aplicación de un cambio en la infraestructura y/o software productivo de la agencia, la cual puede originarse a través de los roles que tienen rol de administradores de	Jefatura Dpto. Administradora del Sistema / Unidad de TIC	2

		los sistemas[10] de la Agencia, sean éstos Jefaturas de Departamento o la Unidad de TIC.		
2	Establecer el requerimiento de manera formal	Una vez validada la necesidad de cambio por la Jefatura de División Dueña de el o los Sistemas[11] Involucrados en el cambio, se debe hacer llegar el requerimiento a la Unidad de TIC – DAG.	Jefatura Dpto. Administradora del Sistema / Unidad de TIC	3
3	Realizar evaluación de impacto potencial	Se debe realizar una evaluación de impacto potencial del cambio según los lineamientos de este procedimiento. Se pueden dar los siguientes escenarios: - El cambio es significativo (4). - El cambio no es significativo (6).	Unidad de TIC - DAG	4 o 6
4	Definir implicancia y condiciones de aplicación del cambio	Se debe establecer el plan de ejecución del cambio, considerando los lineamientos entregados en este procedimiento, para que el Dueño Funcional del sistema y el o los Propietarios de los activos de información puedan validarlo. Se pueden dar los siguientes escenarios: - La aplicación del cambio requiere participación de terceros o externos a la Agencia (5). - La aplicación del cambio NO requiere participación de terceros o externos a la Agencia (6).	Unidad de TIC - DAG	5 o 6
5	Contactar a entidad ejecutora del cambio y coordinar ejecución del cambio.	Se debe contactar y coordinar con la entidad externa que apoyará el cambio, para gestionar todos los aspectos necesarios para la correcta ejecución del cambio.	Unidad de TIC - DAG	6
6	Aplicación de cambios en ambiente de prueba	Se debe ejecutar el cambio sobre un ambiente reducido y controlado según los lineamientos entregados en este documento.	Unidad de TIC - DAG	7

7.3. Matriz de Responsabilidades

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 control de cambios TIC:

ID	ACTIVIDAD	JEFATURA DIVISIÓN DUEÑA SISTEMA	JEFATURA DAG	JEFATURA PROP. ACTIVOS	JEFATURA DPTO. ADMIN.	UNIDAD TIC - DAG	ENC. SI / LÍDER SSI

[10] 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 6.3.1), sobre los roles y responsabilidades en el SSI.

[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 6.3.1), sobre los roles y responsabilidades en el SSI.

1	Necesidad de aplicar un cambio	-	-	-	R/E	R/E	-
2	Establecer el requerimiento de manera formal	R/A	-	-	E	E	C
3	Realizar evaluación de impacto potencial	C	R	C	C	E	C
4	Definir implicancia y condiciones de aplicación del cambio	C/A	R	C/A	C/I	E	C
5	Contactar a entidad ejecutora del cambio y coordinar ejecución del cambio.	I	R	I	I/C	E	I
6	Aplicación de cambios en ambiente de prueba	I	R	I	I	E	I
7	Validación del cambio a nivel técnico	I	R	I	I	E	I
8	Validación del cambio a nivel de usuario	R	I	C/I	E	C/I	I
9	Aplicar cambio en producción	I	R	I	I	E	I

8. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-7.1—Registro de aplicación de cambios
MANUAL / PROCEDIMIENTO	Control de cambios TIC
CONTROLES ISO 27.001	a) A.12.01.02 – Control de cambios. b) A.12.01.03 – Gestión de la capacidad. c) A.12.04.04 – Sincronización de relojes. d) A.12.05.01 – Instalación de software en sistemas operacionales. e) A.14.02.01 – Revisión de las aplicaciones después de los cambios en la plataforma de operación. f) A.14.02.01 – Revisión de las aplicaciones después de los cambios en la plataforma de operación.
RESPONSABLE	Jefatura de Unidad TIC – DAG
DESCRIPCIÓN	Corresponde al documento mediante el cual se registra el proceso de gestión de un cambio sobre las TIC de la Agencia.
FRECUENCIA	Dependerá de ejecución de cambios TIC.
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)[12].

10. ANEXOS

10.1. Anexo 1: Documento de registro de cambios TIC

Ficha de Registro de Aplicación de Cambios			
Nivel de Confidencialidad	*Medio Uso Interno*	Páginas	1 de 1
		Versión	0
Fecha versión del documento	TBD	Código	SSI-RO-PRO-7.1
Ficha de Registro de Aplicación de Cambios			

FECHA	HORA	SISTEMA O PLATAFORMA	DESCRIPCIÓN DEL CAMBIO	APROBADO POR	OBSERVACIONES

TERCERO: APRUEBASE, el Manual el Procedimiento de Respaldo de Sistemas, Software y Cuentas de Usuario de Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Evitar la pérdida de datos por indisponibilidad de la tecnología que soporta los activos de información de la Agencia.

2. ALCANCE

Se deben realizar respaldos de todos los activos de información, software y sistemas críticos 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 27.001:2013, Control A.12.3.1 – Respaldo de información

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

3. NORMAS Y REFERENCIAS

- 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 de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

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

- 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 cumplir con el objetivo de este procedimiento, se establecen dos tipos de respaldos:

a) **Respaldo de sistemas y software:** corresponde a la ejecución de respaldos a nivel de sistema operativo, base de datos y capa aplicativa de la infraestructura tecnológica de la Agencia. Requiere de definiciones por parte de las áreas funcionales dueñas de la tecnología, que serán aplicadas técnicamente por la Unidad de TIC – DAG, de forma de mantener el respaldo de información alineado con los requisitos organizacionales.

b) **Respaldo de cuentas de usuario:** corresponde a la ejecución de respaldos de las cuentas de usuario Google de la Agencia, y requiere de la adopción de los lineamientos de este procedimiento por parte de los usuarios de la Agencia para complementar la ejecución técnica del mismo por parte de la Unidad de TIC – DAG.

6.1. Lineamientos de respaldo para sistemas y software

Se debe establecer la configuración sobre el sistema o software respectivo que ejecute de forma automatizada los respaldos de información de los servidores de la Agencia bajo las siguientes condiciones:

a) Los respaldos se ejecutarán bajo una periodicidad diaria, al final de cada jornada.

b) Los respaldos se realizarán con una base incremental diaria de 15 días hábiles, o tres (3) semanas laborales de cinco (5) días corridos en horario de 5x8.

c) Para software o sistemas críticos o especiales, se consideran 20 días hábiles de base incremental, o cuatro (4) semanas laborales de cinco (5) días corridos en horario 5x8.

d) Se debe configurar el envío de un correo al Encargado de plataforma, con copia a la Jefatura de Unidad de TIC, en caso de que alguno de los respaldos falle en su ejecución ya sea automática o manual.

e) En caso de requerirse, los Líderes Internos del SSI, podrán solicitar la ejecución de respaldos sobre sistemas críticos que soporten la operación de su División, con una periodicidad menor a la detallada en los puntos anteriores.

f) Se deberá llevar a cabo de forma periódica, una prueba de respaldos que permita validar que éstos, además de realizarse conforme a lo establecido, son funcionales ante un incidente de indisponibilidad

6.2. Lineamientos de respaldo para cuentas de usuario

Dado que la Agencia posee licencia para uso de Google Workspace, lo que incluye el servicio de almacenamiento en la nube en Google Drive, se establecen los siguientes lineamientos para el respaldo automático de la información de usuarios:

a) Toda información utilizada por los usuarios en su día a día para el cumplimiento de sus responsabilidades con la Agencia debe ser almacenada únicamente en los repositorios de Google Drive correspondientes a cada usuario.

b) No se debe almacenar información personal en la nube de Google Drive de los usuarios.

c) La información almacenada en el disco local del equipamiento dispuesto para los usuarios no será respaldada de manera alguna por la institución, por lo que la pérdida parcial o total de activos de información de la Agencia es de exclusiva responsabilidad del usuario.

d) Los respaldos de los repositorios de Google Drive se realizarán de forma online y constante mediante la aplicación de sincronización de Google Drive Sync.

e) En caso de existir la necesidad, los usuarios pueden solicitar la ejecución de respaldos automáticos sobre sobre directorios específicos de sus equipos de trabajo, lo cual deberá ser aplicado por la Unidad de TIC mediante la aplicación de sincronización de Google Drive Sync.

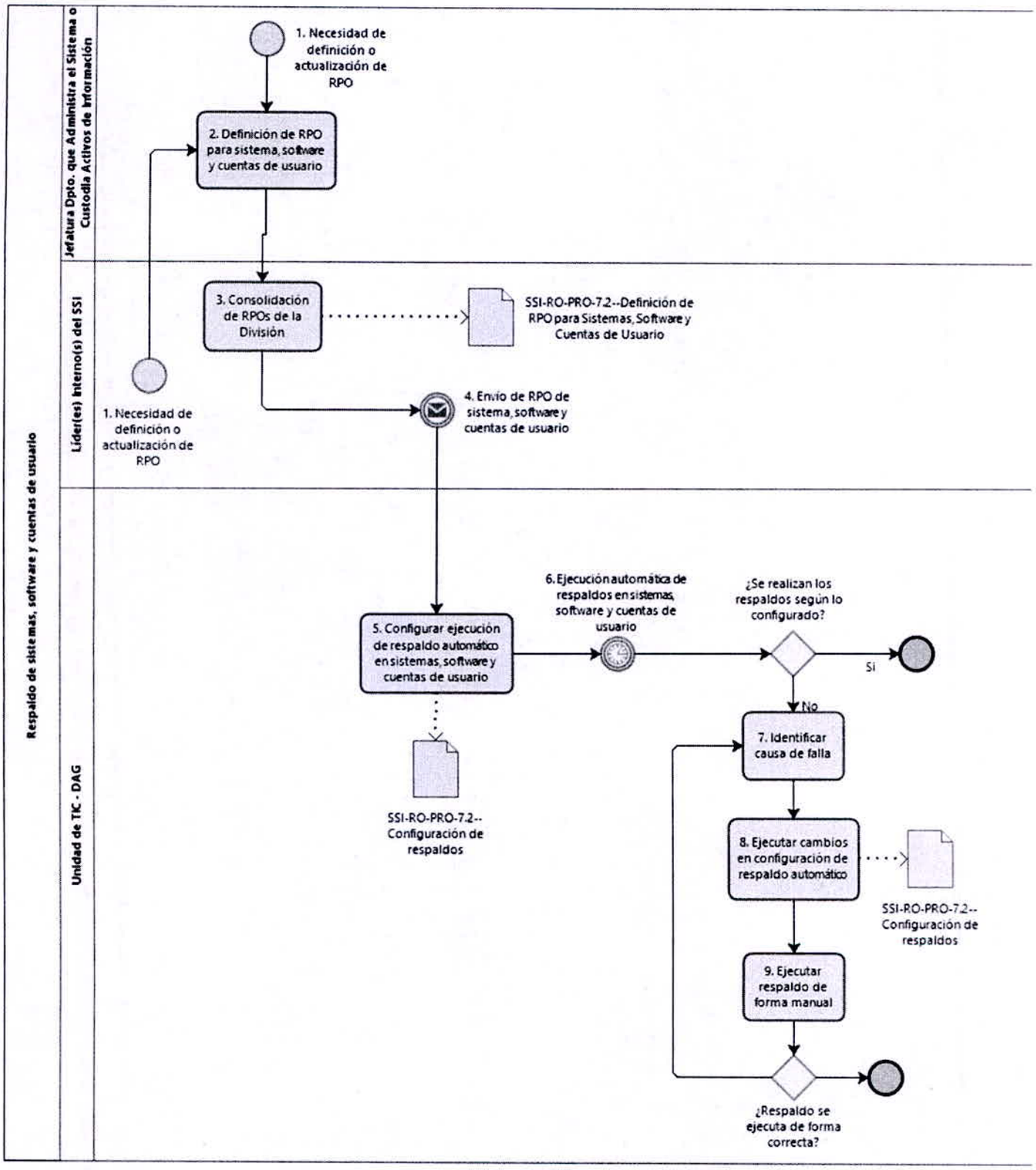
7. MODO DE OPERACIÓN

A continuación, se describen los flujos de actividades para los siguientes procedimientos de respaldo de información:

a) Procedimiento de respaldo de sistemas, software y cuentas de usuario.

