MEMORÁNDUM N° 83/2019

DE: **DANIEL RODRÍGUEZ MORALES**
SECRETARIO EJECUTIVO

A: **JEFATURAS DE LAS DIVISIONES DE LA AGENCIA DE CALIDAD DE LA EDUCACIÓN**

C/C: **JEFATURA DEL DEPARTAMENTO DE AUDITORÍA**

JEFATURA DE LA UNIDAD DE PLANIFICACIÓN

REF.: **Decreto Exento N° 324, de 2018, del Ministerio de Hacienda, que aprueba Programa Marco de los Programas de Mejoramiento de la Gestión de los servicios en el año 2019, para el pago del incremento del desempeño institucional del artículo 6° de la Ley N° 19.553.**

FECHA: 26 DIC 2019

Como es de su conocimiento los Programas de Mejoramiento de la Gestión (PMG) en los servicios públicos tienen su origen en la Ley N° 19.553, de 1998, que concede una asignación de modernización y otros beneficios, y asocian el cumplimiento de objetivos de gestión a un incentivo monetario para los funcionarios públicos.

En dicho contexto, para el año 2019 se incluyó el objetivo de gestión eficaz, cuyo grado de cumplimiento se mide a través de indicadores de desempeño, siendo, uno de ellos, el relativo a controles de seguridad de la información.

Es debido a lo anterior, que el Comité de Seguridad de la Información de la Agencia aprobó, a través de actas de 02 de octubre y 05 de diciembre, ambas, de 2019, entre otros documentos, los procedimientos sobre:

1. Segregación de funciones.

2. Elaboración del plan anual de capacitación, formación y entrenamiento.

3. Alta y baja de cuentas de usuario a la red y servicios de red.

4. Gestión de contraseñas.

5. Gestión de incidentes.

6. Sincronización de relojes.

7. Gestión de vulnerabilidades técnicas.

8. Gestión para el desarrollo y mantención de software seguro.

9. Documentación de los procedimientos operacionales.

10. Privacidad y protección de la información de identificación personal.

En consecuencia, y ya que la difusión de dichos procedimientos resulta imprescindible de realizarse al interior de la Agencia, es que, por lo manifestado previamente, solicito a ustedes puedan dar a conocer el material que se acompaña adjunto entre todo el personal que desarrolle labores en sus dependencias.

Saluda atentamente a ustedes,

REPUBLICA DE CHILE
Agencia de Calidad de la Educación
SECRETARIO EJECUTIVO

DANIEL RODRÍGUEZ MORALES
SECRETARIO EJECUTIVO
AGENCIA DE CALIDAD DE LA EDUCACIÓN

ASA/GCL/DBL
Distribución:
- Divisiones (5)
- Archivo Secretaría Ejecutiva
- Unidad de Planificación
- Departamento de Auditoría
- Departamento Jurídico
- Oficina de Partes

Procedimiento de Segregación de Funciones
Control A.06.01.02

Tabla de Contenidos

Revisiones del Procedimiento.....2
1. Objetivo......3
2. Alcance......3
3. Normas y Referencias......3
4. Términos y Definiciones......3
5. Roles y Responsabilidades.....4
6. Definiciones para la Segregación de Funciones.....5
7. Modo de Operación.....6
7.1 Flujo de Procedimiento para el Enmascaramiento y la Entrega de Información.6
7.2 Matriz del Procedimiento para Segregación de funciones.....7
7.3 Matriz de Responsabilidades......8
8. Registro de Operación......9
9. Anexo.....9

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC)	**María Loreto Salinas Jefa Departamento de Gestión y Desarrollo de las Personas**	**Andrea Soto Araya Encargada Seguridad de la Información**	**Comité SGSIC**

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	31/10/2019	Elaboración Inicial	Todas

1. Objetivo.

El objetivo del presente documento es entregar el flujo secuencia, tanto de las actividades como las definiciones, asociadas a la descripción de las responsabilidades asociadas a la seguridad de información, para ser incluida en las descripciones de cargo de los diferentes roles y perfiles del personal de la Agencia de Calidad de la Educación, en adelante, la Agencia.

2. Alcance.

El presente procedimiento debe ser aplicado para todas las descripciones de cargo de todos los funcionarios y funcionarias, de planta y contrata, honorarios, o de cualquier naturaleza jurídica de su vinculación internos la Agencia de Calidad de la Educación, que, conforme a sus responsabilidades, tengan acceso a los activos de información de ésta.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27.002:2013, el presente documento tiene su alcance sobre el siguiente control:

- A.06.01.02 – Segregación de Funciones.

3. Normas y Referencias.

- NCh ISO 27.001:2013.
- NCh ISO 27.002:2013.
- Política General de Seguridad de la Información y Ciberseguridad, aprobada por Resolución Exenta N° 589, de 2019, de la Agencia de Calidad de la Educación.
- Estructura Funcional del Sistema de Gestión de Seguridad de Información y Ciberseguridad, aprobada por Resolución Exenta N° 1024, de 2019, de la Agencia de Calidad de la Educación.

4. Términos y Definiciones.

Amenaza	Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.
Riesgo	Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.
Autoridad	Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.
Evento de Seguridad de la Información	Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.
Incidente de	Se refiere a la Identificación y materialización de una amenaza o riesgo

Seguridad	detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.
Vulnerabilidad	Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.
Evento de Seguridad	Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia
Plan de Contingencia	Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.
Activos de Información	Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
Contactos críticos	Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o incidentes.
Red de Seguridad	Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.
Seguridad de la Información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.

5. Roles y Responsabilidades.

a) **Jefatura del Departamento de Gestión y Desarrollo de las Personas, División de Administración General:** Será este rol el encargado de velar por la correcta ejecución de este procedimiento. Adicionalmente, deberá determinar los tiempos y alcances del mismo.

b) **Encargada de Desarrollo de las Personas, Departamento de Gestión y Desarrollo de las Personas:** Será este rol el encargado de ejecutar de forma correcta el presente procedimiento, implementando el levantamiento o actualización de perfiles de cargo, cada vez que sea requerido por los niveles directivos de la Agencia y aprobado por la Jefatura Departamento de Gestión y Desarrollo de las Personas.

c) **Encargada/o de Seguridad de la Información:** Como líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, será este rol el encargado de asesorar en la definición de responsabilidades en seguridad de información y ciberseguridad de los diferentes perfiles de cargo de la Agencia, considerando su relevancia para el servicio y su rol en el Sistema de Gestión de Seguridad de la Información.

d) **Jefatura de División o Macrozona o Unidad Asesora Secretaria Ejecutiva solicitante:** Corresponde a la Jefatura de División, de Macrozona o de Unidad Asesora de Secretaria Ejecutiva, que solicita una incorporación o actualización a un perfil de cargo al Departamento de Gestión y Desarrollo de las Personas.

6. Definiciones para la Segregación de Funciones.

Según lo especificado en la Estructura Funcional del Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC), se deberán definir responsabilidades de diferente grado de implicancia a roles en el SGSIC.

De esta forma, se definen las siguientes definiciones de responsabilidades a incluir en las descripciones de cargo de los funcionarios y funcionarias de la Agencia:

a) **Responsabilidad en Seguridad de la Información Transversal:** Corresponde a la definición de responsabilidad en estas temáticas a incorporar en la descripción de la totalidad de los cargos que componen la Agencia de Calidad de la Educación. En detalle, esta descripción debe ser la siguiente:

"Será parte de las responsabilidades asociadas al cargo, el velar por mantener la confidencialidad, disponibilidad, integridad y privacidad de los activos que contengan información tanto propia del servicio como sensible de terceros, y, que sean accedidos, almacenados y/o tratados de forma directa o indirecta como efecto del desempeño de sus funciones, según lo declarado en la Política General de Seguridad de la Información y Ciberseguridad de la Institución y todos los documentos atingentes al cargo que de ésta se desprendan."

b) **Responsabilidades en Seguridad de la Información para Jefaturas de División y Jefaturas de Macrozonas:**

Corresponde a la definición de responsabilidad en estas temáticas a incorporar en la descripción de los cargos de Jefaturas de las Divisiones y de Macrozonas que componen la Agencia de Calidad de la Educación. En Detalle, esta descripción debe ser la siguiente:

"Será parte del cargo, ejercer como Propietario o Dueño de los Activos de Información que fluyen por los procesos que se encuentran bajo su gestión, según lo estipulado en la Estructura Funcional del Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC). Por lo tanto, será responsable de velar por la correcta ejecución de las actividades asociadas a esta designación, según lo estipulado en la Política General de Seguridad de Información y Ciberseguridad de la Institución y todos los documentos atingentes al cargo que de ésta se desprendan. Adicionalmente, será parte de las facultades asociadas a esta responsabilidad, el designar como Custodio de los Activos de Información a aquellos roles que desempeñen labores de jefatura en los Departamentos, Unidades y/o Sub-Departamentos que se encuentren bajo el alero de la División, delegando en éstos, las actividades (más no las responsabilidades) asociadas a la gestión de activos de información según lo estipulado en la Estructura Funcional del Sistema de Gestión de Seguridad de la Información."

c) **Responsabilidades en Seguridad de la Información para Jefaturas de Departamento/Unidad:**

Corresponde a la definición de responsabilidad en estas temáticas a incorporar en la descripción de los cargos de Jefaturas de Departamentos y/o Unidades que componen la Agencia de Calidad de la Educación. En detalle, esta descripción debe ser la siguiente:

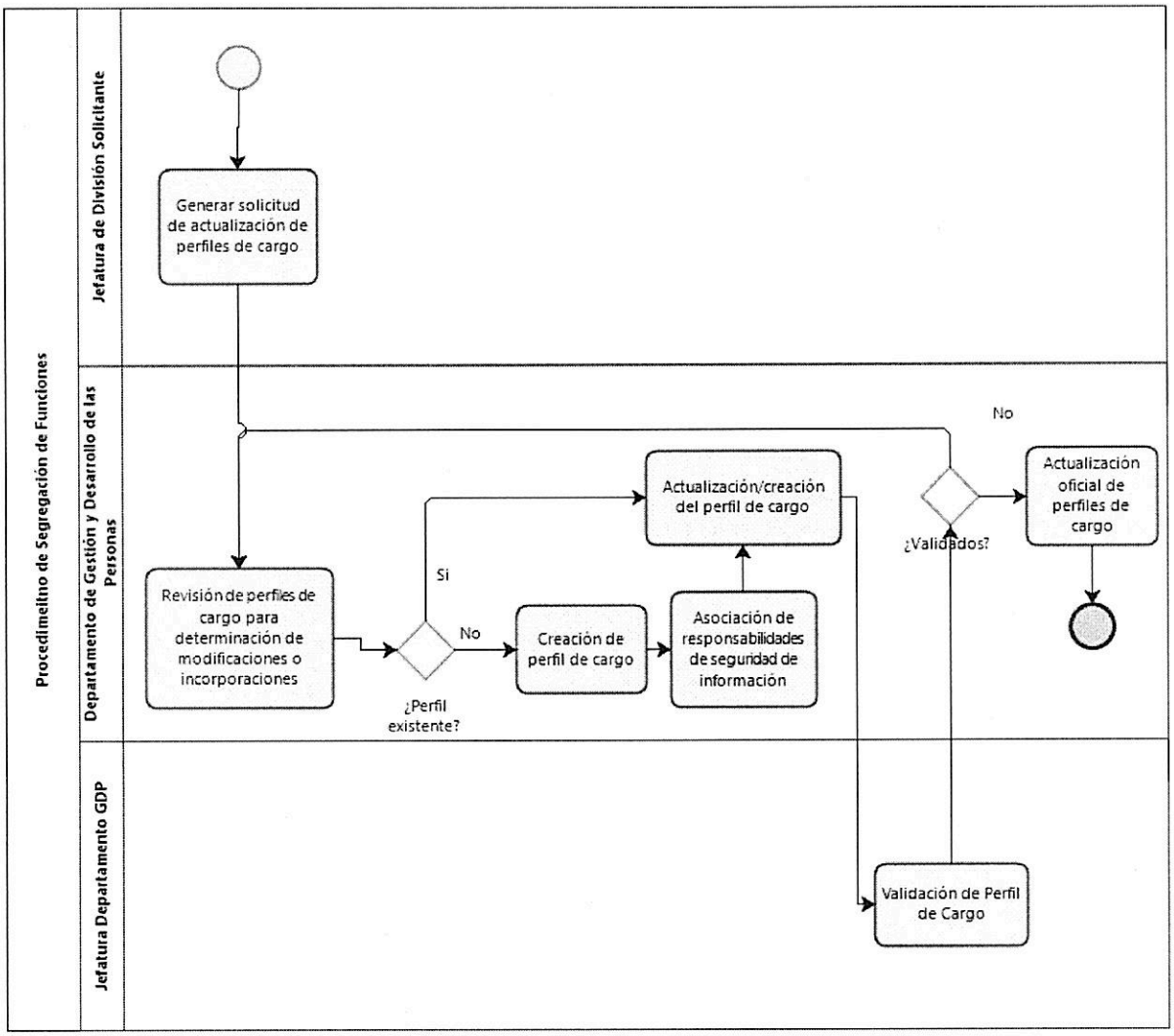
"Como Jefatura de Departamento/Unidad, este cargo podrá ser designado, por la Jefatura de División Directa, es decir, por el Propietario(a) de los Activos de Información, como Custodio de los mismos cuando éstos fluyan por los procesos que se encuentran bajo su gestión, según lo estipulado en la Estructura Funcional del Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC). Por lo tanto, será responsable de velar por la correcta ejecución de las actividades asociadas, según lo estipulado en la Política General de Seguridad de

Información y Ciberseguridad de la Institución y todos los documentos atingentes al cargo y designación de Custodio que de ésta se desprendan."

7. Modo de Operación.

A continuación, se describen los flujos procedimentales para el levantamiento o actualización del perfil de cargo.

7.1 Flujo de Procedimiento para levantamiento o actualización del perfil de cargo.



7.2 Matriz del Procedimiento para levantamiento o actualización de perfil de cargo.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Generar solicitud de actualización de perfiles de cargo	Para dar inicio formal al procedimiento, se debe enviar al Departamento de Gestión y Desarrollo de las Personas, una solicitud formal para actualización o incorporación de perfiles de cargo. Esta solicitud debe considerar la mayor cantidad de información sobre el perfil del cargo asociado a su ámbito de responsabilidades.	Jefatura de División Solicitante	2
2	Revisión de perfiles de cargo para determinación de modificaciones o incorporaciones	Dado lo descrito en la solicitud recibida, se debe realizar una revisión de los perfiles de cargo para determinar si: • Los perfiles de cargo considerados en el alcance deben ser creados desde cero (2A). • Los perfiles de cargo considerados en el alcance ya existen y deben ser modificados en temáticas específicas (3).	Departamento de Gestión y Desarrollo de las Personas	2A y/o 3
2A	Creación de perfil de cargo	Se deberá proceder a la creación formal de el o los perfiles de cargo en cuestión.	Departamento de Gestión y Desarrollo de las Personas	2B
2B	Asociación de responsabilidades de seguridad de información	Dado que el o los roles en cuestión responden a nuevas incorporaciones, se debe evaluar la funcionalidad de éstos en el Sistema de Gestión de Seguridad de la Información (SGSIC) para poder definir sus responsabilidades asociadas a estas materias.	Departamento de Gestión y Desarrollo de las Personas	3
3	Actualización/creación del perfil de cargo	Se debe actualizar o incorporar al perfil del cargo, las responsabilidades que éste o éstos requieren en materias de seguridad de información, según lo descrito en el punto seis (6) de este documento.	Departamento de Gestión y Desarrollo de las Personas	4

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
4	Validación de Perfil de Cargo	Una vez realizadas las incorporaciones de cargo, o las incorporaciones de éstos a la Agencia, se debe proceder a su validación. • Las actualizaciones / incorporaciones son validadas (2). • Las actualizaciones / incorporaciones no son validadas (5).	Jefatura de Departamento de Gestión y Desarrollo de las Personas	2 o 5
5	Actualización oficial de perfiles de cargo	Una vez validadas las actualizaciones e/o incorporaciones, se debe proceder a su formalización institucional.	Departamento de Gestión y Desarrollo de las Personas	FIN

7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

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

De esta forma, la matriz de responsabilidades se estructura de la siguiente manera:

ID	ACTIVIDAD	Jefatura de División Solicitante	Dpto. de GDP	Encargada(o) Seguridad	Jefatura Dpto. GDP
1	**Generar solicitud de actualización de perfiles de cargo**	R/E	I	-	I
2	**Revisión de perfiles de cargo para determinación de modificaciones o incorporaciones**	C	R/E	-	I
2A	**Creación de perfil de cargo**	C	R/E	-	I
2B	**Asociación de responsabilidades de seguridad de información**	I	R/E	C	I
3	**Actualización/creación del perfil de cargo**	I	R/E	C	I
4	**Validación de Perfil de Cargo**	C	I	C/I	R/A
5	**Actualización oficial de perfiles de cargo**	I	R/E	I	I

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Perfil Agencia de Calidad de la Educación, con la(s) definiciones asociadas a seguridad de información.	-	Jefa(e) Departamento de Gestión y Desarrollo de las Personas	1 año / Carpeta compartida	Digital	Carpeta compartida de Departamento de Gestión y Desarrollo de las Personas.

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Política de Revisión Independiente del Sistema de Gestión de Seguridad de Información y Ciberseguridad (Control A.5.1.2, A.18.2.1, A.18.2.2 y A.18.2.3)
2. Procedimiento de Segregación de Funciones (Control A. 6.1.2)
3. Política para Transferencia y Manejo de Información (A. 8.2.2, A.8.2.3, A.8.3.2, A.13.2.1 y A.13.2.3)
4. Procedimiento de Controles y Perímetro de Seguridad Física (Control A.11.1.2 y A.11.1.4)
5. Procedimiento para Documentación de los Procedimientos Operacionales (control A.12.1.1 y A.18.1.3)
6. Política de Protección Contra Código Malicioso (Control A.12.02.01, A.12.5.1 y A.12.6.2)
7. Procedimiento de Gestión de Vulnerabilidades Técnicas (A.12.6.1)
8. Política de Controles de Red (control .13.1.1 y A.13.1.2)
9. Política de Seguridad de la Información para los Proveedores (A.15,1,1 y A.15.2.1)
10. Política de Planificación de la Continuidad Operacional (control A.17.1.1, A.17.1.2 y A.17.1.3)
11. listado de legislación vigente (A.18.1.1)
12. Procedimiento de Privacidad y Protección de la Información de Identificación Personal (Control A.18.01.04)

Fecha: 5 de diciembre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodriguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	Gabriela Cares	Jefa de DIEST	
6	Ana María Concha	Jefe DAG	
7	Sergio Hidalgo	Jefe Departamento de Auditoría	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Andrea Soto Araya	Encargada de SSI	
10	Nicol Jeria O.	Encargada de Ciberseguridad	
11			
12			

1

Procedimiento de Elaboración de Plan Anual de Capacitación, Formación y Entrenamiento
Control A.07.02.02

Tabla de Contenidos

Revisiones del Procedimiento.....2
1. Objetivo.....2
2. Alcance.....3
3. Normas y Referencias.....3
4. Términos y Definiciones.....3
5. Roles y Responsabilidades.....4
6. Modo de Operación.....4
6.1 Flujo de Procedimiento de Gestión de la Capacitación.....5
6.2 Flujo de Sub Procedimiento de Conformación de Comité Bipartito de Capacitación.....6
6.3 Flujo de Sub Procedimiento de Detección de Necesidades de Capacitación.....7
6.4 Flujo de Sub Procedimiento de Elaboración de Plan Anual de Capacitación.....8
6.5 Matriz del Procedimiento de Gestión de la Capacitación.....9
6.6 Matriz del Sub Procedimiento de Conformación de Comité Bipartito de Capacitación.....11
6.7 Matriz del Sub Procedimiento de Detección de Necesidades de Capacitación...12
6.8 Matriz del Sub Procedimiento de Plan Anual de Capacitación.....13
7. Matriz de Responsabilidades......13
8. Registro de Operación......15
9. Anexo.....15

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de Información y Ciberseguridad	**María Loreto Salinas Jefa de Departamento de Gestión y Desarrollo de Personas**	**Andrea Soto Encargada de Seguridad de la Información**	**Comité de SGSIC**

REVISIONES DEL PROCEDIMIENTO			
N° Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	27/09/2019	Elaboración inicial	Todas

1. Objetivo.

El objetivo del presente documento es establecer un procedimiento estandarizado para la gestión de la capacitación que se realizará al interior de la Agencia de Calidad de la Educación, en adelante la Agencia.

2. Alcance.

Este procedimiento se debe aplicar a nivel nacional, de forma de extender el proceso de gestión de capacitación a todo el personal de la Agencia de Calidad de la Educación.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27002:2013, el presente documento tiene su alcance sobre los siguientes controles:

- A.07.02.02 – Capacitación y Formación en Seguridad de Información.

3. Normas y Referencias.

a. NCh ISO 27.001:2013.

b. NCh ISO 27.002:2013.

c. Política General de Seguridad de Información, aprobada por Resolución Exenta N° 589, de 2019, de la Agencia de Calidad de la Educación.

d. Política de Seguridad para Gestión de Personas, aprobada por Resolución Exenta N° 1152, de 2019, de la Agencia de Calidad de la Educación.

e. Política de Personas, aprobada por Resolución Exenta N° 1560, de 2019, de la Agencia de la Calidad de la Educación.

f. Resolución N° 2, de 2018, del Ministerio de Hacienda, que aprueba normas de aplicación general en materias de participación funcionaria, cumplimiento de estándares en formación y capacitación de funcionarios públicos, rol de jefaturas en dirección de equipos y gestión del desempeño individual y sistema de calificaciones para todos los servicios públicos conforme la facultad establecida en el artículo 2° letra q) de la Ley Orgánica de la Dirección Nacional del Servicio Civil, contenida en el artículo vigésimo sexto de la Ley N° 19.882.

g. Lo dispuesto en el DFL N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.575.

h. Ley N° 19.880, de 2003, que establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

i. Decreto con Fuerza de Ley N° 29, de 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley 18.834 sobre Estatuto Administrativo.

j. Artículo 10 de la Ley N°19.518, que fija el estatuto de Capacitación y Empleo.

k. Documento "Guía práctica para gestionar la Capacitación en los Servicios Públicos". Servicio Civil, diciembre 2014.

l. Formato Programa de Trabajo Evaluación de Transferencia y Plan Anual de Capacitación (PAC), señalado en la Resolución N° 2, de 2018, del Ministerio de Hacienda antes referida.

m. Estrategia de Planificación Trienal de Capacitación, señalada en la Resolución N° 2, de 2018, del Ministerio de Hacienda antes referida.

4. Términos y Definiciones.

Capacitación	La capacitación comprende un conjunto de actividades permanentes, organizadas y sistemáticas destinadas a que los colaboradores adquieran y/o perfeccionen el conjunto de conocimientos, habilidades y actitudes que se requieran o son necesarias para el eficiente desempeño de sus cargos o funciones dentro de la Agencia.
Plan Anual de Capacitación	El Plan Anual de Capacitación, es una planificación se basa en la información generada en la fase de Detección de Necesidades de Capacitación del presente procedimiento, la cual contiene acciones de capacitación o líneas de formación, las que deben ser percibidas como

	aquellas que permitan un desarrollo, complemento, perfeccionamiento o actualización de los conocimientos y destrezas técnicas u operativas que requieran las personas para realizar sus tareas, así como también debe abordar la formación integral que un servicio público necesita, a partir de valores, principios, conocimientos y aptitudes genéricas y transversales comunes a toda la gestión pública, con el objetivo de desempeñar adecuadamente la función asignada. Estas actividades de capacitación son para todo el personal de la Agencia, independiente de su calidad jurídica. Este plan cuenta con presupuesto propio y tiene una duración de un año calendario.
Comité Bipartito de Capacitación	Corresponde a una instancia de participación que asesora a la administración de la Agencia en la orientación, priorización, programación, ejecución y evaluación de las acciones de capacitación en beneficio de los colaboradores de la institución. El objetivo de este Comité es promover la participación y compromiso de los funcionarios respecto de su propia formación y capacitación, para incrementar la eficiencia y productividad de la Agencia. El rol del Comité es de revisor y consultivo. Este Comité se encuentra integrado por representantes de los colaboradores y del empleador.

5. Roles y Responsabilidades.

a) **Jefatura del Departamento de Gestión y Desarrollo de las Personas, de la División de Administración General:** Será el rol encargado de velar porque el proceso se lleve a cabo durante el año calendario. Dentro de sus principales funciones destacan el liderazgo en la conformación del Comité Bipartito de Capacitación, la detección de las necesidades de capacitación del personal de la Agencia, de la materialización de la compra de las actividades y seguimiento de ejecución. Además del control de la planificación y ejecución presupuestaria de las actividades de capacitación.

b) **Comité Bipartito de Capacitación:** Tiene dentro de sus principales responsabilidades asesorar en la elaboración y validación de la propuesta del Plan de Capacitación, el cual fomentará el desarrollo continuo de los colaboradores a través de actividades de formación, desarrollo y perfeccionamiento individual y grupal.

c) **Secretario Ejecutivo:** Será este rol el encargado de participar de forma activa en la conformación del Comité Bipartito mediante la designación de los representantes institucionales y la posterior aprobación mediante VB. Adicionalmente deberá participar en la aprobación del Plan Anual de Capacitación mediante la oficialización de este a través de resolución exenta.

d) **Unidad de Compras del Departamento de Compras y Servicios Generales de la División de Administración General**: Le corresponde gestionar la compra de los servicios presentados por el Departamento de Gestión y Desarrollo de las Personas.

e) **Encargado/a de Capacitación del Departamento de Gestión y Desarrollo de las Personas:** Profesional responsable de la planificación, elaboración y ejecución de las acciones de capacitación y formación para los/as funcionarios/as y colaboradores/as de la Agencia.

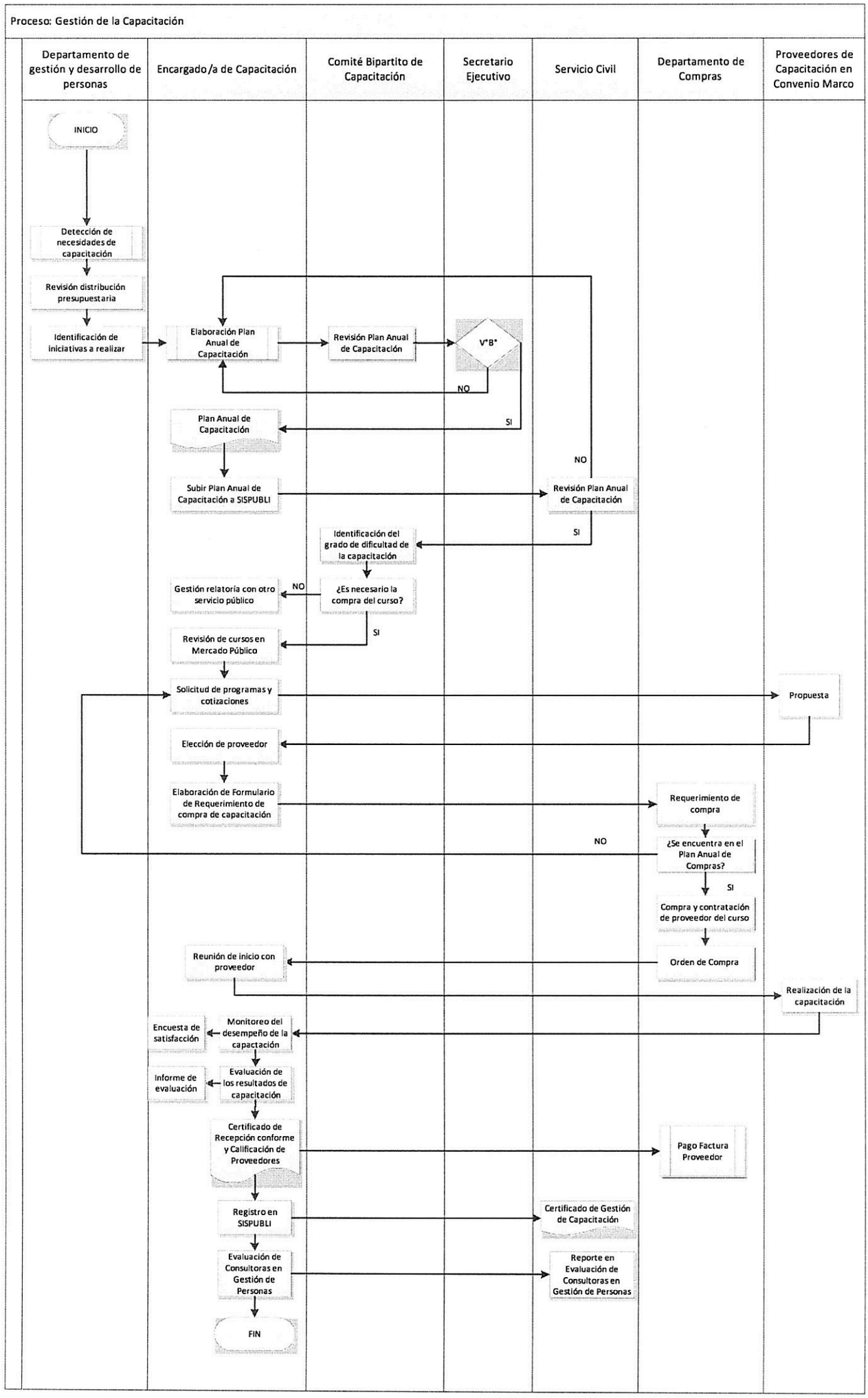
f) **Encargado/a de Seguridad de Información:** Como rol líder del SGSCI, será éste el encargado de asesorar en la inclusión de las temáticas de Seguridad de Información y Ciberseguridad en el Plan de Capacitación Anual.