b) Procedimiento de prueba de respaldos

7.1. Flujo de Procedimiento para respaldo de sistemas, software y cuentas de usuario

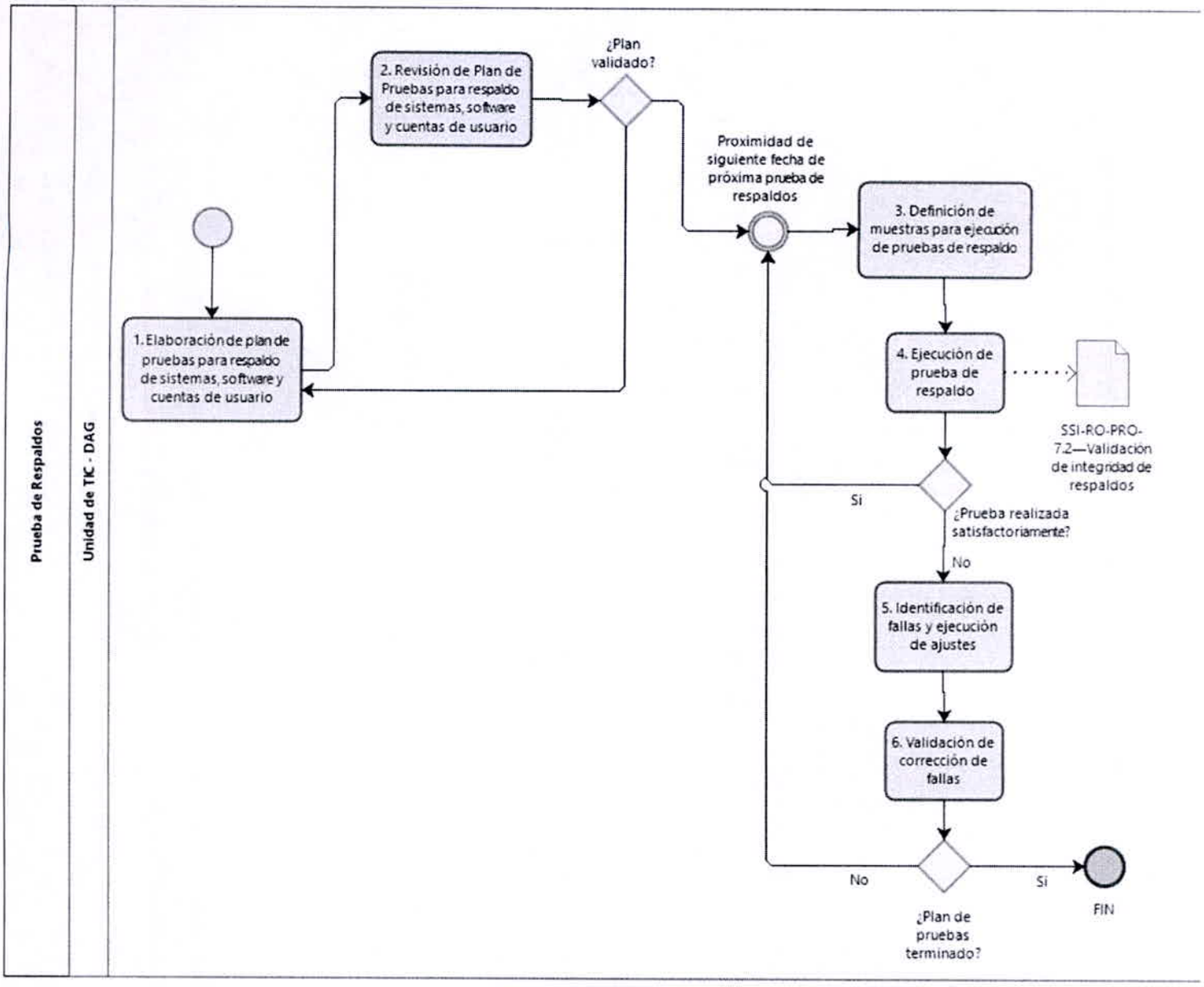


7.2. Matriz de Procedimiento para respaldo de sistemas y software

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Necesidad de definición o actualización de RPO[13]	El procedimiento se gatilla dada la necesidad de definir y/o actualizar el Punto de Recuperación Objetivo (RPO), o frecuencia de respaldos de algún sistema, software o cuenta de usuario.	Líder(es) Interno(s) del SSI / Departamento que Administra el Sistema o que Custodia los Activos de Información	2
2	Definición de RPO para sistema, software y cuentas de usuario	Se debe definir el RPO para los sistemas, softwares y cuentas de usuario de la División, lo que definirá a su vez la periodicidad de los respaldos de cada uno de éstos.	Jefatura de Departamento que Administra el Sistema o que Custodia los Activos de Información	3
3	Consolidación de RPOs de la División	Se deberán recolectar y consolidar los RPO de los sistemas, software y cuentas de usuario de la División.	Líder(es) Interno(s) del SSI	4
4	Envío de RPO de sistemas, software y cuentas de usuario	Una vez consolidados los RPO de la División, se debe enviar al Equipo de Soporte e Infraestructura de la Unidad de TIC – DAG para que los respaldos sean configurados en función de los RPO.	Líder(es) Interno(s) del SSI	5
5	Configurar ejecución de respaldo automático en sistema, software y cuentas de usuario	Se deben configurar los respaldos según los requerimientos de RPO recibidos. Esta acción deberá reflejarse en la configuración de los sistemas, software y cuentas de usuario involucradas.	Unidad de TIC - DAG	6
6	Ejecución automática de respaldos en sistemas, software y cuentas de usuario	Cada uno de los sistemas, softwares y cuentas de usuario ejecutan sus respaldos según la periodicidad y tipo configurados. Se pueden dar las siguientes condiciones: - La totalidad de los respaldos se ejecutaron de forma correcta (FIN). - Uno o varios respaldos no se ejecutaron de forma correcta (7).	Ejecución automática por cada sistema / software	7 o FIN
7	Identificar causa de falla	Para los sistemas, software y cuentas de usuario que no hayan ejecutado de forma correcta sus respaldos, se deberán identificar las causas de falla para corregir la configuración de respaldo respectiva.	Unidad de TIC - DAG	8
8	Ejecutar cambios en configuración de respaldo automático	Se deben ejecutar los cambios necesarios en la configuración de los sistemas, software y cuentas de usuario para evitar fallas futuras de ejecución del respaldo automático. Se deberá actualizar el Registro de Configuración de Respaldos Automáticos de la Unidad de TIC.	Unidad de TIC - DAG	9
9	Ejecutar respaldo de forma manual	Se deberá ejecutar manualmente el o los respaldos fallidos. Se pueden dar las siguientes condiciones: - El respaldo se ejecuta de forma correcta (FIN). - La ejecución del respaldo sigue presentando fallas (7).	Unidad de TIC - DAG	7 o FIN

[13] Punto de recuperación objetivo.

7.3. Flujo de Procedimiento para prueba de respaldos



7.4. Matriz de Procedimiento para prueba de respaldos

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Elaboración de plan de pruebas para respaldo de sistemas, software y cuentas de usuario	De manera anual, se debe elaborar un plan de pruebas para validar el correcto funcionamiento de los respaldos de sistemas, software y cuentas de usuario, según la definición de RPO de cada División. Este plan debe abarcar la totalidad de los sistemas productivos de la Agencia durante el transcurso de un año.	Unidad de TIC - DAG	2
2	Revisión de plan de pruebas para respaldo de	Se debe validar el plan de pruebas para respaldos. Se pueden dar las siguientes opciones:	Unidad de TIC - DAG	1 o 3

	sistemas, software y cuentas de usuario	- El plan no es validado (1). - El plan es validado (3)		
3	Definición de muestras para ejecución de pruebas de respaldo	En función del plan de respaldos, se deben seleccionar las muestras sobre las cuales se ejecutarán las pruebas respectivas. Esta selección de muestras puede considerar sistemas, aplicaciones, bases de datos, cuentas de usuario tanto para Google Drive como para correo electrónico, entre otros a fin.	Unidad de TIC - DAG	4
4	Ejecución de prueba de respaldo	Se deben restaurar los respaldos de las muestras seleccionadas en la actividad anterior, de forma de validar que éstos se encuentran operativos e íntegros, y por ende cumplen con el objetivo de minimizar el impacto de la pérdida de información y datos ante una incidencia. Se pueden dar los siguientes escenarios: - La totalidad de respaldos pasa las pruebas de manera exitosa (3). - Uno o varios respaldos presentan problemas para ser restaurado (5).	Unidad de TIC - DAG	5
5	Identificación de fallas y ejecución de ajustes	Se deben identificar las causas que generan que la restauración de los respaldos falle, para posteriormente aplicar los cambios y configuraciones necesarios para que ese problema no se repita. Se debe validar también si este problema se presenta en otros respaldos del mismo sistema, software o cuenta de usuario.	Unidad de TIC - DAG	6
6	Validación de corrección de fallas	Se debe validar que los nuevos respaldos sean restaurables una vez aplicados los cambios para corrección de las fallas obtenidas al aplicar las pruebas de restauración de respaldo. Esta validación puede incluir, más no limitarse a la repetición de la prueba de respaldo al día siguiente con el nuevo respaldo diario ya ejecutado. Una vez validada la corrección de las fallas, pueden darse los siguientes escenarios: - Esta es la última prueba del plan de pruebas anual se da por cerrado (FIN) - Aún quedan más pruebas que realizar durante el año (3).	Unidad de TIC - DAG	3 o FIN

7.5. Matriz de Responsabilidades

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 respaldo de sistemas, software y cuentas de usuario se distribuye de la siguiente forma:

ID	ACTIVIDAD	JEFATURA DIVISIÓN DUEÑA DE SISTEMA O PROP. ACTIVOS INFO.	JEFATURA DAG	JEFATURA DPTO. ADMIN. DE SISTEMA O CUSTODIO DE ACTIVOS INFO.	UNIDAD DE TIC - DAG	LÍDER INTERNO SSI	ENC. CIBER
1	Necesidad de definición o actualización de RPO	R	-	E	-	E	C
2	Definición de RPO para sistema, software y cuentas de usuario	R	-	E	-	C	C
3	Consolidación de RPOs de la División	R	-	C	-	E	I
4	Envío de RPO de sistemas, software y cuentas de usuario	R	-	C	I	E	I
5	Configurar ejecución de respaldo automático en sistema, software y cuentas de usuario	-	R	I/C	E	I	C
6	Ejecución automática de respaldos en sistemas, software y cuentas de usuario	-	R	-	-	-	-
7	Identificar causa de falla	I	R	I/C	E	I/C	C
8	Ejecutar cambios en configuración de respaldo automático	-	R	I/C	E	I	C
9	Ejecutar respaldo de forma manual	I	R	I/C	E	I/C	C

Adicionalmente, la matriz de responsabilidades para el procedimiento de prueba de respaldos de sistemas, software y cuentas de usuario se distribuye de la siguiente manera:

ID	ACTIVIDAD	JEFATURA DAG	UNIDAD TIC - DAG	JEFATURA DPTO. ADMIN. DE SISTEMA	LÍDER INTERNO SSI	ENC. CIBER
1	Elaboración de plan de pruebas para respaldo de sistemas, software y cuentas de usuario	R	E	-	-	-
2	Revisión de plan de pruebas para respaldo de sistemas, software y cuentas de usuario	R	E	I	I	I
3	Definición de muestras para ejecución de pruebas de respaldo	R	E	I	I	I
4	Ejecución de prueba de respaldo	R	E	I	I	I
5	Identificación de fallas y ejecución de ajustes	R	E	I	I	I
6	Validación de corrección de fallas	R	E	I	I	I

8. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-7.2—Validación de integridad de respaldos
PROCEDIMIENTO	Pruebas de Respaldo
CONTROLES ISO 27.001	• A.12.3.1 – Respaldo de información
RESPONSABLE	Jefatura de Unidad TIC - DAG

DESCRIPCIÓN	La ejecución del procedimiento arrojará como registro de operación un plan con el estado de las pruebas sobre respaldos, que en la medida que se vaya ejecutando deberá ser completado.
FRECUENCIA	Dependerá de las definiciones establecidas en el plan de pruebas de respaldo
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-7.2—Definición de RPO para sistemas, software y cuentas de usuario
PROCEDIMIENTO	Respaldo de sistemas, software y cuentas de usuario
CONTROLES ISO 27.001	• A.12.3.1 – Respaldo de información
RESPONSABLE	Jefatura División o a quien ésta designe
DESCRIPCIÓN	Correo con la definición del Punto de Recuperación Objetivo (RPO) de los sistemas, software y cuentas de usuario de la División
FRECUENCIA	Este registro de operación se deberá obtener en función de las necesidades de definición o actualización de los RPO de los sistemas, software y cuentas de usuario de la División.
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-7.2—Registro de configuración de respaldos automáticos
PROCEDIMIENTO	Respaldo de sistemas, software y cuentas de usuario
CONTROLES ISO 27.001	A.12.3.1 – Respaldo de información.
RESPONSABLE	Jefatura Unidad TIC - DAG
DESCRIPCIÓN	Corresponde a las capturas de pantalla que validan que la configuración de respaldo automático se condice con las definiciones establecidas por las Divisiones
FRECUENCIA	La obtención del registro de operación dependerá de la frecuencia de los cambios en la configuración de respaldo de los sistemas, software y cuentas de usuario.
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)[14].

CUARTO: el Procedimiento de Gestión de Vulnerabilidades Técnicas de Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Reducir los riesgos resultantes de la explotación de vulnerabilidades en la infraestructura tecnológica de la Agencia.

2. ALCANCE

Este procedimiento aplica sobre todo tipo de vulnerabilidades técnicas presentes en la infraestructura tecnológica de la Agencia, independiente de su origen o metodología de descubrimiento.

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

- ISO/IEC 27.001:2013, Control A.12.6.1 – Gestión de vulnerabilidades técnicas.

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 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

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

La gestión de vulnerabilidades es un proceso cíclico que debe ejecutarse de forma recurrente para abarcar la infraestructura crítica de la Agencia de forma lo más completa posible. La tecnología es un ecosistema dinámico, que cambia en el tiempo a nivel de configuraciones, actualizaciones y cambios dados por requisitos propios del negocio, y, por ende, ejecutar una sola vez de este procedimiento, o entre períodos prolongados de tiempo, apalancará la remediación de vulnerabilidades correspondientes a un momento

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

específico, más no permitirá mitigar de manera efectiva los riesgos asociados a la explotación de vulnerabilidades.
En base a lo anterior, se deben considerar las siguientes directrices para la ejecución de este procedimiento:

a) Se debe contar con un inventario de sistemas tecnológicos productivos que permita definir el alcance específico para las iteraciones de descubrimiento de vulnerabilidades. Para esto, se debe considerar el principio de gestión de activos establecido en la Política General de Seguridad de Información (SSI-POL-01)[15].

b) El procedimiento de gestión de vulnerabilidades contempla desde las actividades de descubrimiento, hasta las actividades de remediación y retest para validar su remediación, es decir, contempla la gestión completa de la brecha o vulnerabilidad.

c) El descubrimiento de vulnerabilidades puede darse bajo ejercicios de ethical hacking, análisis de vulnerabilidades, reportes externos de vulnerabilidades, entre otros, y, por ende, el flujo de procedimiento debe ser capaz de lograr una gestión y remediación efectiva de las brechas y vulnerabilidades independiente de su origen.

d) Al momento de calendarizar los ejercicios de descubrimiento de vulnerabilidades, se debe velar por afectar lo menos posible la operación de la Agencia.

e) Dada la criticidad que reviste la ejecución de las remediaciones para mitigar las vulnerabilidades descubiertas, estas actividades deben ser llevadas a cabo por equipos internos de la Agencia. Para el caso de que se requiera ayuda de un proveedor para la remediación, estas actividades deben ser coordinadas y gestionadas por los equipos internos de la Agencia.

f) Previo a la ejecución de actividades de remediación, se debe establecer una priorización de las vulnerabilidades de forma de optimizar la remediación de éstas.

g) En caso de descubrirse una vulnerabilidad de alta criticidad o que pueda ser considerada un evento de seguridad, debe ser reportada de forma inmediata a los equipos y roles respectivos. Todo lo anterior según lo especificado en el Procedimiento de Respuesta ante Incidentes de Seguridad (SSI-PRO-5.1)[16].

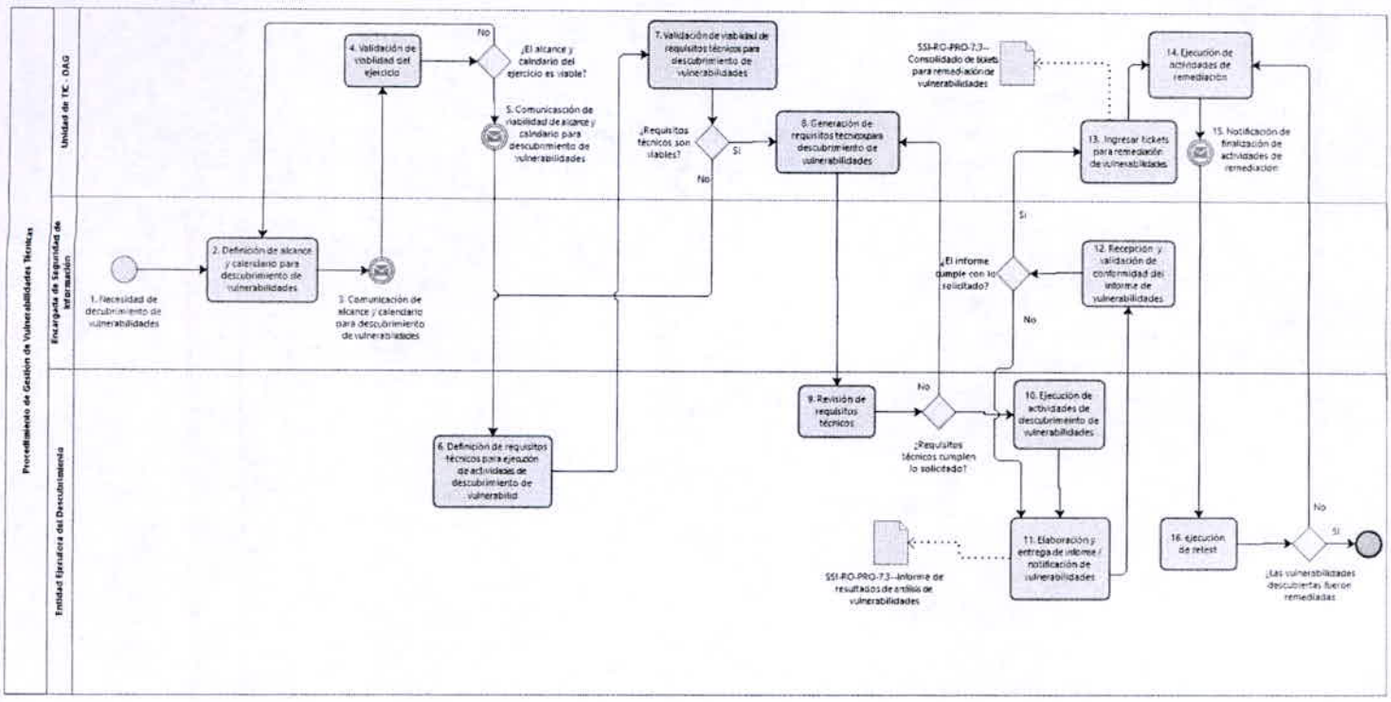
7. MODO DE OPERACIÓN

A continuación, se describen los flujos de actividades para los siguientes procedimientos:

a) Procedimiento de Gestión de Vulnerabilidades Técnicas.

[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 6.2.2), letra a), punto i) sobre la elaboración y actualización del inventario de activos de información.
[16] Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.

7.1. Flujo de Procedimiento para Gestión de Vulnerabilidades Técnicas



7.2. Matriz de Procedimiento para Gestión de Vulnerabilidades Técnicas

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Necesidad de descubrimiento de vulnerabilidades	El procedimiento parte al momento en que se requiere, ya sea por calendarización de la Agencia o por necesidades específicas, la ejecución de actividades de descubrimiento de vulnerabilidades.	Encargada de Seguridad de Información	2
2	Definición de alcance y calendario para descubrimiento de vulnerabilidades	Se debe definir un alcance específico a nivel de sistemas productivos de la Agencia para ejecutar el descubrimiento de vulnerabilidades, así como definir el período de días que se considerarán para este. Lo anterior siguiendo los lineamientos descritos en este documento.	Encargada de Seguridad de Información	3
3	Comunicación de alcance y calendario para descubrimiento de vulnerabilidades	Una vez definidos, se debe comunicar el alcance y calendarización del ejercicio a la Unidad de TIC.	Encargada de Seguridad de Información	4
4	Validación de viabilidad del ejercicio	Se debe validar la viabilidad del alcance y calendario para la realización del ejercicio, velando por afectar lo menos posible la operación tecnológica de la	Unidad de TIC - DAG	2 o 5

		Agencia. Se pueden dar los siguientes escenarios: - El calendario y alcance no son validados (2). - El calendario y alcance son validados (5).		
5	Comunicación de viabilidad de alcance y calendario para descubrimiento de vulnerabilidades	Se debe comunicar el calendario y alcance del ejercicio a la Entidad Ejecutora del mismo.	Unidad de TIC - DAG	6
6	Definición de requisitos técnicos para ejecución de actividades de descubrimiento de vulnerabilidad	Se deben definir los requisitos técnicos necesarios para la ejecución del ejercicio, lo que puede incluir, más no limitarse a cuentas de usuario, configuración de firewall, entre otros.	Entidad Ejecutora[17]	7
7	Validación de viabilidad de requisitos técnicos para descubrimiento de vulnerabilidades	Se debe validar la viabilidad de los requisitos técnicos necesarios para la ejecución del ejercicio de descubrimiento de vulnerabilidades. Se pueden dar los siguientes escenarios: - Los requisitos técnicos no son viables (6). - Los requisitos técnicos son viables (8).	Unidad de TIC - DAG	6 u 8
8	Generación de requisitos técnicos para descubrimiento de vulnerabilidades	Se deben ejecutar las actividades y gestiones necesarias para la generación de los requisitos técnicos necesarios para la ejecución del ejercicio.	Equipo Soporte / Equipo Desarrollo – Unidad de TIC	9
9	Revisión de requisitos técnicos	Se debe revisar que los requisitos técnicos entregados sean correctos y permitan la correcta ejecución del ejercicio.	Entidad Ejecutora	8 o 10
10	Ejecución de actividades de descubrimiento de vulnerabilidades	Se deben ejecutar las actividades de descubrimiento acorde al alcance y el calendario definido.	Entidad Ejecutora	11
11	Elaboración y entrega de informe / notificación de vulnerabilidades	Una vez ejecutadas las actividades se debe elaborar y entregar un informe de resultados para su posterior remediación. En caso de descubrirse una vulnerabilidad de alto riesgo o crítica, debe ser notificada de inmediato para su remediación por parte de la Agencia.	Entidad Ejecutora	12
12	Recepción y validación de conformidad del informe de vulnerabilidades	Una vez recibido el informe de vulnerabilidades por parte de la Entidad Ejecutora, se debe validar la conformidad del mismo para posteriormente ser enviado a la	Encargada de seguridad de información	11 o 13