6. Modo de Operación.

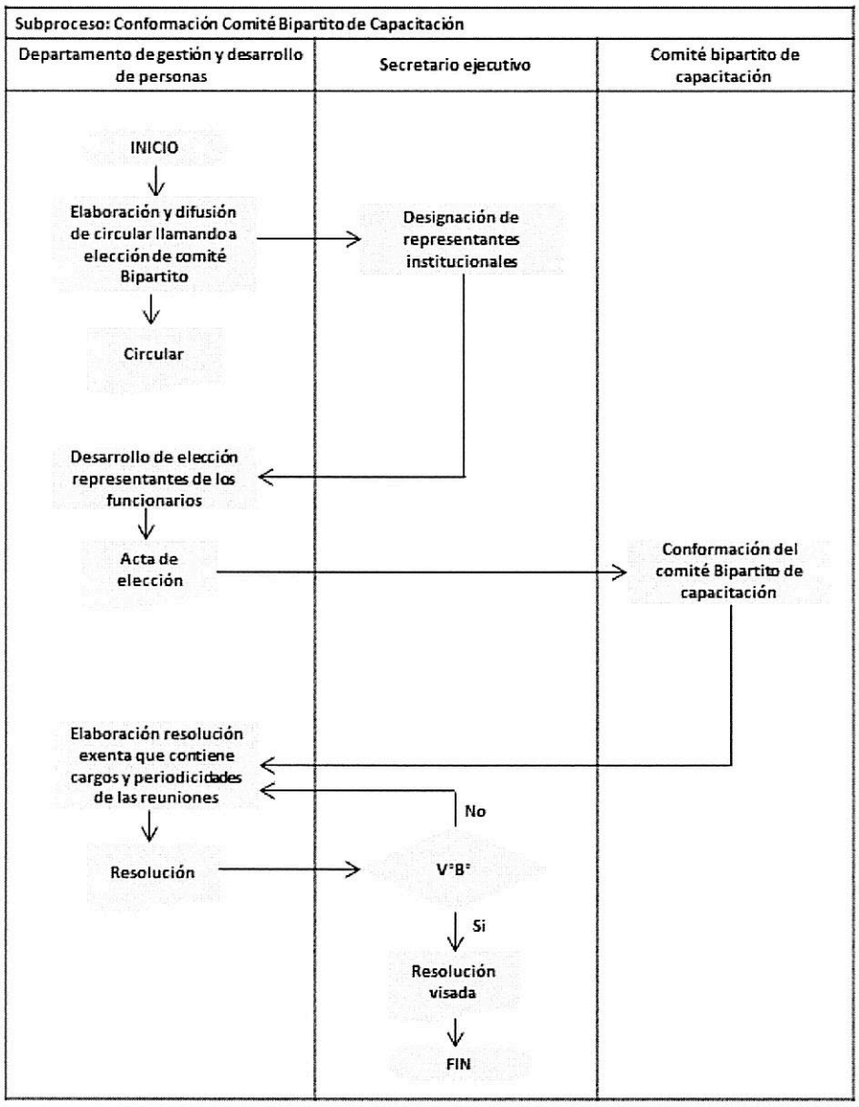
A continuación, se describen los flujos procedimentales para:

a. Procedimiento de Gestión de la Capacitación.
b. Sub procedimiento de Conformación de Comité Bipartito de Capacitación.
c. Sub procedimiento de Detección de Necesidades de Capacitación.
d. Sub procedimiento de Elaboración de Plan Anual de Capacitación.

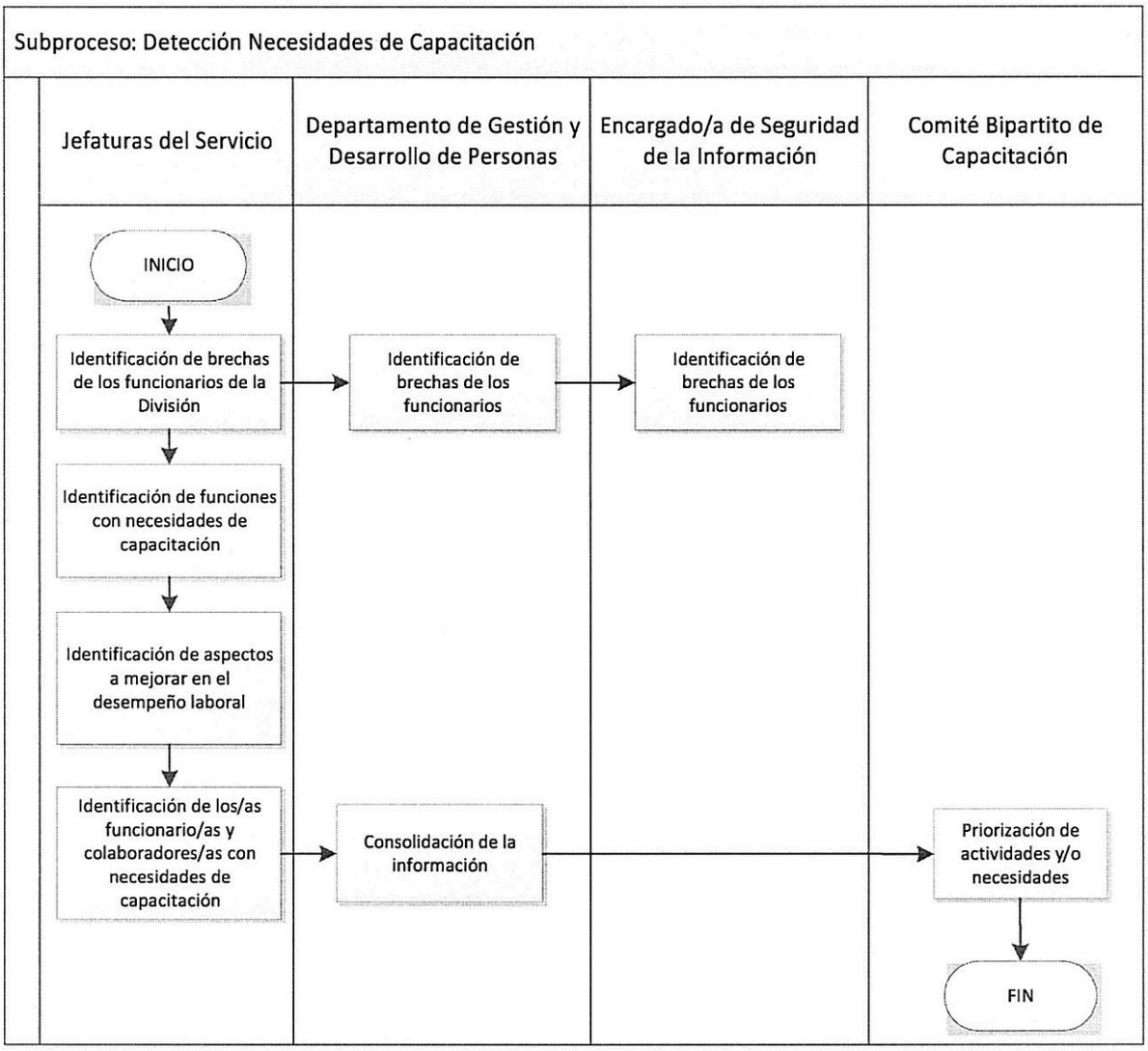
6.1 Flujo de Procedimiento de Gestión de la Capacitación.



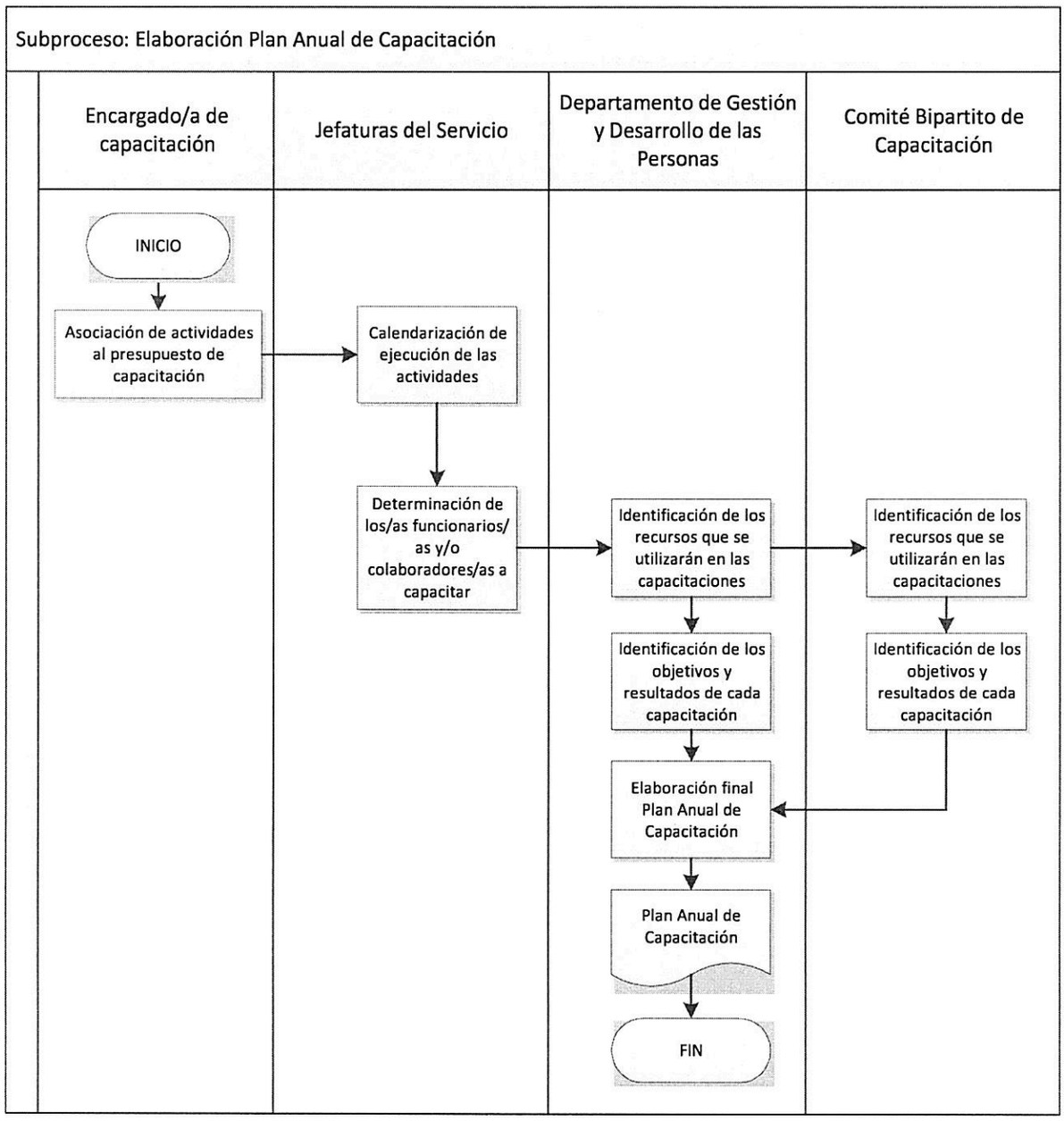
6.2 Flujo de Sub Procedimiento de Conformación de Comité Bipartito de Capacitación.



6.3 Flujo de Sub Procedimiento de Detección de Necesidades de Capacitación.



6.4 Flujo de Sub Procedimiento de Elaboración de Plan Anual de Capacitación.



6.5 Matriz del Procedimiento de Gestión de la Capacitación.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Detección de necesidades de capacitación	Se debe realizar la encuesta de detección de necesidades según lo establecido en el punto 6.3 de este documento.	Departamento de Gestión y Desarrollo de las Personas	2
2	Revisión distribución presupuestaria	En función de los resultados de la encuesta, se debe realizar una revisión de la distribución presupuestaria para la ejecución del plan de capacitación.	Departamento de Gestión y Desarrollo de las Personas	3
3	Identificación de iniciativas a realizar	Se deben identificar, en función de los resultados de la encuesta y la distribución presupuestada, las iniciativas de capacitación a aplicar en el año t.	Departamento de Gestión y Desarrollo de las Personas	4
4	Elaboración Plan Anual de Capacitación	Se debe elaborar el Plan Anual de Capacitación según lo establecido en el punto 6.4 de este documento. Éste debe ser aprobado mediante la obtención del VB por parte del Comité Bipartito de Capacitación, para lo cual se pueden dar las siguientes alternativas: - El Plan de Capacitación Anual es aprobado (6). - El Plan de Capacitación Anual no es Aprobado (4).	Encargado/a Capacitación	5
5	Revisión Plan Anual de Capacitación	El Plan Anual de Capacitación es revisado en Comité Bipartito de Capacitación, en donde sus integrantes pueden sugerir cambios en beneficio de los/as funcionarios/as y colaboradores/as de la Agencia.	Comité Bipartito de Capacitación	6
6	Formalización Plan Anual de Capacitación	Aprobación, mediante resolución de Secretario Ejecutivo Plan Anual de Capacitación firmando e instruye su implementación.	Secretario Ejecutivo	7
7	Subir Plan Anual de Capacitación a Sispubli	Una vez formalizado el Plan Anual de Capacitación se debe subir a la plataforma del Servicio Civil Sispubli	Encargada de Capacitación	8
8	Revisión Plan Anual de Capacitación	A través de la plataforma SISPUBLI, es donde es revisado por el Servicio Civil, en donde comprueban que contiene las normas y políticas que regulan la gestión de personas en el Estado	Servicio Civil	9
9	Identificación del grado de dificultad de la capacitación	Se debe identificar el grado de dificultad de las iniciativas de capacitación para determinar si se requiere apoyo de externos para llevarlas a cabo. Se pueden dar las siguientes opciones: - Se requiere el apoyo de consultora externa (16). - No se requiere apoyo de una consultora externa (6A).	Encargado/a de Capacitación	10

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
10	Revisión de proveedores de actividades de capacitación disponibles en convenio marco	Se debe revisar en el portal de Chile Compra, aquellas consultoras disponibles para prestar el servicio de capacitación requerido.	Encargado/a de Capacitación	11
11	Solicitud de envío de propuestas	Se debe enviar una licitación para comenzar con la recepción de propuestas asociadas a la prestación del servicio de capacitación.	Encargado/a de Capacitación	12
12	Elección de proveedor de la capacitación	Una vez recibidas las propuestas, en función de lo establecido en las bases de licitación, se debe elegir la consultora que se adjudicará el servicio.	Encargado/a de Capacitación	13
13	Elaboración de requerimiento de compra de la capacitación	Una vez seleccionado el proveedor, se debe elevar el requerimiento de solicitud de compra correspondiente.	Encargado/a de Capacitación	14
14	Envío a unidad de compras	La solicitud de requerimiento de compra debe ser enviada a la Unidad correspondiente, donde se debe revisar si este requerimiento responde al Plan Anual de Capacitación. Se pueden dar las siguientes alternativas: - El requerimiento de compra no responde al Plan Anual de Capacitación (12). - El requerimiento de compra responde al Plan Anual de Capacitación (14).	Encargado/a de Capacitación	15
15	Modificación del Plan Anual de Capacitación	Se debe modificar el Plan Anual de Capacitación para incluir el requerimiento de compra en cuestión. Se informa a Comité Bipartito de Capacitación.	Departamento de Gestión y Desarrollo de las Personas	16
16	Analizar pertinencia y presupuesto	Se debe volver a analizar la pertinencia presupuestaria previo a la inclusión del requerimiento en el Plan Anual de Capacitación.	Comité Bipartito de Capacitación / Departamento de Gestión y Desarrollo de las Personas	17
17	Compra y contratación de proveedor	Se formaliza la compra según lo establecido en el Manual de Compras de la Agencia de Calidad de la Educación.	Unidad de compras	18
18	Reunión de inicio con proveedor	Se debe dar inicio formal al servicio de capacitación con la Consultora que se adjudicó el servicio mediante una reunión inicial para alineamiento de expectativas y planificación detallada.	Contraparte de la División en conjunto con Encargado/a de Capacitación	19
19	Gestión de relatoría con otro servicio público	La capacitación se realiza por parte de otros servicios públicos.	Encargado/a de Capacitación	20
20	Realización de la capacitación	La capacitación se realiza por parte del proveedor.	Proveedor	21
21	Monitoreo del desempeño de la capacitación	Se debe realizar la encuesta de satisfacción para determinar el desempeño de la capacitación.	Encargado/a de Capacitación	22

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
22	Evaluación de los resultados de la capacitación	En función de los resultados de la encuesta de satisfacción, se determina la evaluación general de la capacitación.	Encargado/a de Capacitación	23
23	Certificado de Recepción Conforme y Calificación de Proveedores	Se debe certificar la recepción de la capacitación a través de documento que indique la fecha de la realización y si el servicio fue exitoso o no. A la vez, se debe calificar al proveedor del servicio a través de documento que evalúa distintos factores que impactan en la calidad del servicio. Estos documentos son entregados al Departamento de Compras.	Departamento de Gestión y Desarrollo de las Personas	24
24	Pago factura proveedor	El Departamento de Compras debe realizar el pago de los servicios adquiridos.	Departamento de Compras	25
25	Registro en SISPUBLI	La actividad de capacitación se debe registrar en SISPUBLI. Plataforma del Servicio Civil que controla las capacitaciones de los servicios públicos.	Encargado/a de Capacitación	26
26	Evaluación de Proveedor	Se debe evaluar el servicio entregado por el proveedor de la actividad de capacitación en portal de Servicio Civil.	Encargada de Capacitación	FIN

6.6 Matriz del Sub Procedimiento de Conformación de Comité Bipartito de Capacitación.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Elaboración y difusión de circular llamando a elección de Comité Bipartito	Se debe elaborar y difundir la circular de llamado a elección del Comité Bipartito de Capacitación de la Agencia.	Departamento de Gestión y Desarrollo de las personas	2
2	Designación de representantes institucionales	Se debe realizar la designación de los representantes institucionales que conformarán el Comité.	Secretario Ejecutivo	3
3	Desarrollo de elección representantes de los funcionarios	Se deben desarrollar las elecciones correspondientes para la elección de los representantes de los funcionarios y funcionarias en el Comité Bipartito de Capacitación.	Departamento de Gestión y Desarrollo de las personas	4
4	Conformación Comité Bipartito de Capacitación	Según los resultados de la elección, se conforma el Comité Bipartito de Capacitación para el año en curso.	Comité Bipartito de Capacitación	5
5	Elaboración Resolución Exenta que contiene cargos y periodicidades de las reuniones	Se debe formalizar la conformación del Comité Bipartito de Capacitación mediante la elaboración de una Resolución Exenta.	Departamento de gestión y desarrollo de personas	6

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
6	Visto bueno	Aprobación por Resolución Exenta de conformación del Comité Bipartito de Capacitación. Se pueden dar las siguientes alternativas: - La conformación del comité no es aprobada y no se dicta la resolución (5). - La conformación del comité es aprobada y se dicta la resolución (FIN).	Secretario Ejecutivo	5 o FIN

6.7 Matriz del Sub Procedimiento de Detección de Necesidades de Capacitación.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Identificación de brechas de los/as funcionario/as y colaboradores/as de las Divisiones	Se deben identificar las necesidades de capacitación en la Institución. **NOTA:** Se deben identificar de forma transversal aquellas necesidades que tengan que ver con Seguridad de Información.	Jefaturas de División/ Encargada de Seguridad de Información / Departamento de Gestión y Desarrollo de las Personas	2
2	Identificación de funciones con necesidades de capacitación	Posterior a la detección de necesidades, se deben identificar aquellos roles que requieren cubrir esa brecha de capacitación. **NOTA:** Al igual que en el punto anterior, la Encargada de Seguridad de Información debe determinar los roles asociados a las brechas detectadas en el punto anterior.	Jefaturas de División	3
3	Identificación de aspectos a mejorar en el desempeño laboral	En función de las funciones que tienen asociadas necesidades de capacitación, se debe ajustar esta definición de aspectos más granulares en busca de la mejora del desempeño laboral.	Jefaturas de División	4
4	Identificación de los funcionarios con necesidades de capacitación	Posterior a la detección de necesidades, se deben identificar aquellos roles que requieren participar en las actividades de mejora del desempeño.	Jefaturas de División	5
5	Consolidación de información	Una vez realizadas las identificaciones antes detalladas, se debe consolidar la información para poder conformar el mapa de necesidades de la organización en temáticas de capacitación.	Encargado/a de Capacitación	6
6	Priorización de actividades y/o necesidades	En función de las necesidades de la Institución, se debe realizar una priorización de las necesidades y actividades de capacitación propuestas.	Comité Bipartito de capacitación / Departamento de Gestión y Desarrollo de las Personas	FIN

6.8 Matriz del Sub Procedimiento de Plan Anual de Capacitación.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Asociación de actividades al presupuesto de capacitación	Según el presupuesto de la Institución asignado a capacitaciones, y considerando la priorización de las actividades y necesidades de capacitación, se debe establecer la asociación entre estas dos variables.	Encargado/a de Capacitación	2
2	Calendarización de ejecución de las actividades	Una vez asociadas las actividades con el presupuesto, éstas deben ser calendarizadas a razón de un año.	Jefaturas del Servicio	3
3	Determinación de los/as funcionarios/as y/o colaboradores/as a capacitar	Se deben definir los funcionarios y funcionarias que participarán de cada una de las actividades, en función de lo establecido en el Sub Procedimiento de Detección de Necesidades y las capacidades presupuestarias del servicio.	Jefaturas del Servicio	4
4	Identificación de los recursos que se utilizarán en las capacitaciones	Se deben identificar los recursos necesarios para la realización de las capacitaciones.	Comité Bipartito de Capacitación / Departamento de Gestión y Desarrollo de las Personas	5
5	Identificación de los objetivos y resultados de cada capacitación	Se deben identificar los objetivos que debe cumplir cada capacitación, lo cual servirá para evaluar después su efectividad.	Comité Bipartito de Capacitación / Departamento de Gestión y Desarrollo de las Personas	6
6	Elaboración final plan anual de capacitación	Se debe elaborar el plan final de capacitación.	Encargada de Capacitación	FIN

7. Matriz de Responsabilidades.

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

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

De esta forma las matrices de responsabilidades asociadas a los procesos establecidos por el presente documento son las siguientes:

a) Matriz de responsabilidades para el Procedimiento de Gestión de la Capacitación:

ID	ACTIVIDAD	DPTO GDP	ENCARGDO/A DE CAPACITACIÓN	COMITÉ BIPARTITO	UNIDAD COMPRAS	CONTRAPARTE DIVISIÓN	PROFESIONAL UNIDAD DESARROLLO PERSONAS	PROVEEDOR
1	**Conformación Comité Bipartito de capacitación**	R	E	-	-	-	-	-
2	**Detección de necesidades de capacitación**	R	E	I	-	-	-	-
3	**Revisión distribución presupuestaria**	R	E	C	-	-	-	-
4	**Identificación de iniciativas a realizar**	R	E	C	-	-	-	-

5	**Elaboración Plan Anual de Capacitación**	R	E	C	-	-	-	-
6	**Identificación del grado de dificultad de la capacitación**	R	E	C	-	C	-	-
7	**Revisión de consultoras disponibles en convenio marco**	I	R/E	I	-	C	-	-
8	**Solicitud de envío de propuestas**	R	E	I	-	-	-	-
9	**Elección de proveedor de la capacitación**	R	E	I	-	C	-	-
10	**Elaboración de requerimiento de compra de la capacitación**	R	E	I	C	-	-	-
11	**Envío a unidad de compras**	R	E	I	I	I	-	-
12	**Modificación del Plan Anual de Capacitación**	R	E	C	-	-	-	-
13	**Analizar pertinencia y presupuesto**	R	E	C	-	-	-	-
14	**Compra y contratación de proveedor**	I	C	I	R/E	I	-	-
15	**Reunión de inicio con proveedor**	R	E	I	-	C	-	I/C
16	**Realización de la capacitación**	R	E	I	-	I	E	-
17	**Realización de la capacitación**	R	E	I	I	I	-	E
18	**Monitoreo del desempeño de la capacitación**	R	E	I	-	I	-	-
19	**Evaluación de los resultados de la capacitación**	R	E	I	-	I	-	-

b) Matriz de responsabilidades para el Sub Procedimiento de Conformación de Comité Bipartito de Capacitación:

ID	ACTIVIDAD	DPTO. GDP	SE	COMITÉ BIPARTITO
1	**Elaboración y difusión de circular llamando a elección de Comité Bipartito**	R/E	I	-
2	**Designación de representantes institucionales**	R	E	-
3	**Desarrollo de elección representantes de los funcionarios**	R/E	I	-
4	**Conformación Comité Bipartito de Capacitación**	C	I	R/E
5	**Elaboración Resolución Exenta que contiene cargos y periodicidades de las reuniones**	R/E	I	I
6	**Visto bueno**	R	E	I

c) Matriz de responsabilidades para el Sub Procedimiento de Detección de Necesidades de Capacitación:

ID	ACTIVIDAD	JEFATURAS	DEPARTAMENTO DE GESTIÓN Y DESARROLLO DE LAS PERSONAS	ENCARGADO/A CAPACITACIÓN	COMITÉ BIPARTITO	ENC. SI
1	Identificación de brechas de los colaboradores de la División	E	R	R	I	C
2	Identificación de los colaboradores con necesidades de capacitación	E	R	E	I	C
3	Identificación de aspectos a mejorar en el desempeño laboral	R/E	R	E	C	C
4	Identificación de los funcionarios con necesidades de capacitación	R/E	R	E	R	C
5	Consolidación de información	C	R	E	I	C
6	Priorización de actividades y/o necesidades	I	R	E	C	I

d) Matriz de responsabilidades para el Sub Procedimiento de Elaboración del Plan Anual de Capacitación:

ID	ACTIVIDAD	DEPARTAMENTO DE GESTIÓN Y DESARROLLO DE LAS PERSONAS	ENCARGADO/A DE CAPACITACIÓN	ENC. SI	JEFATURAS
1	Asociación de actividades al presupuesto de capacitación	R	E	-	-
2	Calendarización de ejecución de las actividades	R	E	I	C
3	Determinación de los colaboradores a capacitar	R	E	C	C
4	Identificación de los recursos que se utilizarán en las capacitaciones	R	E	C	I
5	Identificación de los objetivos y resultados de cada capacitación	R	E	C	C
6	Elaboración final plan anual de capacitación	R	E	I	I

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Resolución Exenta que aprueba el Plan anual de capacitación	GC-20-16-02	Departamento de Gestión y Desarrollo de las Personas	5 años / Archivo Departamento	Papel o digital	Oficinas Departamento de Gestión y Desarrollo de las Personas / PC del analista del departamento
Listado de asistencia a capacitaciones		Departamento de Gestión y Desarrollo de las Personas	5 años / Archivo Departamento	Papel o digital	Oficinas Departamento de gestión y desarrollo de personas / PC del funcionario del departamento

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Procedimiento de Elaboración de Plan Anual de Capacitación, Formación y Entrenamiento (Control A.07.02.02)
2. Política de Gestión de Activos (Control A.8.1.2, A.8.1.3, A.8.3.1 Y A.8.3.3)
3. Procedimiento de Alta y Baja de Cuentas de Usuario a la Red y Servicios de Red (Control A.9.1.2, A.9.2.1, A.9.2.2 Y A.9.2.3)
4. Procedimiento de Gestión de Contraseñas (A.9.4.3, A.9.2.4 y A.9.3.1)
5. Política de Gestión de Controles Criptográficos y Contraseñas (Control A.10.1.1 y A.10.1.2)
6. Procedimiento de Gestión para el Desarrollo y Mantención de Software Seguro (A.14.1.1, A.14.1.2, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9 y A.12.1.4)
7. Procedimiento de Sincronización de Relojes (Control A.12.04.04)
8. Política de desarrollo seguro (control A.14.2.1)
9. Política de gestión de Incidentes control A.16.01.01
10. Procedimiento de Gestión de Incidentes (Control A.12.4.1, A.12.4.3, A.16.1.02, A.16.1.4, A.16.1.5 Y A.16.1.6)

Fecha: 2 de octubre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodríguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD (S)	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	María de la Luz González.	Jefa de DIEST (S)	
6	Ramón Gutiérrez P.	Jefe DAG (S)	
7	Sergio Hidalgo	Jefe Departamento de Auditoria	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Patrick Soto A.	Jefe TIC	
10	Andrea Soto Araya	Encargada de SSI	
11	Nicol Jeria O.	Encargada de Ciberseguridad	
12			

Agencia de Calidad de la Educación – Gobierno de Chile	Procedimiento de Alta y Baja de Cuentas de Usuario			
	Nivel de Confidencialidad	-	Páginas	**1 de 16**
			Versión	**0**
	Fecha versión del documento	**31-07-2019**	Código	**SGIC-PRO-A.9.1.2**
	Procedimiento de Alta y Baja de Cuentas de Usuario			

Procedimiento de Alta y Baja de Cuentas de Usuario
Control A.09.01.02

Tabla de Contenidos

Revisiones del Procedimiento....2
1. Objetivo. 3
2. Alcance. 3
3. Normas y Referencias. 3
4. Términos y Definiciones. 3
5. Roles y Responsabilidades 4
6. Definiciones para Alta y Baja de Usuarios, Accesos y Privilegios 5
6.1. Tipificación y Creación de Usuarios 5
6.2. Tipificación de Accesos y Privilegios 5
7. Modo de Operación 6
7.1 Flujo de Procedimiento para Alta de Usuario 7
7.2 Flujo de Procedimiento para Baja de Usuario 7
7.3 Flujo de Procedimiento para Entrega/Revocación de Accesos Especiales 8
7.4 Flujo de Procedimiento para Revisión de Asignación de Accesos 8
7.5 Matriz del Procedimiento para Alta de Usuario 9
7.6 Matriz del Procedimiento para Baja de Usuario 11
7.7 Matriz de Procedimiento para Entrega/Revocación de Accesos Especiales 12
7.8 Matriz de Procedimiento para Revisión de Asignación de Accesos 13
7.9 Matriz de Responsabilidades.... 14
8. Registro de Operación.... 16
9. Anexo....16

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de Información y Ciberseguridad	**Patrick Soto Jefe Unidad TIC**	**Andrea Soto Araya Encargada de Seguridad de la Información**	**Comité de Seguridad de la Información**

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	31/07/2019	Elaboración inicial	Todas

1. Objetivo.

Según lo establecido en la Política de Control de Acceso Físico y Lógico de la Agencia de Calidad de la Educación, en adelante la Agencia, el presente documento busca como objetivo establecer los procedimientos institucionales para realizar la gestión y administración de las cuentas de usuario para autenticación y acceso a los activos de información que se gestionan de forma digital en la organización.