[17] Se define Entidad ejecutora como el equipo que ejecuta las actividades de descubrimiento de vulnerabilidades, independiente si éste pertenece a la Unidad de TIC de la Agencia o es externo a la institución

		Unidad de TIC – DAG para comenzar la remediación de hallazgos. Se pueden dar los siguientes escenarios: - El informe NO está conforme a lo solicitado (11). - El informe está conforme a lo solicitado (13).		
13	Ingresar tickets para remediación de vulnerabilidades	Una vez recibidas las vulnerabilidades descubiertas, se deben ingresar al sistema de tickets para poder hacer gestión interna sobre su remediación.	Unidad de TIC - DAG	14
14	Ejecución de actividades de remediación	Se deben ejecutar las actividades de remediación para mitigar los riesgos que estas suponen.	Unidad de TIC – DAG	15
15	Notificación de finalización de actividades de remediación	Se debe notificar cuando las actividades de remediación finalicen para proceder a la revisión de éstas.	Unidad de TIC - DAG	16
16	Ejecución de retest	Se debe repetir el ejercicio de descubrimiento de vulnerabilidades para validar que las vulnerabilidades descubiertas hayan sido efectivamente remediadas. Se pueden dar los siguientes escenarios: - Las vulnerabilidades no han sido completamente remediadas (13). - Las vulnerabilidades han sido remediadas (FIN).	Entidad Ejecutora	14 o 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 DAG	UNIDAD DE TIC – DAG	ENTIDAD EJECUTORA
1	Necesidad de descubrimiento de vulnerabilidades	R/E	-	C	-
2	Definición de alcance y calendario para descubrimiento de vulnerabilidades	R/E	-	C	-
3	Comunicación de alcance y calendario para	R/E	I	I	-

	descubrimiento de vulnerabilidades				
4	Validación de viabilidad del ejercicio	C	R	E	-
5	Comunicación de viabilidad de alcance y calendario para descubrimiento de vulnerabilidades	I	R	E	I
6	Definición de requisitos técnicos para ejecución de actividades de descubrimiento de vulnerabilidad	I/C	R	E	E
7	Validación de viabilidad de requisitos técnicos para descubrimiento de vulnerabilidades	A	R	E	C
8	Generación de requisitos técnicos para descubrimiento de vulnerabilidades	I	R	E	I/C
9	Revisión de requisitos técnicos	I	R	E	E
10	Ejecución de actividades de descubrimiento de vulnerabilidades	I	R	E	E
11	Elaboración y entrega de informe / notificación de vulnerabilidades	I	R	E	E
12	Recepción y validación de conformidad del informe de vulnerabilidades	R/E	I	C	C
13	Ingresar tickets para remediación de vulnerabilidades	I	R	E	I
14	Ejecución de actividades de remediación	I	R	E	C
15	Notificación de finalización de actividades de remediación	I	R	E	C
16	Ejecución de retest	I	R	E	E

8. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-7.3—Informe de resultados de descubrimiento de vulnerabilidades.
MANUAL / PROCEDIMIENTO	Gestión de Vulnerabilidades Técnicas
CONTROLES ISO 27.001	• A.12.6.1 – Gestión de vulnerabilidades técnicas
RESPONSABLE	Encargada de Seguridad de Información

DESCRIPCIÓN	Corresponde al informe de ejecución de labores técnicas para descubrimiento de vulnerabilidades.
FRECUENCIA	En función de la ejecución de este procedimiento.
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	**DESCRIPCIÓN**
NOMBRE	SSI-RO-PRO-7.3—Consolidado de tickets para gestión de vulnerabilidades.
MANUAL / PROCEDIMIENTO	Gestión de Vulnerabilidades Técnicas
CONTROLES ISO 27.001	A.12.6.1 – Gestión de vulnerabilidades técnicas
RESPONSABLE	Jefatura Unidad TIC
DESCRIPCIÓN	Corresponde al consolidado de tickets mediante los cuales se lleva la gestión de remediación de vulnerabilidades técnicas.
FRECUENCIA	En función de la ejecución de este procedimiento.
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 de 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)[18].

QUINTO: APRUEBASE, el Manual de Protección Contra Código Malicioso de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Establecer los lineamientos para detectar oportunamente código malicioso que afecte la infraestructura tecnológica de la Agencia.

2. ALCANCE

La protección contra código malicioso debe ser aplicada a todos los servidores tecnológicos y estaciones de trabajo que sean administrados por la Unidad de TIC 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.12.02.01 – Protección contra código malicioso

3. NORMAS Y REFERENCIAS

a) 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

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

Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

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°587, de 2021, de la Agencia de Calidad de la Educación, que aprueba la actualización y creación de los manuales y procedimientos asociados con el principio de gestión de activos y transferencia de información.

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) **Jefatura División de Administración General (DAG):** 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) **Jefatura de la Unidad de TIC – DAG:** ejecutar y dar 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.

c) **Encargada de Seguridad de la 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 DAG	UNIDAD DE TIC - DAG	ENC. SI / CIBERSEGURIDAD
RESPONSABLE	X		
EJECUTOR		X	
CONSULTADO			X
INFORMADO			

6. LINEAMIENTO DEL MANUAL

La Agencia, deberá implementar herramientas corporativas, que, siendo administradas de manera regular y constante por los roles respectivos de la institución, debe brindar las siguientes capacidades de detección frente a código malicioso o malware por el acrónimo en inglés para *malicius software*:

a) Detectar de manera oportuna la instalación de software que posea indicadores de compromiso asociados a comportamientos maliciosos tanto en estaciones de trabajo como en servidores de la infraestructura TIC.

b) Escanear de manera constante, automática y rutinaria los equipos y servidores de la Agencia en busca de posible código malicioso.

c) Detectar la existencia de código malicioso, antes de su uso, en cualquier fichero recibido a través de las redes informáticas o vía cualquier forma de soporte electrónico u óptico, como dispositivos USB, discos duros externos, o CDs.

d) Detectar la existencia de código malicioso, antes de su uso, en los adjuntos al correo electrónico y las descargas.

e) Comprobación de páginas web para detectar código o comportamiento malicioso.

Para lograr las capacidades de detección anteriores, se debe garantizar que la o las herramientas de protección contra código malicioso son administradas correctamente, para lo cual se deben tener en cuenta los siguientes lineamientos:

a) Se debe garantizar la actualización de la base de datos de firma y/o heurística de la o las herramientas antimalware al menos diariamente.

b) Cuando las herramientas de protección contra código malicioso lo permitan, se debe mantener actualizado el registro de dominios y direcciones IP bloqueados por asociación a indicadores de compromiso, o que se sospecha pueden generar comportamiento malicioso.

c) Cuando las herramientas de protección contra código malicioso lo permitan, se debe mantener actualizado el registro de software autorizado en el equipamiento de la Agencia, de manera de detectar cualquier intento de instalación de aplicaciones no autorizadas que puedan suponer un riesgo para la organización.

Así mismo, para una correcta gestión de las herramientas o mecanismos de protección contra código malicioso, se debe procurar mantener actualizado el inventario de equipos asignados al personal de la agencia, según lo estipulado en el Procedimiento de Entrega y Devolución de Equipos (SSI-MAN-3.3)[19]. Lo anterior permitirá mantener un panel de control "limpio" para este tipo de herramientas, optimizando la detección de equipos que puedan no tener al día la actualización de la base de datos del sistema antimalware, la detección de alertas asociadas a posibles infecciones por código malicioso, y la detección de falsos positivos asociados a los indicadores que define esta manual.

6.1. Medidas complementarias a la detección mediante herramientas de protección contra código malicioso

Dado que las medidas descritas anteriormente están enfocadas en la detección de código malicioso, se deben considerar procesos complementarios para la prevención de este tipo de amenazas. De esta forma, la siguiente tabla muestra la relación de estos procesos de control y su relación con el set documental del SSI de la ACE:

PROCESO DE CONTROL COMPLEMENTARIO	REFERENCIA A DOCUMENTO DEL SSI

[19] Resolución Exenta N°587, de 2021, de la Agencia de Calidad de la Educación, que aprueba la actualización y creación de los manuales y procedimientos asociados con el principio de gestión de activos y transferencia de información.

Reducción de vulnerabilidades potencialmente explotables por software malicioso.	• Procedimiento de gestión continua de vulnerabilidades técnicas (SSI-PRO-7.3)[20].
Control del software y datos contenidos en los sistemas que soportan los activos de información críticos de la Agencia, de forma de impedir la presencia de ficheros no aprobados o modificaciones no autorizadas.	• Procedimiento de Control de Cambios TIC (SSI-PRO-7.1)[21]. • Procedimiento de Desarrollo Seguro y Soporte (SSI-PRO-7.5)[22].
Aplicación de protocolos de respuesta y recuperación para reaccionar ante incidentes de infección por código malicioso.	• Procedimiento de respuesta ante incidentes de ciberseguridad (SSI-PRO-5.1)[23]. • Procedimiento de respaldos de información (SSI-PRO-7.2)[24].
Establecimiento de lineamientos para comportamiento de usuarios y acceso a la información y recursos de la organización.	• Manual de responsabilidades del usuario en el acceso a la información (SSI-MAN-4.3)[25].
Monitoreo de uso de recursos de la infraestructura tecnológica de la Agencia para detección de comportamientos anómalos asociados a código malicioso.	• Manual de Seguridad en Operaciones TIC (SSI-MAN-7.1)[26].

7. REGISTRO DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-7.2--Cobertura de herramienta antimalware en equipos.
MANUAL	Protección contra código malicioso
CONTROLES ISO 27.001	A.12.02.01 – Protección contra código malicioso
RESPONSABLE	Jefe Unidad TIC - DAG
DESCRIPCIÓN	Corresponde a la captura de pantalla del panel de control de la herramienta antimalware, en la cual se indica la cantidad de equipos de usuario que cuentan con la actualización de la base de datos.
FRECUENCIA	Mensual
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-7.2--Cobertura de herramienta antimalware en servidores.
MANUAL	Protección contra código malicioso
CONTROLES ISO 27.001	A.12.02.01 – Protección contra código malicioso

[20] 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 vi) sobre la gestión de vulnerabilidades técnicas.
[21] 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 iv) sobre la gestión de cambios TIC.
[22] 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 b), punto ii) sobre la gestión en el proceso de desarrollo y mantención de software.
[23] Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.
[24] 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 b), punto ii) sobre la gestión en el proceso de desarrollo y mantención de software.
[25] 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.
[26] 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 i) sobre la seguridad en las operaciones TIC.

RESPONSABLE	Jefe Unidad TIC - DAG
DESCRIPCIÓN	Corresponde a la captura de pantalla del panel de control de la herramienta antimalware, en la cual se indica la cantidad de servidores que cuentan con la actualización de la base de datos.
FRECUENCIA	Mensual
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) [27].

SEXTO: APRUEBASE, el Procedimiento de Gestión para el Desarrollo y Mantención de Software de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Establecer el flujo de actividades que permitan incorporar la seguridad de la información durante el ciclo de vida de desarrollo del software.

2. ALCANCE

Este procedimiento debe ser aplicado para todos los requerimientos de desarrollo, adquisición y mantención de software 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 27.001:2013, Control A.14.02.02 – Procedimiento de control de cambio en el sistema.

b) ISO/IEC 27.001:2013, Control A.14.02.04 – Restricciones de cambio a los paquetes de software.

c) ISO/IEC 27.001:2013, Control A.14.02.08 – Prueba de seguridad del sistema.

d) ISO/IEC 27.001:2013, Control A.14.02.09 – Prueba de aprobación del sistema.

e) ISO/IEC 27.001:2013, Control A.14.03.01 – Protección de datos de prueba.

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 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

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

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°1612, de 2019, de la Agencia de Calidad de la Educación, aprueba la Política de Seguridad de Información para Relación con Proveedores de la Agencia de Calidad de la Educación.

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

A nivel general, el ciclo de vida de desarrollo de software considera las siguientes fases:

a) Análisis y definición de requerimientos.
b) Diseño del producto.
c) Desarrollo o codificación.
d) Pruebas y validación del producto.
e) Puesta en producción.

Las fases de desarrollo anteriores pueden ser abordadas en base a diferentes metodologías, dependiendo del proyecto o tipo de requerimiento al que esté asociado el nuevo software o nueva funcionalidad de un software existente en la Agencia.

Así mismo, es necesario que, durante todas las fases del desarrollo de software, se considere la participación del negocio, considerando, pero no limitándose a los dueños funcionales y administradores del software, y los propietarios o custodios de los activos de información que serán procesados, almacenados o transferidos por el nuevo software o la nueva funcionalidad de un software existente.

En complemento, cuando un desarrollo es apoyado por terceros o proveedores, se deberán aplicar los lineamientos establecidos en la Política de Seguridad en la Relación con Proveedores (SSI-POL-08)[28].

6.1. Seguridad en la fase de análisis y definición de requerimientos

La inclusión de requisitos de seguridad para nuevos desarrollos es abordada en el principio de seguridad en la gestión de tecnologías de información y comunicación (TIC) establecido en la Política General de Seguridad de Información (SSI-POL-01)[29].

[28] ·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.
[29] 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 b), punto i) sobre requisitos de seguridad para el desarrollo y mantención de software.

6.2. Seguridad en la fase de diseño

En función de los requerimientos funcionales que considera el desarrollo, y los requisitos de seguridad definidos para éste, se debe elaborar un diseño de la solución que considere los siguientes lineamientos de seguridad:

a) El diseño de la solución debe considerar los requisitos tanto funcionales como de seguridad establecidos para el proyecto.

b) El diseño de la solución debe considerar como input al menos los siguientes recursos:

   i. OWASP top 10 de riesgos: Define los 10 riesgos más comunes en el desarrollo de software, y ayudará a identificar aquellos aspectos de seguridad que deben ser subsanados desde el diseño del producto.
   ii. OWASP top 10 de controles: Define los 10 controles necesarios para mitigar los riesgos definidos en el OWASP top 10 de riesgos, y ayudará a diseñar un producto que considere de base estas medidas de mitigación.
   iii. Guía Técnica para el Desarrollo de Software de Gobierno Digital, que define aspectos base para el diseño de productos de software en entidades de gobierno.

c) Se puede complementar el diseño de la solución con un modelamiento de amenazas, de forma de identificar proactivamente en esta etapa temprana del desarrollo de software, que se han identificado y considerado en el diseño, los requisitos de seguridad para el desarrollo de software.

d) El diseño de la solución o nueva funcionalidad debe contar con la participación activa del rol dueño funcional del sistema o software, así como del propietario/ custodio de los activos de información involucrados.

6.3. Seguridad en la fase de desarrollo o codificación

La construcción o codificación del software deberá alinearse a las definiciones de seguridad establecidas en las fases anteriores de definición de requerimientos y diseño. En complemento, deberá considerar los siguientes lineamientos:

a) Se deben seguir estándares y buenas prácticas de codificación en función de los lenguajes de programación escogidos para el proyecto.

b) Se deberán utilizar los frameworks de desarrollo con mayor madurez del mercado, para lo cual se debe seguir la Guía Técnica para el Desarrollo de Software de Gobierno Digital.

c) Se deberá utilizar un repositorio de código fuente para gestionar el avance y modificaciones al mismo mientras dure esta fase del ciclo de vida del software. Este lineamiento deberá ser aplicado tanto si el desarrollo es interno como si es apoyado por proveedores, de forma de que el código fuente del programa, como activo de información, siempre se encuentre bajo la gestión y seguridad de la Agencia.

d) Para establecer un ambiente de desarrollo seguro, se deben seguir el principio de seguridad en la gestión de tecnologías de información y comunicación (TIC) establecido en la Política General de Seguridad de Información (SSI-POL-01)[30].

[30] 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 b), punto i) sobre requisitos de seguridad para el desarrollo y mantención de software.

6.4. Seguridad en la fase de pruebas y validación del producto

Es de carácter obligatoria la ejecución de pruebas sobre los nuevos desarrollos, de forma de validar si tanto los aspectos funcionales que requiere el negocio fueron correctamente abordados, como para garantizar que el software cumple con los requisitos mínimos de seguridad para ser puesto en producción y que garantice la operación y seguridad de información. Los lineamientos de seguridad para esta fase son los siguientes:

a) Es obligatoria la planificación y ejecución de pruebas de seguridad sobre los nuevos desarrollos, previo a su puesta en producción. Estas pruebas deben considerar:

   i. Pruebas de seguridad funcional durante el desarrollo: Los sistemas nuevos y actualizados requieren pruebas y verificación exhaustivas en los procesos de desarrollo, incluyendo la preparación de un programa detallado de actividades y datos de prueba junto a los resultados esperados bajo condiciones establecidas.
   ii. Para desarrollos internos como externalizados, estas pruebas inicialmente deben ser realizadas por el equipo de desarrollo, sin embargo, se debe considerar la realización de pruebas de aceptación independientes para validar que el sistema funciona como se esperaba y sólo como se esperaba.
   iii. La extensión de las pruebas deberá ser proporcional a la importancia y la naturaleza del sistema.
   iv. Los resultados de las pruebas deben ser informados al menos a los dueños funcionales del sistema y el propietario o custodio de los activos de información involucrados.

b) Se deben establecer programas de pruebas de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones.

   i. Estas pruebas deben incluir las pruebas de los requisitos de seguridad de la información definidos en fases anteriores.
   ii. Estas pruebas deben incluir la validación de que se han aplicado las prácticas de desarrollo seguro definidas para la Agencia.
   iii. Las pruebas deben llevarse a cabo sobre componentes recibidos y los sistemas integrados.
   iv. Se pueden usar herramientas automatizadas como las herramientas de análisis de código y análisis de vulnerabilidades para verificar defectos asociados a la seguridad de información.
   v. Ningún sistema o actualización de software podrá implementarse en ambientes productivos si no cumple con los criterios de aceptación de estas pruebas.
   vi. Las pruebas de aceptación de sistemas deben considerar la ejecución de pruebas de estrés de forma de validar que éstos soportan el flujo de usuarios concurrentes planificado. Este punto se puede complementar con los lineamientos de gestión de capacidad establecidos en el Procedimiento para Control de Cambios TIC (SSI-PRO-7.1).
   vii. Los resultados de las pruebas deben ser informados al menos a los dueños funcionales del sistema y el propietario o custodio de los activos de información involucrados.

c) Los datos para utilizar en la ejecución de las pruebas de validación del software deberán ser cuidadosamente seleccionados y debidamente protegidos y controlados. Se debe evitar el uso de datos reales de producción que contengan datos personales o información confidencial, pero, en caso de ser necesarios, se deben seguir los siguientes lineamientos para su protección:

   i. Los lineamientos de control acceso establecidos en el Manual para Gestión de Accesos y Privilegios en Sistemas (SSI-MAN-4.2), así como

los establecidos en el Procedimiento de Gestión de Cuentas y Accesos (SSI-PRO-4.1) deben ser aplicados en los sistemas sobre los cuales se desarrollarán las pruebas.

ii. Debe haber una autorización específica del propietario de los activos, o en su defecto su custodio, para la utilización de datos productivos en ambientes de prueba.

iii. La información y datos operacionales deben ser borrados de forma inmediata del ambiente de pruebas una vez realizadas las pruebas.

6.5. Seguridad en la Puesta en Producción

Una vez el software o actualización de software ha pasado satisfactoriamente las pruebas de seguridad y pruebas de aceptación cumpliendo con los requisitos mínimos de seguridad establecidos para darlas por aprobadas, deberá ser puesto en producción para comenzar su explotación por parte de la Agencia. En esta fase, se deben considerar los siguientes lineamientos:

a) Si un sistema o actualización de sistema no cumple con las pruebas de aceptación y pruebas de seguridad de forma que asegure un nivel mínimo de seguridad, no podrá ser pasada a producción.

b) Se debe considerar una estrategia de vuelta atrás en caso de que el paso a producción falle, de forma que la operación normal de la Agencia no se vea afectada.

c) Una vez concretado el paso a producción, se debe realizar una revisión técnica del sistema o actualización de sistema para validar que su funcionamiento es homólogo al evidenciado durante la fase de testing.

6.6. Seguridad en el control de cambios sobre sistemas y software

Adicional a los lineamientos anteriores, en los casos referentes a actualizaciones o nuevas versiones del software existente, se deben considerar estar directrices:

a) Los cambios a lo largo del ciclo de vida de un software deben ser controlados, responder a requisitos del negocio y ceñirse a este procedimiento para dejar evidencia de su aplicación.

b) Los cambios en sistemas y softwares deben abarcar todas las fases del ciclo de vida del software descritas anteriormente.

c) Durante las fases de análisis de requerimientos y diseño de las nuevas versiones o actualizaciones en sistemas de la Agencia se debe validar que los controles de seguridad de la versión actual del mismo no se vean afectadas, y, en caso de que así sea, se deben definir y diseñar controles de seguridad que mitiguen el riesgo asociado.

d) Los cambios en sistemas y software, deben integrarse con los cambios en plataforma e infraestructura TI, cuyos lineamientos están en el Procedimiento de Control de Cambios TIC (SSI-PRO-7.1). Es así como se deben considerar los siguientes lineamientos:

   i. Los cambios deben ser aprobados por el propietario o custodio de los activos de información involucrados, así como por el dueño funcional del sistema.

   ii. Revisión de la integridad de la actualización o nueva versión del software para verificar que no se ha visto comprometida por los cambios.

   iii. Identificación de todo el software, información, bases de datos y hardware implicados en el cambio.

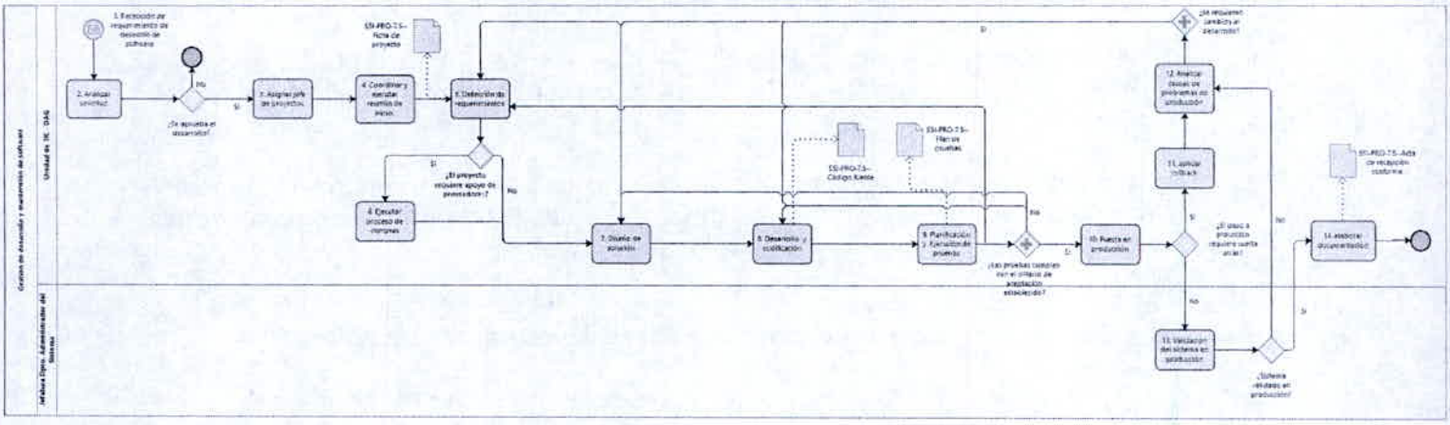
iv. Actualización de la documentación asociada al software.
v. Mantenimiento del control de versiones del software.
vi. Los paquetes de software cerrados de proveedores, obtenidos mediante la compra de una licencia, deben evitar ser cambiados por la Agencia, a menos que se cuente con el apoyo de dicho proveedor. Esto para mitigar posibles riesgos derivados del desconocimiento en el diseño de la solución y su código fuente.