2. Alcance.

Este documento considera los procedimientos asociados a todo el ciclo de vida de las cuentas de usuario de la Agencia de Calidad de la Educación, desde la asignación de accesos y privilegios al momento de darlas de alta, la administración de éstas a lo largo del tiempo, hasta la cancelación de los accesos y privilegios al momento de su baja.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27002:2013, el presente documento tiene su alcance sobre los siguientes controles:

1. A.09.01.02 – Control de Acceso Lógico: Acceso a la red y los servicios de red.
2. A.09.02.01 – Registro y Cancelación de Registro de Usuario
3. A.09.02.02 – Entrega de Acceso a los Usuarios.
4. A.09.02.03 – Administración de Derechos de Acceso Privilegiados.

3. Normas y Referencias.

a) NCh ISO 27,001:2013.

b) NCh ISO 27,002:2013.

c) Política de Control de Acceso Físico y Lógico, aprobada por Resolución Exenta N° 1027, de 2019, de la Agencia de Calidad de la Educación.

d) Política de Gestión de Activos, aprobada por Resolución Exenta N° 1527, de 2019, de la Agencia de Calidad de la Educación.

e) Procedimiento de Segregación de Funciones para Seguridad de la Información, año 2019.

4. Términos y Definiciones.

Amenaza	Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.
Riesgo	Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.
Autoridad	Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.
Evento de Seguridad de la Información	Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.
Incidente de	Se refiere a la Identificación y materialización de una amenaza o riesgo

Seguridad	detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.
Vulnerabilidad	Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.
Evento de Seguridad	Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia
Plan de Contingencia	Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.
Activos de Información	Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
Contactos críticos	Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o incidentes.
Red de Seguridad	Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.
Seguridad de la Información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.

5. Roles y Responsabilidades.

a) **Encargada de Seguridad de Información:** Como líder del Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC), será este rol el responsable de supervisar el correcto funcionamiento de los procedimientos que conforman este documento. Asimismo, se encargará de promover mejoras y actualizaciones a éste en función de cambios específicos o las necesidades de la Agencia a lo largo del tiempo, velando constantemente por que este documento esté alineado con la Política de Control de Acceso de la Organización. Por otra parte, deberá ejercer labores de asesoramiento en temáticas de seguridad asociadas al control de acceso que permitan apoyar la operación y mejora continua de este procedimiento.

b) **Jefatura Unidad de Tecnologías de la Información y Comunicación, de la División de Administración General:** Como dueño funcional de este procedimiento, será este rol el encargado de velar por la correcta aplicación de lo establecido en el presente documento, ejerciendo las labores necesarias para esto. Asimismo, será este rol el encargado de proponer e impulsar mejoras y actualizaciones a los procedimientos, en función tanto de los cambios que el entorno en el que se desenvuelve la Agencia pueda experimentar, así como de los requerimientos particulares que ésta experimente en el tiempo. Asimismo, será el encargado de velar por la ejecución de las actividades de revisión de las cuentas de usuario creadas a lo largo del tiempo, manteniendo así un control sobre el acceso y privilegios otorgados.

c) **Analista de Soporte al Usuario de la Unidad de Tecnologías de la Información y Comunicación:** Será este rol el principal encargado de la correcta ejecución de los procedimientos que conforman este documento, asegurando así la efectividad que éste busca en relación a la seguridad de información y ciberseguridad dentro del ciclo de gestión de las cuentas de usuario. Será su responsabilidad el proponer mejoras que eleven el nivel de madurez de la organización en estas temáticas mediante la aplicación de este procedimiento.

d) **Analista de Gestión y Desarrollo de las Personas, del Departamento de Gestión y Desarrollo de las Personas:** Será este rol el responsable de emitir las solicitudes de alta y baja de usuarios para gatillar la ejecución del procedimiento asociado respectivo.

e) **Dueño del Activo de Información:** Como rol responsable de la seguridad de los activos de información que se encuentran bajo su gestión, será su responsabilidad el autorizar todas las solicitudes de acceso/privilegios especiales definidas en este documento.

6. Definiciones para Alta y Baja de Usuarios, Accesos y Privilegios.

Según lo establecido tanto en su Política de Control de Acceso Físico y Lógico, como en las definiciones de seguridad de información descritas en las descripciones de cargo, la Agencia de Calidad de la Educación entrega las siguientes definiciones tanto para dar de alta como de baja usuarios en sus redes y sistemas de información, considerando el otorgamiento y revocación de accesos y privilegios según el ámbito de responsabilidades y descripciones de cargo de los diferentes usuarios:

6.1. Tipificación y Creación de Usuarios.

Como primera definición, se establece que la información mínima para una alta o baja segura y efectiva de usuarios en el dominio y servicios de red de la Agencia, es la siguiente:

a) Nombre y apellido de la persona asignada o a asignar a la cuenta de usuario.
b) RUN de la persona asignada o a asignar a la cuenta de usuario.
c) Rol asignado al interior de la organización.
d) Jefatura Directa.
e) Tipo de Usuario (Interno/Externo).
f) Fecha de alta de cuenta de usuario.
g) Fecha de caducidad de la cuenta de usuario (sólo si aplica. Parámetro a utilizar únicamente en solicitud de alta de usuario).

De esta forma, y, siempre que sea posible, se deberá automatizar el proceso de bloqueo o dada de baja de cuentas de usuario según el perfil de la cuenta y criticidad de la información asociada. El bloqueo de las cuentas de usuario, facultad de la Unidad de TIC se puede dar por las siguientes razones:

a) Por baja definitiva o caducidad de la relación laboral.
b) Inactividad de la cuenta de usuario.
c) Por intento de acceso fallido utilizando la misma cuenta de usuario en repetidas ocasiones.
d) Por cambio de funciones.

Dado lo anterior, y, considerando tanto su estructura de roles, responsabilidades y perfiles de cargo, así como la tecnología asociada a sus procesos críticos, la Agencia de Calidad de la Educación define los siguientes usuarios para dar de alta cuentas de usuario:

a) **Usuario Estándar:** Corresponde al tipo de usuario a crear que posee los mínimos accesos y privilegios según su perfil de cargo. De forma general, a toda nueva cuenta de usuario que no considera la administración de algún sistema o tecnología del servicio se le otorga este nivel de privilegios.

b) **Usuario Administrador:** Corresponde al tipo de usuario a crear que posee privilegios de administrador o privilegios superiores a los mínimos. De forma general, este nivel de privilegio se asigna a cuentas de usuarios con la Unidad de TIC y/o Jefaturas de División/Departamento que contemplan en su ámbito de responsabilidades la administración de sistemas y tecnologías.

6.2. Tipificación de Accesos y Privilegios.

De la misma forma, y considerando tanto la tipificación de usuarios descrita en el punto anterior, así como el perfil de cargo asociado a éstos, la Agencia de Calidad de la Educación define el siguiente

conjunto de accesos y privilegios para ser asignados tanto al momento de dar de alta por primera vez una cuenta de usuario específica, así como según las solicitudes especiales que puedan surgir a lo largo del tiempo:

a) **Accesos y privilegios estándar:** Según lo establecido en el punto de tipificación de usuarios de este documento, este tipo de accesos y privilegios están asociados al Usuario Estándar y deben ser asignados por la Unidad de TIC. Este tipo de accesos y privilegios consta del siguiente detalle:

    1. Acceso al dominio de la organización con mínimos privilegios. El usuario creado será agregado al grupo de usuario del controlador de dominio dependiendo de la División de la cual dependa el perfil de cargo.
    2. Anexo telefónico.
    3. Cuenta de correo electrónico. En caso de corresponder, se incluirá la cuenta de correo en grupos o listas de difusión asociadas al perfil de cargo del usuario.
    4. Acceso a impresoras con privilegios de impresión a blanco y negro o color según corresponda.
    5. Acceso a redes WiFi.

b) **Accesos y privilegios de administración:** Según lo establecido en el punto de tipificación de usuarios de este documento, este tipo de accesos y privilegios están asociados al Usuario Administrador y deben ser Asignados por la Unidad de TIC. Este tipo de accesos y privilegios consta del siguiente detalle:

    1. Acceso al dominio de la organización con privilegios de administración. El usuario creado será agregado al grupo de usuario del controlador de dominio dependiendo de la División de la cual dependa el perfil de cargo.
    2. Acceso a sistemas de información específicos con privilegios de administración.
    3. Anexo telefónico.
    4. Cuenta de correo electrónico. En caso de corresponder, se incluirá la cuenta de correo en grupos o listas de difusión asociadas al perfil de cargo del usuario.
    5. Acceso a impresoras con privilegios de impresión a blanco y negro o color según corresponda.
    6. Acceso a redes WiFi especiales o genéricas según corresponda.

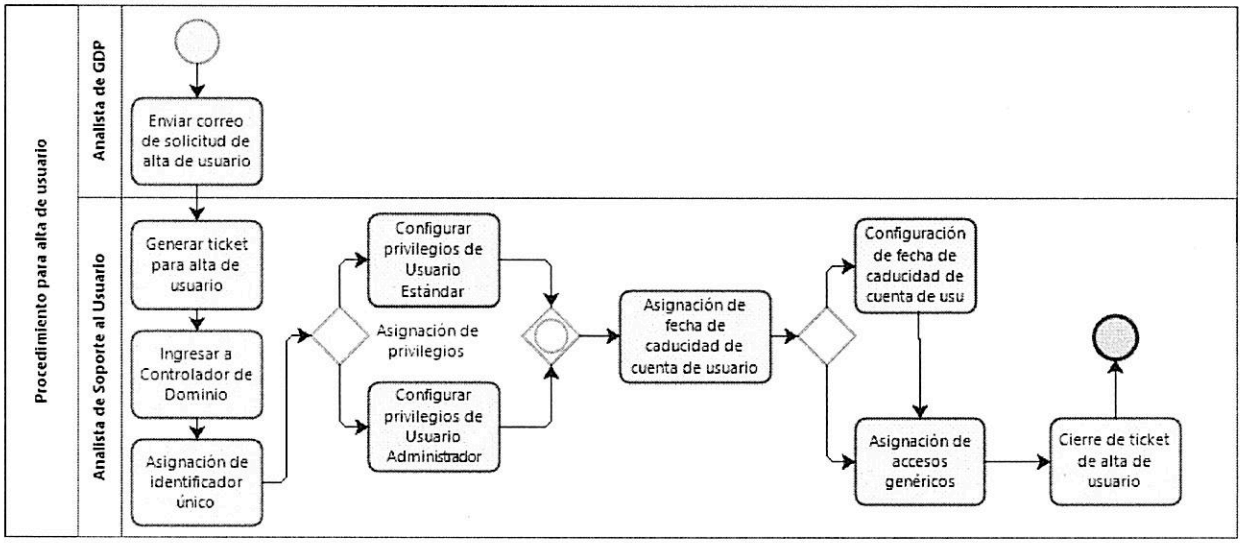
c) **Accesos y privilegios especiales:** Según lo establecido en el punto de tipificación de usuarios de este documento, existirán funciones de administración asignadas a roles de Jefatura de División, Departamento y/o Unidad, es decir, al Propietario y/o Custodio de los activos de información involucrados.

    Estas funciones corresponderán a la administración de sistemas de información específicos que tengan directa relación con la operación de estas áreas institucionales. De esta forma, la asignación de accesos y privilegios especiales corresponderá a todo acceso o privilegio que, no está dentro del alcance de gestión de la unidad de TIC (a menos que corresponda a carpetas compartidas o carpeta de Google Drive) pero que se añade a los accesos y privilegios otorgados por ésta, y del cual, serán los roles mencionados anteriormente los responsables de aprobar y ejecutar.

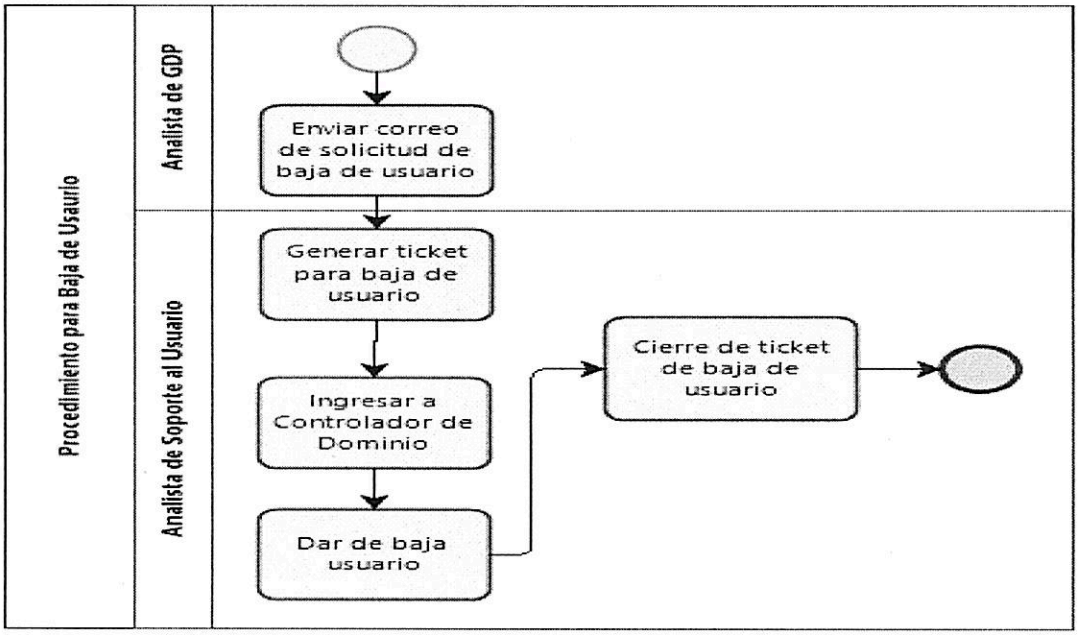
7. Modo de Operación.

A continuación, se describen los flujos procedimentales para la asignación del acceso a los usuarios, hacia las redes y los servicios de red:

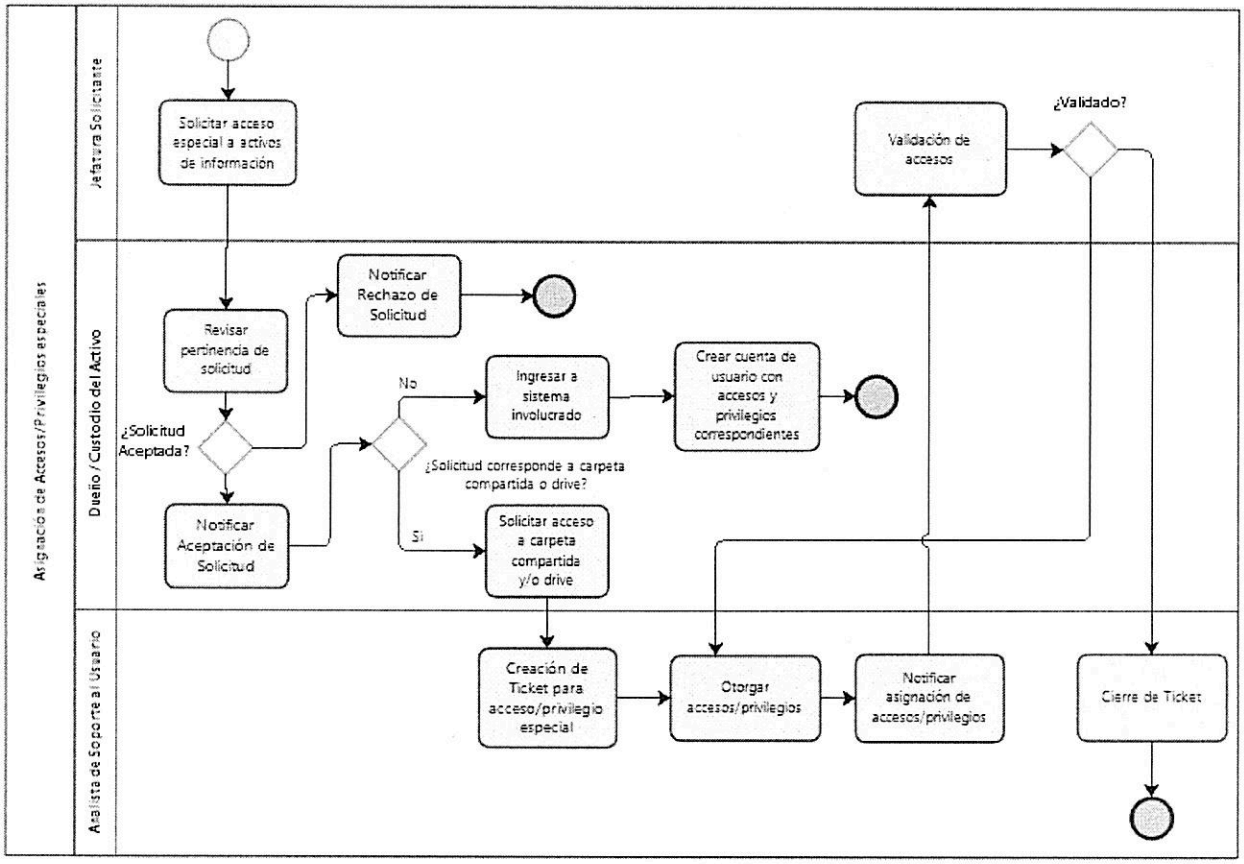
7.1 Flujo de Procedimiento para Alta de Usuario.



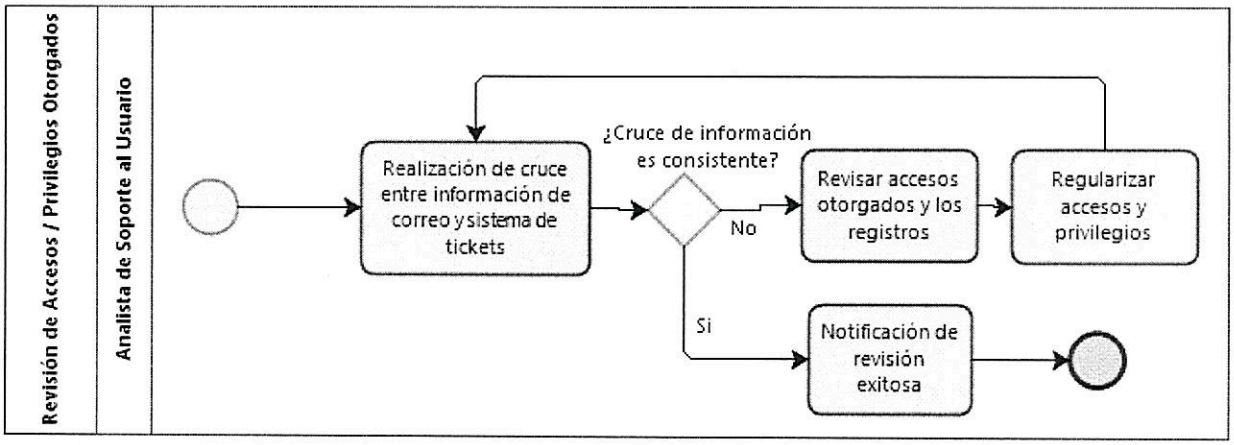
7.2 Flujo de Procedimiento para Baja de Usuario.



7.3 Flujo de Procedimiento para Entrega/Revocación de Accesos Especiales.



7.4 Flujo de Procedimiento para Revisión de Asignación de Accesos.



7.5 Matriz del Procedimiento para Alta de Usuario.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Enviar correo de solicitud de alta de usuario	Se debe enviar un correo electrónico al Jefe de la Unidad de TIC solicitando la creación del nuevo usuario. En éste se debe detallar la siguiente información: 1. Nombres y apellidos de la persona asignada o a asignar a la cuenta de usuario. 2. RUT de la persona asignada o a asignar a la cuenta de usuario. 3. Rol asignado al interior de la organización. 4. Jefatura Directa. 5. Tipo de Usuario (Interno/Externo). 6. Fecha de alta de cuenta de usuario. 7. Fecha de Caducidad de la cuenta de usuario.	Analista GDP	2
2	Generar Ticket de solicitud de alta de usuario.	Para llevar un registro de las altas de usuario, se debe generar, en función de lo descrito en el correo al que hace alusión la Actividad (1), un ticket en el sistema de mesa de ayuda de la Agencia.	Analista de Soporte al Usuario	3
3	Ingresar a Controlador de Dominio	Se debe ingresar al controlador de dominio de la Agencia, Active Directory, para empezar la creación del usuario nuevo.	Analista de Soporte al Usuario	4
4	Asignación de identificador único	Según lo especificado en la Política de Control de Acceso Físico y Lógico, se debe asignar un nombre inequívoco de identificación del nuevo usuario. La asignación de éste debe seguir la siguiente nomenclatura: - "nombreapellido" para usuarios internos de la Agencia. - "nombreapellidoext" para usuarios externos a la organización.	Analista de Soporte al Usuario	5

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
5	Asignación de privilegios	Según lo establecido en el ticket de solicitud de alta con respecto al rol asignado al nuevo usuario, la asignación de recursos puede darse de la siguiente manera: - Usuario Estándar: Corresponde a la asignación de los mínimos privilegios. Está asociada a roles que no consideran tareas de administración de tecnologías en su ámbito de responsabilidades (6). - Usuario Administrador: Corresponde a la asignación de los privilegios de administración sobre sistemas tecnológicos de la Agencia. Son asignados a roles asociados a la Unidad de TIC y/o jefaturas (7).	Analista de Soporte al Usuario	6 o 7
6	Configurar privilegios de Usuario Estándar	Se debe configurar la asignación de los mínimos privilegios para el nuevo usuario según lo definido en este documento.	Analista de Soporte al Usuario	8
7	Configurar privilegios de Usuario Administrador	Se debe configurar la asignación de privilegios de administración para el nuevo usuario según lo definido en este documento.	Analista de Soporte al Usuario	8
8	Asignación de fecha de caducidad de cuenta de usuario	En consecuencia, con lo estipulado en la Política de Control de Acceso Físico y Lógico, siempre que sea posible se deben automatizar las tareas relacionadas con la baja de usuarios. Por ende, se podrían producir los siguientes escenarios: - El ticket de solicitud de alta de usuario especifica una fecha de caducidad para la cuenta de usuario (9). - El ticket de solicitud de alta de usuario NO especifica una fecha de caducidad de la cuenta de usuario (10).	Analista de Soporte al Usuario	9 o 10
9	Configuración de fecha de caducidad de cuenta de usuario	Se debe configurar que de forma automática, al cumplirse la fecha de caducidad de la cuenta de usuario, ésta sea movida al grupo de "Usuarios Deshabilitados".	Analista de Soporte al Usuario	10

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
10	Asignación de accesos genéricos	Una vez creado el usuario en el dominio, se deben hacer entrega de los demás accesos según corresponda. Éstos son: - Cuenta de correo electrónico con asignación a grupos y listas de difusión según corresponda. - Acceso a impresión con los privilegios correspondientes. - Acceso a redes Wifi.	Analista de Soporte al Usuario	11
11	Cierre de ticket de alta de usuario	Una vez creada la cuenta de usuario y otorgados los accesos al dominio y los servicios de red.se debe dar por cerrado el ticket de mesa de ayuda asociado.	Analista de Soporte al Usuario	FIN

7.6 Matriz del Procedimiento para Baja de Usuario.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Enviar correo de solicitud de baja de usuario	Se debe Enviar un correo a la Unidad de TIC solicitando la baja de una cuenta de usuario previamente dada de alta. En éste se debe detallar la siguiente información: - Nombres y apellidos de persona asignada a la cuenta de usuario. - Rol asignado en la organización - Jefatura. - Motivo de dada de baja.	Analista GDP	2
2	Generar Ticket para baja de usuario.	Para llevar un registro de las bajas de usuario, se debe generar, en función de lo descrito en el correo al que hace alusión la Actividad (1), un ticket en el sistema de mesa de ayuda de la Agencia.	Analista de Soporte al Usuario	3
3	Ingresar a Controlador de Dominio	Se debe ingresar al controlador de dominio de la Agencia, Active Directory, para dar de baja al usuario según lo estipulado en el ticket solicitud de baja.	Analista de Soporte al Usuario	4
4	Dar de baja usuario	Para dar de baja el usuario, se procede a bloquear y mover la cuenta asociada al grupo de desactivados. Esto automáticamente inhabilita cualquier acceso a la red y los servicios de red que la cuenta pudiese tener asignado.	Analista de Soporte al Usuario	5

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
5	Cierre de ticket de baja de usuario	Una vez dada de baja la cuenta de usuario y deshabilitados los accesos al dominio y los servicios de red.se debe dar por cerrado el ticket de mesa de ayuda asociado.	Analista de Soporte al Usuario	FIN

7.7 Matriz de Procedimiento para Entrega de Accesos Especiales.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Solicitar acceso especial a activos de información	Se debe enviar por correo electrónico al Dueño/Custodio la solicitud de autorización para obtención de acceso especial. Se debe detallar la siguiente información: - Nombres y apellidos de la persona a la cual se le busca conceder el acceso. - Nombre de usuario asociado, el cual debe coincidir con el nombre de usuario del controlador del dominio. - Motivo de la solicitud.	Jefatura Solicitante	2
2	Revisar pertinencia de la solicitud	Se debe validar la pertinencia de la solicitud realizada. Se pueden dar las siguientes opciones: - La solicitud es rechazada (2A). - La solicitud es aceptada (3).	Dueño/Custodio del activo	2A o 3
2A	Notificar rechazo de solicitud	Se debe notificar por correo electrónico el rechazo de la solicitud, detallando las razones de ésta.	Dueño/Custodio del activo	FIN
3	Notificar aceptación de solicitud	Se debe notificar por correo electrónico la aceptación de la solicitud. Se pueden dar las siguientes opciones: - El acceso a otorgar es en sistema tecnológico específico (3A). - El acceso a otorgar es en carpeta compartida o carpeta de drive (4).	Dueño/Custodio del activo	3A o 4
3A	Ingresar a sistema involucrado	Para conceder el acceso al sistema específico involucrado en la solicitud, se debe ingresar a éste con perfil de administrador.	Dueño/Custodio del activo	3B
3B	Crear cuenta de usuario con accesos y privilegios correspondientes	Se debe proceder a crear la cuenta de usuario con sus respectivos privilegios según lo indicado la solicitud.	Dueño/Custodio del activo	FIN

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
4	Solicitar acceso a carpeta compartida o carpeta drive	Se debe solicitar mediante correo electrónico la entrega del acceso con sus respectivos privilegios, según lo indicado en la solicitud.	Dueño/Custodio del activo	5
5	Creación de ticket para acceso/privilegio especial	Para llevar un registro de las bajas de usuario, se debe generar, en función de lo descrito en el correo al que hace alusión la Actividad (1), un ticket en el sistema de mesa de ayuda de la Agencia.	Analista de Soporte al Usuario	6
6	Otorgar accesos/privilegios	Se debe efectuar la asignación de accesos con sus privilegios en la carpeta compartida o carpeta drive según corresponda.	Analista de Soporte al Usuario	7
7	Notificar asignación de accesos/privilegios	Se debe notificar mediante correo electrónico a la jefatura solicitante, que los accesos y privilegios fueron concedidos para proceder a su validación.	Analista de Soporte al Usuario	8
8	Validación de accesos	Se debe validar que los accesos y privilegios se hayan otorgado según lo solicitado. Se pueden dar las siguientes alternativas: - Los accesos/privilegios no corresponden a lo solicitado (6). - Los accesos y privilegios corresponden a lo solicitado (9).	Jefatura Solicitante	9
9	Cierre de Ticket	Una vez validada la asignación de acceso/privilegio, se debe cerrar el ticket asociado.	Analista de Soporte al Usuario	FIN

7.8 Matriz de Procedimiento para Revisión de Asignación de Accesos.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Realización de cruce entre información de correo y sistema de tickets	Para realizar la revisión de los accesos concedidos en la organización, se debe realizar un cruce entre los tickets de solicitud de alta y baja de accesos, privilegios y usuarios, con la efectiva asignación o baja de éstos en el dominio, carpetas compartidas y carpetas drive. Se pueden dar las siguientes alternativas: - El cruce de información no es consistente (2). - El cruce de información es consistente (4)	Analista de Soporte al Usuario	2 o 4