7. MODO DE OPERACIÓN

A continuación, se describe los flujos de actividades para los siguientes procedimientos de respaldo de información:

a) Gestión para el desarrollo y mantención de software

7.1. Flujo de Procedimiento de Gestión para el desarrollo y mantención de software



7.2. Matriz de Procedimiento de Gestión para el desarrollo y mantención de software

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Recepción de requerimiento de desarrollo de software	El procedimiento se inicia al momento de recibir a través del sistema de gestión documental, un requerimiento de desarrollo de software solicitado por alguna de las áreas funcionales de la Agencia.	Unidad de TIC - DAG	2
2	Analizar solicitud	Se debe analizar la solicitud para determinar su alcance, esfuerzo requerido, dimensionamiento, y si ésta requiere un nuevo desarrollo, la actualización de otro existente y/o la adquisición de un producto nuevo. Se deberá evaluar si el requerimiento es aplicable o pertinente. Este análisis debe considerar la identificación de los involucrados en el proyecto, que además del área funcional que envía el requerimiento debe incluir al propietario o custodio de los activos de información involucrados en el posible nuevo desarrollo, así como al	Unidad de TIC - DAG	3 o FIN

		dueño funcional de éste. En base a este análisis se pueden dar los siguientes casos: - El requerimiento es pertinente (3) - El requerimiento no es pertinente (FIN).		
3	Asignar jefe de proyectos	Se asignará un jefe de proyectos interno de la Unidad de TIC, el cual deberá ser comunicado al área funcional requirente del sistema. Éste analizará en función del dimensionamiento del requerimiento, si se requiere el apoyo de un proveedor.	Unidad de TIC - DAG	4 o 5
4	Coordinar y ejecutar reunión de inicio	Se debe coordinar y ejecutar la reunión de inicio del proyecto, en la cual se deben incluir todos los involucrados en el proyecto identificados en etapas anteriores de este procedimiento, así como al proveedor.	Unidad de TIC - DAG	5
5	Definición de requerimientos	Se debe establecer los requerimientos funcionales y de seguridad del sistema de acuerdo con los lineamientos de este procedimiento. Se pueden dar las siguientes opciones: - Se requiere apoyo de proveedor (6). - No se requiere apoyo de proveedor (7).	Unidad de TIC - DAG	6 o 7
6	Ejecutar Proceso de Compras	Se debe ejecutar el proceso de compras para contratación del proveedor de acuerdo con los procedimientos internos de la Agencia y la legislación vigente al respecto.	Unidad de TIC - DAG	7
7	Diseño de solución	- Se debe diseñar el requerimiento de software considerando los lineamientos establecidos en este procedimiento.	Unidad de TIC - DAG	8
8	Desarrollo y codificación	Se debe desarrollar el sistema o actualización del sistema de acuerdo a los lineamientos de este procedimiento.	Unidad de TIC - DAG	9
9	Planificación y ejecución de pruebas	Se deben ejecutar las pruebas de aceptación del sistema y pruebas de seguridad del sistema según los lineamientos establecidos en este procedimiento. Se pueden dar las siguientes opciones: - Los resultados de las pruebas no cumplen con el criterio de aceptación establecido. En este caso se debe identificar en que fase se debe retomar el desarrollo para pasar las pruebas (6, 8 o 10). - Los resultados de las pruebas cumplen con el criterio de aceptación establecido (13)	Unidad de TIC - DAG	(5, 7, o 8) o 10
10	Puesta en producción	Se debe implementar el sistema o nueva versión del sistema en producción de acuerdo con los lineamientos de este procedimiento. Se pueden dar las siguientes opciones:	Unidad de TIC - DAG	11 o 13

		- Se requiere dar vuelta a tras por mal funcionamiento en producción (11). No se requiere dar vuelta atrás en el paso a producción (13)		
11	Aplicar Rollback	- Se debe aplicar la estrategia de vuelta atrás.	Unidad de TIC - DAG	12
12	Analizar causas de problemas en producción	Se debe identificar la causa raíz de los problemas del sistema en producción, para lo cual se pueden dar los siguientes escenarios: - La causa raíz requiere retomar el desarrollo desde la fase de requerimientos (5). - La causa raíz requiere retomar el desarrollo desde la fase de diseño (7). - La causa raíz requiere retomar el desarrollo desde la fase de desarrollo (8).	Unidad de TIC - DAG	5, 7 o 8
13	Validación del sistema en producción	Se debe validar que el sistema cumple con los requisitos funcionales y de seguridad una vez puesto en producción. Se pueden dar las siguientes opciones: - El sistema no es validado en producción (12). - El sistema es validado en producción (14).	Jefatura Dpto. Administrador del Sistema / Custodio de los Activos	12 o 14
14	Elaborar documentación	Se debe elaborar o actualizar la documentación del sistema.	Unidad de TIC - DAG	FIN

7.3. Matriz de Responsabilidades

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 gestión de desarrollo y mantención de software se distribuye de la siguiente forma:

ID	ACTIVIDAD	JEFATURA DAG	UNIDAD DE TIC - DAG	JEFATURA DIVISIÓN DUEÑA SISTEMA / PROP. ACTIVOS	JEFATURA DPTO ADMIN. SISTEMA / CUSTODIO ACTIVOS	ENC. SI / LIDER SSI
1	Recepción de requerimiento de desarrollo de software	R	E	-	-	-
2	Analizar solicitud	R	E	C	C	C
3	Asignar jefe de proyectos	R	E	I	I	I
4	Coordinar y ejecutar reunión de inicio	R	E	I	I	I
5	Definición de requerimientos	R	E	-	C/I	C/I
6	Ejecutar Proceso de Compras	R	E	C	C	C
7	Diseño de solución	R	E	A	A	C/I
8	Desarrollo y codificación	R	E	C	C	C
9	Planificación y ejecución de pruebas	R	E	A	A	C/I

10	Puesta en producción	R	E	C/I	C/I	C/I
11	Aplicar Rollback	I	C	A	A	C/I
12	Analizar causas de problemas en producción	R	E	I	I	I
13	Validación del sistema en producción	R	E	R	E	I/C
14	Elaborar documentación	R	E	I	I	I

8. REGISTROS DE OPERACIÓN

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Ficha de Proyecto (A.14.1.1; A.14.1.2)	-	Jefe de Proyecto	1 año / Google Drive	Digital	Google Drive, Documentación por Proyecto
TDR o especificaciones técnicas (solo para desarrollos externos) (A.14.1.1; A.14.1.2; A.14.2.5)	-	Encargado Área Desarrollo	2 años / Mercado Público	Digital	Mercado Público
Acta de Recepción Conforme (A.14.2.2; A.14.2.8; A.14.2.9)	-	Jefe de Proyecto	2 años / Google Drive	Digital	Google Drive, Documentación por Proyecto
Plan de Pruebas (A.14.2.8; A.14.2.9)	-	Jefe de Proyecto	2 años / Google Drive	Digital	Google Drive, Documentación por Proyecto
Código Fuente (A.14.2.2; A.14.2.6)	-	Jefe de Proyecto	3 años / Repositorios	Digital	GitLab
Pantalla de AWS Console (A.12.1.4)	-	Encargado Área Desarrollo	1 año / Google Drive	Digital	Google Drive Unidad de TIC

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).

SEPTIMO: APRUEBASE, el Manual de Requisitos de Seguridad para el Desarrollo y Adquisición de Software de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVOS

Asegurar que la seguridad de información es parte integral de los sistemas de información en todo su ciclo de vida.

2. ALCANCE

Las directrices de este manual deben ser aplicadas para todo nuevo desarrollo o adquisición de software 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 27.001:2013, Control A.14.01.01 – Análisis y especificaciones de requisitos de seguridad.
b) ISO/IEC 27.001:2013, Control A.14.01.02 – Aseguramiento de servicios de aplicación en redes públicas.
c) ISO/IEC 27.001:2013, Control A.14.02.01 – Política de desarrollo seguro.
d) ISO/IEC 27.001:2013, Control A.14.02.05 – Principios de ingeniería para sistemas seguros.
e) ISO/IEC 27.001:2013, Control A.14.02.06 – Entorno de desarrollo seguro.
f) ISO/IEC 27.001:2013, Control A.14.02.07 – Desarrollo tercerizado.

3. NORMAS Y REFERENCIAS

- 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 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

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

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

- Resolución Exenta N°1612, de 2019, de la Agencia de Calidad de la Educación, en donde se aprueba la Política de Seguridad de Información para Relación con Proveedores de la Agencia de Calidad de la Educación.

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) **Jefatura División de Administración General (DAG):** 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) **Jefatura de la Unidad de TIC – DAG:** ejecutar y dar 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.

c) **Líder(es) Interno(s) del SSI:** Serán los responsables de apoyar en la correcta aplicación y adopción de los lineamientos dispuestos en este documento al interior de su División, así como canalizar cualquier incumplimiento o necesidad de mejora asociado a éste.
d) **Jefaturas de Departamento:** Como custodios de los activos de información, serán los responsables de velar por la correcta definición de los requisitos de seguridad a nivel de negocio para los sistemas y software que soporten su operación y los activos de información que custodian.

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 DAG	UNIDAD TIC - DAG	ENC. SI / CIBERSEGURIDAD / LÍDER INTERNO SSI	JEFATURA DPTO. ADMIN. SISTEMA
RESPONSABLE	X			
EJECUTOR		X		
CONSULTADO			X	X
INFORMADO				X

6. LINEAMIENTOS DEL MANUAL

Los requisitos para la seguridad de la información deberán incluirse en los requisitos para nuevos sistemas de información o mejoras en los sistemas de información existentes, para lo cual se deben seguir los siguientes lineamientos:

a) Los requisitos de seguridad deben identificarse en base a los siguientes recursos:

   i. Directrices internas de la Agencia (políticas, manuales y procedimientos).
   ii. Lineamientos Gubernamentales (Guía de desarrollo de software).
   iii. Registro de incidentes, según lo propuesto por el procedimiento de respuesta ante incidentes de ciberseguridad (SSI-PRO-5.1)[31].
   iv. Vulnerabilidades descubiertas, según lo propuesto por el principio de gestión de vulnerabilidades técnicas propuesto en la Política General de Seguridad de Información (SSI-POL-01)[32].
   v. Estándares y buenas prácticas de desarrollo de codificación en función de el o los lenguajes elegidos para el desarrollo.

b) La identificación de requisitos de seguridad debe ser documentada y revisada por todas las partes involucradas, que incluyen, pero no se limitan a el Dueño Funcional del sistema y el Propietario de los Activos de Información involucrados.

c) Los requisitos de seguridad deben establecerse en fases iniciales o tempranas del ciclo de desarrollo.

d) Los requisitos de seguridad deben tener en consideración la criticidad de los activos de información y de la operación de la Agencia involucrados.

---

[31] Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.
[32] 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 vi) sobre la gestión de vulnerabilidades técnicas.

e) Los requisitos de seguridad deben aplicarse en todas las capas de la arquitectura de la solución: de negocio, datos, aplicaciones y tecnología. Esto equilibrando la necesidad de seguridad de información con la usabilidad y experiencia de usuario de la solución

f) Se deben analizar los riesgos de seguridad en las nuevas tecnologías de la Agencia y se debe revisar el diseño propuesto contra patrones de ataque conocidos.