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
2	Revisar accesos otorgados y los registros	Se debe hacer una revisión de las inconsistencias detectadas.	Analista de Soporte al Usuario	3
3	Regularizar accesos y privilegios	Se debe regularizar la baja de usuarios según corresponda.	Analista de Soporte al Usuario	1
4	Notificación de revisión exitosa	Se debe notificar a la Encargada de Seguridad de la Información, la revisión exitosa de los accesos, donde se deben detallar si existieron inconsistencias en el proceso que qué medidas de tomaron para subsanarlas.	Analista de Soporte al Usuario	FIN

7.9 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

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

De esta forma, la matriz de responsabilidades para el alta de usuarios de la Agencia se estructura de la siguiente manera:

ID	ACTIVIDAD	Jefatura TIC	Analista Soporte Usuario	Analista GDP	Jefatura Solicitante
1	**Enviar correo de solicitud de alta de usuario**	-	I	R/E	A
2	**Generar Ticket de solicitud de alta de usuario.**	R	E	-	-
3	**Ingresar a Controlador de Dominio**	R	E	-	-
4	**Asignación de identificador único**	R	E	C	
5	**Asignación de privilegios**	R	E	C	-
6	**Configurar privilegios de Usuario Estándar**	R	E	C	-
7	**Configurar privilegios de Usuario Administrador**	R	E	C	-
8	**Asignación de fecha de caducidad de cuenta de usuario**	R	E	C	-
9	**Configuración de fecha de caducidad de cuenta de usuario**	R	E	-	-
10	**Asignación de accesos genéricos**	R	E	-	-
11	**Cierre de ticket de alta de usuario**	R	E	I	I

La matriz de responsabilidades asociada a la baja de usuarios de la Agencia se estructura de la siguiente manera:

ID	ACTIVIDAD	Jefatura TIC	Analista Soporte Usuario	Analista GDP
1	**Enviar correo de solicitud de baja de usuario**	-	I	R/E
2	**Generar Ticket para baja de usuario.**	R	E	I
3	**Ingresar a Controlador de Dominio**	R	E	-
4	**Dar de baja usuario**	R	E	-
5	**Cierre de ticket de baja de usuario**	R	E	I

La matriz de responsabilidades asociada a la entrega y de accesos especiales de la Agencia se estructura de la siguiente manera:

ID	ACTIVIDAD	Jefatura TIC	Analista Soporte Usuario	Dueño / Custodio	Jefatura Solicitante
1	**Solicitar acceso especial a activos de información**	-	-	I	R/E
2	**Revisar pertinencia de la solicitud**	-	-	R/E	C
2A	**Notificar rechazo de solicitud**	-	-	R/E	I
3	**Notificar aceptación de solicitud**	-	-	R/E	I
3A	**Ingresar a sistema involucrado**	-	-	-	-
3B	**Crear cuenta de usuario con accesos y privilegios correspondientes**	-	-	R/E	I
4	**Solicitar acceso a carpeta compartida o carpeta drive**	I	I	R/E	I
5	**Creación de ticket para acceso/privilegio especial**	R	E	I	I
6	**Otorgar accesos/privilegios**	R	E	C	C
7	**Notificar asignación de accesos/privilegios**	R	E	I	I
8	**Validación de accesos**	I	C	I	R/E
9	**Cierre de Ticket**	R	E	I	I

La matriz de responsabilidades asociada a la revisión de accesos de la Agencia se estructura de la siguiente manera:

ID	ACTIVIDAD	Jefatura	Analista Analista Soporte Usuario	Encargada SI
1	Realización de cruce entre información de correo y sistema de tickets	R	E	I
2	Revisar accesos otorgados y los registros	R	E	-
3	Regularizar accesos y privilegios	R	E	-
4	Notificación de revisión exitosa	R	E	I

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Notificación de revisión de accesos	-	Analista de Soporte al Usuario	1 años / Archivo UTIC	Digital	Correo Electrónico
Consolidado de solicitudes de baja de usuario en mesa de ayuda	-	Analista de Soporte al Usuario	1 años / Archivo UTIC	Digital	Sistema de Mesa de Ayuda

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

1. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
   1. Procedimiento de Elaboración de Plan Anual de Capacitación, Formación y Entrenamiento (Control A.07.02.02)
   2. Política de Gestión de Activos (Control A.8.1.2, A.8.1.3, A.8.3.1 Y A.8.3.3)
   3. Procedimiento de Alta y Baja de Cuentas de Usuario a la Red y Servicios de Red (Control A.9.1.2, A.9.2.1, A.9.2.2 Y A.9.2.3)
   4. Procedimiento de Gestión de Contraseñas (A.9.4.3, A.9.2.4 y A.9.3.1)
   5. Política de Gestión de Controles Criptográficos y Contraseñas (Control A.10.1.1 y A.10.1.2)
   6. Procedimiento de Gestión para el Desarrollo y Mantención de Software Seguro (A.14.1.1, A.14.1.2, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9 y A.12.1.4)
   7. Procedimiento de Sincronización de Relojes (Control A.12.04.04)
   8. Política de desarrollo seguro (control A.14.2.1)
   9. Política de gestión de Incidentes control A.16.01.01
   10. Procedimiento de Gestión de Incidentes (Control A.12.4.1, A.12.4.3, A.16.1.02, A.16.1.4, A.16.1.5 Y A.16.1.6)

Fecha: 2 de octubre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodríguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD (S)	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	María de la Luz González.	Jefa de DIEST (S)	
6	Ramón Gutiérrez P.	Jefe DAG (S)	
7	Sergio Hidalgo	Jefe Departamento de Auditoria	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Patrick Soto A.	Jefe TIC	
10	Andrea Soto Araya	Encargada de SSI	
11	Nicol Jeria O.	Encargada de Ciberseguridad	
12			

1

Procedimiento de Gestión de Contraseñas
Control A.9.4.3

Tabla de Contenidos

Revisiones del procedimiento..... 2
1. Objetivo. 3
2. Alcance. 3
3. Normas y Referencias. 3
4. Términos y Definiciones. 3
5. Roles y Responsabilidades. 4
6. Seguridad en la Gestión de las Contraseñas 4
6.1. Entrega de Contraseñas.....4
6.2. Cambios de Contraseñas 5
6.3. Gestión de Contraseñas 5
7. Modo de Operación 6
7.1 Flujo de Procedimiento para Gestión de Contraseñas del Usuario 6
7.2 Matriz del Procedimiento para Gestión de Contraseñas del Usuario.....6
7.3 Matriz de Responsabilidades. 8
8. Registro de Operación. 9
9. Anexo.....9

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de Información y Ciberseguridad	Patrick Soto Jefe Unidad TIC	Andrea Soto Encargada de Seguridad de Información	Comité de Seguridad de Información

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	26/08/2019	Elaboración inicial	Todas

1. Objetivo.

Según lo establecido en la Política de Seguridad de la Información de la Agencia de Calidad de la Educación, en adelante Agencia, el presente documento tiene por objetivo establecer la secuencia de pasos para gestionar correctamente las contraseñas utilizadas por los usuarios de los diferentes sistemas asociados a la institución, particularmente con el objetivo de garantizar la seguridad de la información en este proceso en cuestión.

2. Alcance.

El presente procedimiento debe ser aplicado a todos los funcionarios y funcionarias, de planta, contrata, y honorarios de la Agencia de Calidad de la Educación y a terceros, que, dado el cumplimiento de sus responsabilidades de cargo, requieran acceso a algún sistema asociado con la Agencia de Calidad de la Educación mediante una contraseña.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27001:2013, el presente documento tiene su alcance sobre los siguientes controles:

- A.09.04.03. – Sistema de Gestión de Contraseñas
- A.09.02.04 - Administración de información secreta de autenticación de usuarios
- A.09.03.01 - Uso de información de autenticación secreta

3. Normas y Referencias.

- NCh ISO 27,001:2013.
- NCh ISO 27,002:2013.
- Política de Control de Acceso Físico y Lógico, aprobada por Resolución Exenta N° 1027, de 2019, de la Agencia de Calidad de la Educación.

4. Términos y Definiciones.

Contraseña	Una contraseña (también conocida como clave o password), es una forma de autenticación que hace utilización de información secreta para controlar el acceso hacia algún recurso. Esta es de uso personal, y debe mantenerse en secreto. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.
Activos de Información	Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
Seguridad de la Información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.
Active Directory (AD)	Repositorio de cuentas de usuarios y equipos asociados a la organización en cuestión.

5. Roles y Responsabilidades.

a) **Encargada de Seguridad de Información:** Como líder del Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC), será este rol el responsable de supervisar el correcto funcionamiento de este procedimiento. Asimismo, se encargará de promover mejoras y actualizaciones a éste en función de cambios específicos o las necesidades de la Agencia a lo largo del tiempo. Asimismo, debe velar por que este documento esté alineado con la Política de Control de Acceso de la Organización. Adicionalmente, deberá ejercer labores de asesoramiento en temáticas de seguridad asociadas al control de acceso que permitan apoyar la operación y mejora continua de este procedimiento.

b) **Administrador de Plataforma de la Unidad de Tecnologías de la Información y Comunicación:** Es este el encargado de efectuar la entrega de las contraseñas en conformidad con lo establecido en el Procedimiento de Alta y Baja de Usuarios. Adicionalmente, realiza la correspondiente gestión sobre estas mediante la utilización del controlador de dominio.

c) **Usuario:** Hace referencia al funcionario/a que cuenta – o debe contar – con acceso a los sistemas o recursos tecnológicos de la agencia según su ámbito de responsabilidades. Tiene la responsabilidad de mantener secreta la información de autenticación que se le ha hecho disponible.

d) **Jefatura Unidad de Tecnologías de la Información y Comunicación, de la División de Administración General:** Será este rol el encargado de velar por la correcta ejecución del presente procedimiento. Asimismo, deberá promover mejoras y actualizaciones que respondan tanto al cambio del entorno como a requerimientos de la Agencia.

6. Seguridad en la Gestión de las Contraseñas.

La seguridad de las contraseñas es de gran importancia para la mantención de la integridad, confidencialidad y disponibilidad de los activos de información que habitan dentro de los sistemas de la institución. En función de lo anterior, y en vista de que cada usuario es responsable de la gestión de su contraseña personal, es de suma importancia que esta se mantenga confidencial y privada en todo momento. De esta manera, cualquier intento de difusión o exfiltración de esta información de carácter personal queda estrictamente prohibida.

6.1. Entrega de Contraseñas.

Todas las contraseñas serán entregadas en conformidad con lo establecido en la Política de Control de Acceso y el Procedimiento de Alta y Baja de Usuarios, procurando garantizar la confidencialidad de estas en la realización del proceso. Sin embargo, existen ciertas consideraciones que se deben tener presentes al momento de recibir esta información:

a) Una vez sea entregada la contraseña al usuario, este debe hacer ingreso al sistema lo antes posible, posterior a lo cual se deberá realizar un cambio obligatorio de contraseña entregada por la Unidad de TIC. Este cambio de contraseña deberá ser realizado en conformidad con lo establecido en el presente procedimiento. En caso de que el sistema no exija realizar este cambio de forma automática, será responsabilidad del usuario realizarlo.

b) Al momento de crear su primera contraseña, se debe considerar que ésta debe contar como mínimo con 7 caracteres alfanuméricos. Adicionalmente, y como recomendación de seguridad, se deberá intentar no utilizar contraseñas de fácil deducción.

c) La contraseña entregada se deberá mantener en secreto hasta que esta sea cambiada durante el primer ingreso a la plataforma en cuestión, con el objetivo de evitar que individuos externos a la organización tengan acceso a ésta.

d) El encargado de plataforma deberá velar por la aplicación de estos controles mediante la configuración del controlador de dominio.

6.2. Cambios de Contraseñas.

Como buena práctica de seguridad, las contraseñas deberán ser cambiadas en conformidad con lo establecido en la Política de Control de Acceso. Sin embargo, en función de la importancia de la información de autenticación, es necesario tener ciertas consideraciones referentes a este proceso:

a) Cualquier contraseña utilizada dentro de la Agencia debe contar como mínimo con 7 caracteres alfanuméricos. Adicionalmente, y como recomendación de seguridad, se deberá intentar no utilizar contraseñas de fácil deducción.

b) Los cambios de contraseña deberán ser realizados de forma obligatoria cada tres (3) meses, con la finalidad de proteger los accesos a los sistemas de la organización. Estos cambios deberán estar de acuerdo con lo establecido en el punto anterior.

c) Al realizar cambios de contraseñas, los usuarios no podrán reutilizar alguna de las últimas cinco (5) contraseñas anteriormente usadas.

d) El cambio de contraseña debe ser realizado con el equipo o laptop conectado a la red de la Agencia.

e) El encargado de plataforma deberá velar por la aplicación de estas consideraciones mediante la utilización de AD.

6.3. Gestión de Contraseñas.

Adicionalmente a cualquier consideración anteriormente mencionada, es de gran importancia gestionar correctamente esta información de autenticación personal. En función de lo anterior, es relevante destacar que el cuidado de esta información es de responsabilidad personal de los usuarios de los sistemas, para lo cual, se deberán tener en cuenta las siguientes consideraciones:

a) Las contraseñas no podrán ser almacenadas físicamente en lugares visibles. En función de lo anterior, se deben evitar malas prácticas como guardar las contraseñas de forma visible en el puesto de trabajo, por el contrario, esta deberá ser resguardada con todas las precauciones pertinentes para garantizar la confidencialidad de la clave en cuestión.

b) Los usuarios de los sistemas deben recordar en todo momento que el cuidado de las contraseñas es de su propia responsabilidad, por lo que debe velar por la confidencialidad de esta información.