6.1. Servicios de Aplicación en Redes Públicas

La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida considerando las siguientes directrices:

a) Aplicación de mecanismos de autenticación que considere el principio de gestión de controles criptográficos establecidos en la Política General de Seguridad de Información (SSI-POL-01)[33].

b) Requisitos para protección de información confidencial y datos privados.

c) Las aplicaciones accesibles a través de redes públicas están sujetas a una serie de amenazas relacionadas con la red, tales como actividades fraudulentas, disputas de contratos o la divulgación de información al público. Por lo tanto, son indispensables las evaluaciones detalladas del riesgo y la selección adecuada de controles. Los controles requeridos a menudo incluyen métodos criptográficos para la autenticación y el aseguramiento de la transferencia de datos.

6.2. Entorno de Desarrollo Seguro

Se debe proteger adecuadamente el entorno de desarrollo de software durante todo el ciclo de vida, considerando las siguientes directrices:

a) Un entorno de desarrollo seguro incluye a las personas, los procesos y la tecnología relacionados con el desarrollo.

b) Se debe tener en cuenta la criticidad de la información y datos involucrados en el desarrollo.

c) Segregación entre los diferentes ambientes de desarrollo, así como el control de acceso a éstos según lo que define el principio de gestión de accesos y privilegios en sistemas establecido en la Política General de Seguridad de Información (SSI-POL-01)[34].

d) Monitoreo de los cambios en el entorno según lo propuesto por el principio de control de cambios TIC establecido en la Política General de Seguridad de Información (SSI-POL-01)[35] y los cambios sobre el código fuente.

---

[33] 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 gestión de controles criptográficos.

[34] 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 ii) sobre la gestión de vulnerabilidades técnicas.

[35] 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 iv) sobre el control de cambios TIC.

6.4. Externalización del Desarrollo de Software

El desarrollo de software externalizado deberá ser supervisado y controlado por la organización, tomando en cuenta, además de los lineamientos que se listan a continuación, lo estipulado en la Política de Relación con Proveedores (SSI-POL-08)[36]:

a) Se deben considerar en los contratos los acuerdos de licencias, propiedad intelectual y propiedad del código fuente, donde este último siempre será de propiedad de la Agencia y el proveedor deberá entregarlo según se estipule en el contrato de prestación de servicios.

b) Se debe considerar en el contrato que el proveedor debe diseñar el software considerando la seguridad de información utilizando modelado de amenazas, desarrollar la solución usando buenas prácticas de codificación en función del lenguaje a utilizar, y la realización de pruebas de seguridad satisfactorias previo a la entrega final del producto.

c) La presentación de las siguientes evidencias:
   i. Evidencia de la ejecución de pruebas de aceptación de calidad.
   ii. Evidencia de que se han realizado suficientes pruebas para proteger contra la presencia en el entregable de código malicioso, tanto intencionado como no intencionado.
   iii. Evidencia de que se han realizado suficientes pruebas para entregar el producto sin vulnerabilidades conocidas.

7. REGISTROS DE OPERACIÓN

El registro de operación para este manual se aplica durante la ejecución del principio de de gestión para desarrollo de software seguro establecido en la Política General de Seguridad de Información (SSI-POL-01)[37].

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) [38].

OCTAVO: APRUEBASE, el Manual para la Gestión de Controles Criptográficos de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVOS

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o confidencialidad de los activos de información de la Agencia.

2. ALCANCE

---

[36] Resolución Exenta N°1612, de 2019, de la Agencia de Calidad de la Educación, que aprueba la Política de Seguridad de Información para Relación con Proveedores de la Agencia de Calidad de la Educación.
[37] 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 b), punto ii) sobre la gestión en el procedimiento de desarrollo y mantención de software.
[38] Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.

Estos lineamientos deberán ser aplicados sobre los mecanismos de autenticación de todos los sistemas y software de la Agencia, así como para los discos duros de los equipos y medios extraíbles que lo requieran.

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.10.01.01 – Política de uso de controles criptográficos.

b) ISO/IEC 27001:2013, Control A.10.01.02 – Gestión de claves criptográficas

3. NORMAS Y REFERENCIAS

- 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 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

- Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, en donde se 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 la aplicación correcta de lo dispuesto en este manual en función de los requerimientos particulares de su División.

b) **Jefatura de la Unidad de TIC – DAG:** Ejecutar y dar cumplimiento a lo estipulado en este manual, así como de facilitar la implementación de las medidas necesarias para cumplir con su objetivo y alcance.

c) **Jefaturas de Departamento:** ejecutar los lineamientos de este manual cuando sea necesario en función de la protección de los activos de información.

d) **Líder(es) Interno(s) del SSI:** Velar por la adopción de estos lineamientos en función de los requerimientos necesarios para preservar la seguridad de la información y datos sensibles de su División.

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 DE DIV.	JEFATURA DPTO.	UNIDAD TIC - DAG	ENC. SI / CIBER	LÍDER SSI

RESPONSABLE	X				
EJECUTOR		X	X		
CONSULTADO				X	
INFORMADO					X

6. LINEAMIENTO DEL MANUAL

Para generar una utilización eficaz de la criptografía, se establecen lineamientos separados en función de las tres (3) características de la información que busca preservar la criptografía:

a) **Confidencialidad:** Considera el uso de algoritmos de cifrado para proteger la información de accesos no autorizados.

   i. Los algoritmos de cifrado pueden ser de tipo simétricos o asimétricos, para los cuales se establecen los siguientes requisitos mínimos:

      - Para uso de cifrado simétrico se debe implementar algoritmos AES 256 como mínimo.
      - Para uno de cifrado asimétrico se debe establecer un largo mínimo de clave de 2048 bits.

   ii. Se deben aplicar mecanismos de cifrado tanto para discos duros internos del equipamiento de los usuarios de la agencia, como para discos duros externos y medios de almacenamiento extraíbles si éstos serán transportados fuera de las instalaciones de la Agencia. Este lineamiento debe ser complementado por el principio de gestión de activos y transferencia de información de la Política General de Seguridad (SSI-POL-01)[39].

b) **Integridad:** Considera el uso de funciones hash como indicador de integridad de la información y datos que se almacenan y transmiten.

   i. Para el uso de funciones hash se debe considerar como mínimo SHA-256.
   ii. La utilización de funciones hash se debe utilizar para el almacenamiento de contraseñas de acceso en todos los mecanismos de autenticación de los sistemas o software de la Agencia.

c) **Autenticidad:** Considera el uso de controles criptográficos para garantizar que la información o datos fueron emitidos efectivamente por una persona, entidad o sistema en específico.

   i. Para aplicar esta característica de la información, se pueden utilizar funciones MAC, teniendo en consideración que éstas no garantizan el no repudio.

[39] 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) Y iii) sobre la asignación y devolución de recursos y la administración de medios removibles, respectivamente.

ii. La forma más recomendable de establecer la autenticidad y no repudio sobre un activo de información o datos, se debe hacer uso de firma electrónica de acuerdo con la legislación vigente.

7. REGISTRO DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-7.4—Criptografía para autenticación en sistemas y software
MANUAL / PROCEDIMIENTO	Controles Criptográficos
CONTROLES ISO 27.001	• A.10.01.01 – Política de uso de controles criptográficos. A.10.01.02 – Gestión de claves criptográficas.
RESPONSABLE	Jefe Unidad TIC – DAG
DESCRIPCIÓN	Corresponde a la captura de pantalla que evidencia la utilización de mecanismos criptográficos de autenticación en los sistemas y software de la Agencia según lo indicado en este manual.
FRECUENCIA	En función de los cambios definidos en las configuraciones de autenticación de equipos, sistemas y software.
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)[40].

NOVENO: APRUEBASE, el Procedimiento de Mantención de Equipos Críticos de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Asegurar el correcto mantenimiento de los equipos críticos para garantizar su disponibilidad e integridad.

2. ALCANCE

Los lineamientos de este procedimiento se deben ejecutar sobre todo equipamiento crítico que soporte la operación de la infraestructura TIC 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 27.001:2013, Control A.11.2.4 – Mantención del equipamiento.

3. NORMAS Y REFERENCIAS

a) 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

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

Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.4 relativo al principio de seguridad en la gestión de las tecnologías de información y comunicación (TIC).

b) Resolución Exenta N°584, de 2021, 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

Se declaran como crítico, el siguiente equipamiento que soporta la operación de la infraestructura tecnológica de la Agencia:

- SAI o UPS
- Storage
- Plataforma de virtualización (VMWare)
- Equipamiento de comunicaciones (Switches)
- Plata telefónica CISCO Call Manager, SBC, Liric GSM
- Equipamiento de Firewall
- Servidores
-

Éstos deberán recibir mantenimiento de acuerdo con las siguientes directrices:

a) Los equipos podrán estar sujetos a mantenciones preventivas y/o correctivas.
b) La mantención preventiva deberá ser programada de acuerdo con intervalos y las recomendaciones del fabricante o proveedor.
c) Sólo el personal debidamente autorizado y calificado deberá realizar el mantenimiento preventivo o correctivo.
d) Se deberán mantener registro de las fallas, reales o sospechados, así como de la ejecución de mantenciones preventivas y correctivas. Esto según el documento de Registro de Mantención, y la Ficha de Consolidado de Mantenciones que se presenta en el Anexo 1 y Anexo 2 de este documento.
e) Se deben adoptar los controles necesarios cuando se va a ejecutar una mantención preventiva o correctiva, de forma de minimizar el riesgo de accesos no autorizados a información y datos sensibles. Este punto aplica tanto para mantenciones realizadas con personal interno de la Agencia como por personal externo de algún proveedor.

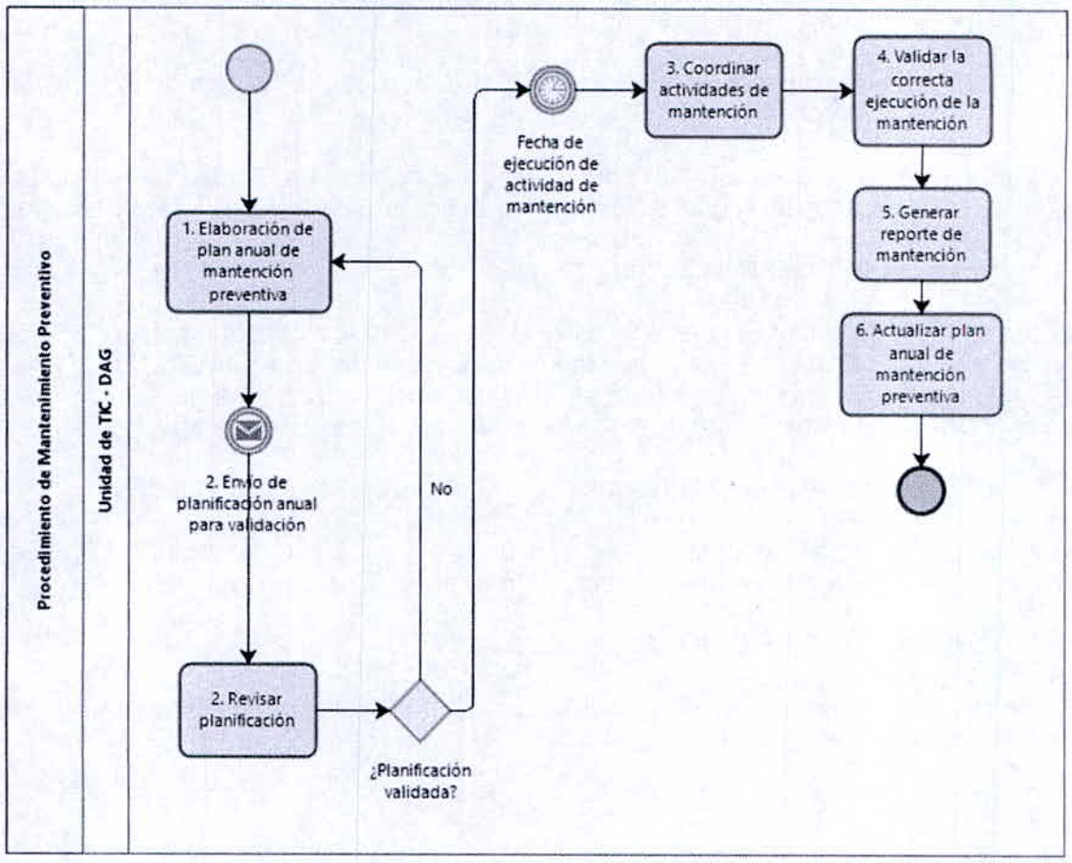
7. MODO DE OPERACIÓN

A continuación, se describen los flujos de actividades para los siguientes procedimientos de respaldo de información:

a) Procedimiento de mantenimiento preventivo.

b) Procedimiento de mantenimiento correctivo.

7.1. Flujo de Procedimiento para Mantenimiento Preventivo

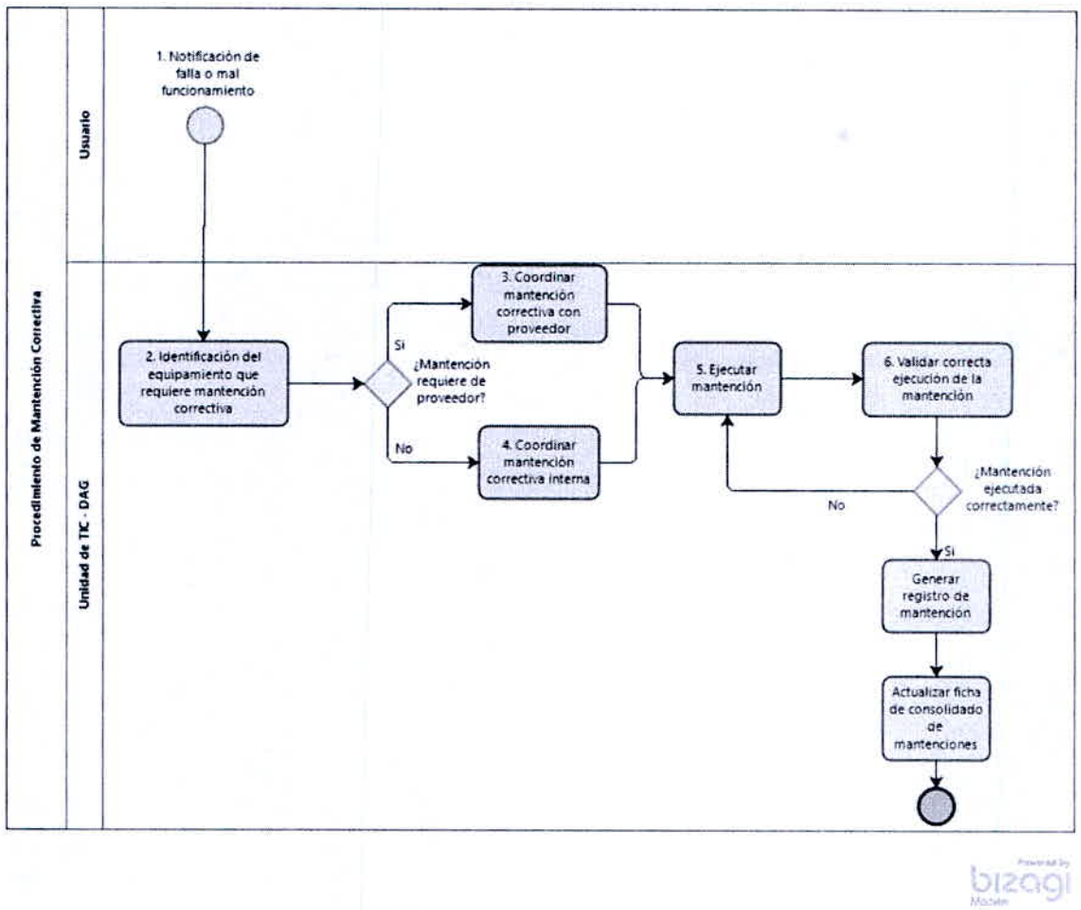


7.2. Matriz de Procedimiento para Mantención Preventiva

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Elaboración de plan anual de mantención preventiva	Se debe elaborar un plan anual que considere todo el equipamiento crítico que requiera mantención preventiva según las especificaciones del fabricante / proveedor. Se deben considerar tanto las mantenciones a realizar de forma interna como las que requieren de participación de proveedores.	Unidad de TIC - DAG	2
2	Enviar plan anual para validación	Se debe enviar el plan anual de mantenimiento preventivo para su validación por parte de la Jefatura de la Unidad de TIC - DAG.	Unidad de TIC - DAG	3
3	Revisar plan anual de mantención preventiva	Se debe validar que el plan anual sea consistente con las necesidades y capacidades de la Agencia, así como que se cumplan con los lineamientos propuestos en este documento. Se pueden dar los siguientes escenarios: - El plan anual es validado (4). - El plan anual no es validado (1).	Unidad de TIC - DAG	1 o 4
4	Coordinar actividades de	Llegada la proximidad de la fecha en la cual está planificada la mantención	Unidad de TIC - DAG	5

	mantención preventiva	preventiva, se deben ejecutar las gestiones necesarias para que ésta se realice en tiempo y forma, lo que puede incluir la contratación de proveedores y coordinación de la actividad, el aviso a los usuarios de indisponibilidad de algún recurso tecnológico por mantenimiento, advertir a los usuarios de que hagan los respaldos respectivos, entre otros.		
5	Ejecutar mantención	Se deben ejecutar las actividades de mantención según lo coordinado en la actividad anterior.	Unidad de TIC - DAG	6
6	Validar la correcta ejecución de la mantención	Se debe realizar un chequeo de que la mantención se realizó según lo planificado y que cubre las necesidades del equipamiento según las especificaciones del fabricante. Se pueden dar los siguientes escenarios: - La mantención se ejecutó según los requisitos del equipo (7). - La mantención no se ejecutó según los requisitos del equipo (5).	Unidad de TIC - DAG	5 o 7
7	Generar registro de mantención	Se debe llenar el documento de Registro de mantención para dejar evidencia de la ejecución de esta.	Unidad de TIC - DAG	8
8	Actualizar la Ficha de Consolidado de Mantenciones	Se debe actualizar la Ficha de Consolidado de Mantenciones de forma de registrar todas las mantenciones que se realizan de forma satisfactoria.	Unidad de TIC - DAG	FIN

7.3. Flujo de Procedimiento para Mantenciones Correctivas



7.4. Matriz de Procedimiento para Mantenciones Correctivas

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Notificación de falla o mal funcionamiento	El proceso comienza ante la notificación por parte de uno o varios usuarios sobre intermitencia o mal funcionamiento de componentes tecnológicos.	Usuario	2
2	Identificación del equipamiento que requiere mantención	Se debe identificar qué equipamiento está causando dicha intermitencia o mal funcionamiento para coordinar su mantención correctiva. Se pueden dar los siguientes escenarios: - El equipamiento requiere mantención por proveedor (3). - El equipamiento requiere mantención interna (4).	Unidad de TIC - DAG	3 o 4
3	Coordinar mantención correctiva con proveedor	Se deben ejecutar las gestiones necesarias para contratación de proveedores y coordinación de la actividad, el aviso a los usuarios de indisponibilidad de algún recurso tecnológico por mantenimiento, advertir a los usuarios de que hagan los respaldos respectivos, entre otros.	Unidad de TIC - DAG	5
4	Coordinar mantención correctiva interna	Se deben ejecutar las gestiones internas necesarias para coordinación de la actividad, el aviso a los usuarios de indisponibilidad de algún recurso	Unidad de TIC - DAG	5

		tecnológico por mantenimiento, advertir a los usuarios de que hagan los respaldos respectivos, entre otros.		
5	Ejecutar mantención	Se deben ejecutar las actividades de mantención según lo coordinado en la actividad anterior.	Unidad de TIC - DAG	6
6	Validar la correcta ejecución de la mantención	Se debe realizar un chequeo de que la mantención se realizó según lo planificado y que se soluciona la intermitencia o falla en el funcionamiento notificados. Se pueden dar los siguientes escenarios: - La mantención se ejecutó según los requisitos del equipo (7). - La mantención no se ejecutó según los requisitos del equipo (5).	Unidad de TIC - DAG	5 o 7
7	Generar registro de mantención	- Se debe llenar el documento de Registro de mantención para dejar evidencia de la ejecución de esta.	Unidad de TIC - DAG	8
8	Actualizar la Ficha de Consolidado de Mantenciones	- Se debe actualizar la Ficha de Consolidado de Mantenciones de forma de registrar todas las mantenciones que se realizan de forma satisfactoria.	Unidad de TIC - DAG	FIN

7.5. Matriz de Responsabilidades

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 mantenciones preventivas se distribuye de la siguiente forma:

ID	ACTIVIDAD	JEFATURA DAG	JEFATURA DPTO. ADMIN. SISTEMAS	LÍDER SSI	UNIDAD DE TIC - DAG	ENC. SI
1	Elaboración de plan anual de mantención preventiva	R	I	I	E	C
2	Enviar plan anual para validación	R	-	-	E	-
3	Revisar plan anual de mantención preventiva	R	-	-	E	-
4	Coordinar actividades de mantención preventiva	R	I	I	E	I/C
5	Ejecutar mantención	R	I	I	E	I/C
6	Validar la correcta ejecución de la mantención	R	I	I	E	I/C
7	Generar registro de mantención	R	-	-	E	-
8	Actualizar la Ficha de Consolidado de Mantenciones	R	-	-	E	-

Adicionalmente, la matriz de responsabilidades para el procedimiento de mantenciones correctivas se distribuye de la siguiente manera:

ID	ACTIVIDAD	JEFATURA DAG	JEFATURA DPTO. ADMIN. SISTEMAS	LÍDER SSI	UNIDAD DE TIC - DAG	ENC. SI	USUARIO
1	Notificación de falla o mal funcionamiento	-	I	I	I	I	R
2	Identificación del equipamiento que requiere mantención	R	I/C	I	E	I	C
3	Coordinar mantención correctiva con proveedor	R	I	I	E	I	I
4	Coordinar mantención correctiva interna	R	I	I	E	I	I
5	Ejecutar mantención	R	I	I	E	I	I
6	Validar la correcta ejecución de la mantención	R	I	I	E	I	I
7	Generar registro de mantención	R	I	I	E	I	I
8	Actualizar la Ficha de Consolidado de Mantenciones	R	I	I	E	I	I

8. REGISTRO DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-7.4—Documento de Mantención
MANUAL / PROCEDIMIENTO	Mantención preventiva Mantención correctiva
CONTROLES ISO 27.001	A.11.2.4 – Mantención del equipamiento
RESPONSABLE	Jefatura de Unidad TIC - DAG
DESCRIPCIÓN	Corresponde al llenado del documento para evidenciar la ejecución de una mantención, sea esta preventiva o correctiva.
FRECUENCIA	Dependerá de la ejecución de mantenciones preventivas y correctivas.
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-7.4—Ficha consolidado de mantenciones
PROCEDIMIENTO	Mantención preventiva Mantención correctiva
CONTROLES ISO 27.001	A.11.2.4 – Mantención del equipamiento
RESPONSABLE	Jefatura de Unidad TIC - DAG
DESCRIPCIÓN	Se debe incorporar de forma consolidada en esta ficha la ejecución de las mantenciones sean estas preventivas o correctivas.
FRECUENCIA	Dependerá de la ejecución de mantenciones preventivas y correctivas.
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)[41].

DÉCIMO: DÉJASE SIN EFECTO la Resolución Exenta N°s. 1026, 1547, 1548, 1613 y 1616, todas de 2019, de la Agencia de Calidad de la Educación.

DÉCIMO PRIMERO: 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.

DÉCIMO SEGUNDO: **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/NIO/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
-

[41] Resolución Exenta N°585, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización del Procedimiento de Respuesta ante Incidentes.