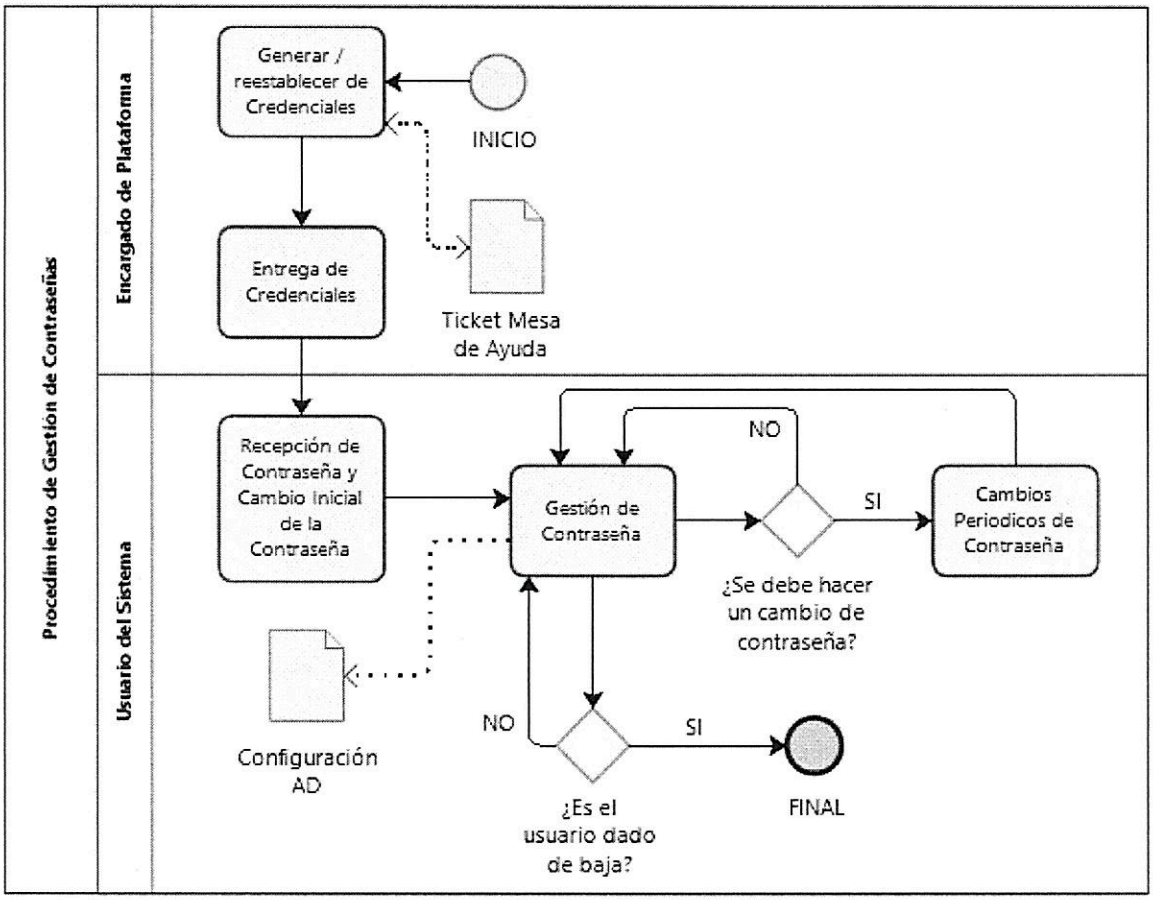
c) Para el caso de información de autenticación secreta compartida, los usuarios se comprometen a mantener esta información dentro del grupo en cuestión.

d) Las contraseñas asociadas a los sistemas no podrán ser compartidas mediante la utilización de aplicaciones de mensajería instantánea, sino que se deben respetar el correo electrónico como canal oficial de entrega de éstas.

7. Modo de Operación.

A continuación, se describen los flujos procedimentales para la Gestión de Contraseñas:

7.1 Flujo de Procedimiento para Gestión de Contraseñas del Usuario.



7.2 Matriz del Procedimiento para Gestión de Contraseñas del Usuario.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Generación / Re establecimiento de Credenciales	Se deberán generar las credenciales del usuario que ha sido dado de alta en concordancia con lo establecido en el presente procedimiento. Esto deberá responder al ticket levantado en la mesa de ayuda. Para el caso del restablecimiento de la contraseña, la solicitud por parte del usuario se debe realizar vía telefónica o presencial por el mismo usuario que realiza la solicitud.	Encargado de Plataforma	2
2	Entrega de Credenciales	El encargado de plataforma deberá hacer entrega de las credenciales generadas vía mail al usuario que ha sido dado de alta. Mediante esta entrega, se establece la declaración de que el usuario mantenga su información de autenticación secreta de manera personal.	Encargado de Plataforma	3
3	Recepción de Contraseña y Cambio Inicial de la Contraseña	Una vez que el usuario ha recibido correctamente las credenciales en cuestión, este deberá hacer ingreso a la plataforma, el cual solicitará un cambio de contraseña. Es importante especificar que cualquier cambio de contraseña deberá ser realizado en función con lo establecido en el presente procedimiento.	Usuario	4

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
4	Gestión de Contraseñas	Las contraseñas deberán ser debidamente gestionadas, en conformidad con lo establecido en el presente documento. Asimismo, es de gran importancia especificar que la protección de las claves en cuestión, son de exclusiva responsabilidad de los usuarios. En función de lo anterior, pueden ocurrir dos posibles escenarios: - El usuario debe efectuar un cambio obligado de la contraseña (5). - El usuario es dado de baja (FIN). **NOTA:** En caso de que el usuario sea dado de baja, esto deberá ser reflejado en un ticket a la mesa de ayuda. Asimismo, la baja del usuario es tratada en el Procedimiento de Alta y Baja de Usuarios.	Usuario	5 o FIN
5	Cambios Periódicos de Contraseña	En conformidad con lo establecido en este procedimiento, los usuarios deberán realizar cambios periódicos de contraseñas cada tres (3) meses. Adicionalmente, cualquier cambio de contraseña no deberá reutilizar ninguna de las últimas cinco (5) credenciales utilizadas. Esto es establecido según la configuración de AD.	Usuario	4

7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

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

De esta forma, la matriz de responsabilidades para el alta de usuarios en la red y los sistemas de red de la Agencia se estructura de la siguiente manera:

ID	ACTIVIDAD	ENC. SI	Admin. Plataforma	Usuario	Jefatura TIC
1	**Generar Credenciales**	I	R / A / E	I	I
2	**Entrega de Credenciales**	I	R / A / E	I	I
3	**Recepción y Cambio Contraseña**	I	I / C	R / A / E	I
4	**Gestión de Contraseña**	-	A / C	R / E	-
5	**Cambios Periódicos de Contraseña**	-	A / C	R / E	-

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Solicitud Creación Credenciales	-	Encargado de Plataforma	1 año / Ticket	Digital	Mesa de Ayuda
Configuración de Contraseñas	-	Encargado de Plataforma	4 años / Configuración AD	Digital	Carpeta Compartida TIC

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

1. Aprobación de los siguientes procedimientos y políticas de seguridad de la Información:
   1. Procedimiento de Elaboración de Plan Anual de Capacitación, Formación y Entrenamiento (Control A.07.02.02)
   2. Política de Gestión de Activos (Control A.8.1.2, A.8.1.3, A.8.3.1 Y A.8.3.3)
   3. Procedimiento de Alta y Baja de Cuentas de Usuario a la Red y Servicios de Red (Control A.9.1.2, A.9.2.1, A.9.2.2 Y A.9.2.3)
   4. Procedimiento de Gestión de Contraseñas (A.9.4.3, A.9.2.4 y A.9.3.1)
   5. Política de Gestión de Controles Criptográficos y Contraseñas (Control A.10.1.1 y A.10.1.2)
   6. Procedimiento de Gestión para el Desarrollo y Mantención de Software Seguro (A.14.1.1, A.14.1.2, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9 y A.12.1.4)
   7. Procedimiento de Sincronización de Relojes (Control A.12.04.04)
   8. Política de desarrollo seguro (control A.14.2.1)
   9. Política de gestión de Incidentes control A.16.01.01
   10. Procedimiento de Gestión de Incidentes (Control A.12.4.1, A.12.4.3, A.16.1.02, A.16.1.4, A.16.1.5 Y A.16.1.6)

Fecha: 2 de octubre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodríguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD (S)	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	María de la Luz González.	Jefa de DIEST (S)	
6	Ramón Gutiérrez P.	Jefe DAG (S)	
7	Sergio Hidalgo	Jefe Departamento de Auditoría	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Patrick Soto A.	Jefe TIC	
10	Andrea Soto Araya	Encargada de SSI	
11	Nicol Jeria O.	Encargada de Ciberseguridad	
12			

1

Procedimiento de Gestión de Incidentes
Control A.16.01.05

Tabla de Contenidos

Revisiones del procedimiento....2
1. Objetivo....3
2. Alcance....3
3. Normas y Referencias....3
4. Términos y Definiciones....3
5. Roles y Responsabilidades....4
6. Definiciones para la Gestión de Incidentes de Seguridad de Información....5
6.1 Detección y Notificación de Eventos o Incidentes de Seguridad....5
6.2 Evaluación y Decisión sobre Eventos de Seguridad....6
6.3 Comunicación durante Incidentes....7
6.4 Cierre de Incidentes de Seguridad....7
6.5 Informe de Incidentes de Seguridad....8
6.6 Aprendizaje de los Incidentes de Seguridad....8
7. Modo de Operación....9
7.1 Flujo de Procedimiento para Gestión de Incidentes....9
7.2 Matriz del Procedimiento Gestión de Incidentes....10
7.3 Matriz de Responsabilidades.....12
8. Registro de Operación.....13
9. Anexo....14

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de Información y Ciberseguridad	**Nicol Jeria Encargada de Ciberseguridad**	**Andrea Soto Encargada de Seguridad de la Información**	**Comité de SGSIC**

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	30/09/2019	Actualización	Todas

1. Objetivo.

En concordancia con lo establecido en la Política de Gestión de Incidentes de Seguridad de la Información y Ciberseguridad, la Agencia de Calidad de la Educación, en adelante la Agencia, el presente documento tiene por objetivo entregar los lineamientos procedimentales para hacer frente a los incidentes que puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información de la institución, así como la continuidad operativa de los procesos más críticos de su cadena de valor.

2. Alcance.

Este procedimiento debe aplicarse ante cualquier evento/incidente, abarcando su detección, respuesta y recuperación. Asimismo, a todo el personal de contrata, honorarios de la Agencia de Calidad de la Educación y externo que, de forma directa o indirecta, tenga relación con la Agencia de Calidad de la Educación.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27002:2013, el presente documento tiene su alcance sobre los siguientes controles:

- A.16.01.02 – Informe de Eventos de Seguridad de la Información.
- A.16.01.04 – Evaluación y Decisión sobre los Eventos de Seguridad de la Información.
- A.16.01.05 – Respuesta ante Incidentes de Seguridad de la Información.
- A.16.01.06 – Aprendizaje de los Incidentes de Seguridad de la Información.
- A.12.04.01 – Registro de Evento.
- A.12.04.03 - Registro del Administrador y del Operador.

3. Normas y Referencias.

- NCh ISO 27,001:2013.
- NCh ISO 27,002:2013.
- Política de Gestión de Incidentes de Seguridad de la Información y Ciberseguridad, aprobada por Resolución Exenta N° 1338, de 2019, de la Agencia de Calidad de la Educación.
- Taxonomías de clasificación de incidentes recomendada por el CSIRT Gubernamental, basado en el documento original, Reference Incident Classification Taxonomy, ENISA, publicado el 26 de enero de 2018.

4. Términos y Definiciones.

Amenaza	Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.
Riesgo	Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.
Autoridad	Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del

	negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.
Evento de Seguridad de la Información	Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.
Incidente de Seguridad	Se refiere a la Identificación y materialización de una amenaza o riesgo detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.
Vulnerabilidad	Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.
Evento de Seguridad	Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia
Plan de Contingencia	Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.
Activos de Información	Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
Contactos críticos	Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o incidentes.
Red de Seguridad	Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.
Seguridad de la Información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.
CSIRT de Gobierno	Equipo de Respuesta Ante Incidentes de Ciberseguridad del Gobierno.

5. Roles y Responsabilidades.

a) **Usuarios(as):** Será responsabilidad de los usuarios de la Agencia, el reportar cualquier evento, incidente o anomalía que pudiese vulnerar la confidencialidad, disponibilidad, integridad y/o privacidad de los activos de información de la institución.

b) **Propietario/Dueño de los Activos de Información:** Será responsabilidad del dueño de los activos afectados por un evento o incidente, como principal responsable y conocedor de la criticidad de éstos para la institución, el apoyar la toma de decisiones asociada a la respuesta de la organización para mitigar el incidente.

c) **Custodio de los Activos de Información:** Como custodio designado de el o los activos de información comprometidos en un incidente o evento, será responsabilidad de este rol el complementar al rol de Propietario de los activos durante el incidente.

d) **Encargada de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC) de la Agencia, será el rol encargado de liderar la gestión del incidente durante todo su ciclo, apoyando en la toma de decisiones y

durante todo el ciclo de la respuesta y recuperación del incidente. Adicional a lo anterior, será responsabilidad de este rol el velar por la correcta documentación y registro de los antecedentes del incidente. Finalmente, es parte de su ámbito de responsabilidades el generar las instancias de aprendizaje y mejora continua posterior a la recuperación de la situación adversa antes mencionada.

e) **Encargado de Ciberseguridad:** Como rol perteneciente al SGSIC, será responsable de apoyar y asesorar al Comité de Seguridad de Información.
f) **Jefatura Unidad de Tecnologías de la Información y Comunicación:** Dada la implicancia estratégica de la tecnología para la operación de la Agencia, será este rol el encargado de liderar las acciones de diagnóstico, contención y recuperación de los incidentes que afecten la tecnología de información y comunicación de la institución. Asimismo, será este rol el encargado de asesorar desde su ámbito de responsabilidades, al Comité de Seguridad de Información que sesiona de forma extraordinaria ante la ocurrencia de un incidente.
g) **Comité de Seguridad de Información:** Será responsabilidad del Comité, el conformar la mesa extraordinaria de toma de decisión, la cual debe incluir a todos sus integrantes, así como al Propietario y/o Custodio de los Activos comprometidos y la Jefatura de la Unidad de TIC. La sesión de gestión de incidentes debe estar activa hasta que el incidente sea superado y la organización logre recuperarse del mismo. La función principal del Comité de Seguridad de Información recaerá en la toma de decisiones conjunta entre todos sus participantes, la cual deberá ser enfocada en la contención y recuperación lo más eficiente posible de la organización frente a un incidente.

6. Definiciones para la Gestión de Incidentes de Seguridad de Información.

A continuación, se realizan definiciones asociadas a mejorar el entendimiento del procedimiento de gestión de incidentes de la Agencia de Calidad de la Educación.

6.1 Detección y Notificación de Eventos o Incidentes de Seguridad.

Todos los funcionarios y funcionarias, personal a honorarios y terceras partes que por motivo de su ámbito de responsabilidades tenga contacto directo o indirecto con la Agencia de Calidad de la Educación, deben informar, de forma inmediata, debilidades, eventos y/o incidentes que pueda tener un impacto en la seguridad de los activos de información de la organización.

Éstos se informarán a través de los canales establecidos por el Comité a la Unidad, Departamento y/o División directamente responsable del ámbito del incidente. Lo anterior, debe ir en concordancia con lo establecido por el área o instancia responsable de las comunicaciones según el tipo de incidente que se esté afrontando. Lo anterior considera al menos los siguientes medios:

a. Correo electrónico.
b. Comunicación telefónica y/o mensajería electrónica debidamente resguardada.
c. Página web de intranet institucional, en el caso que corresponda.

Se debe contemplar más de un canal pues es posible que el incidente afecte a uno de dichos medios de comunicación.

Para realizar la notificación de un evento o incidente, los usuarios deben incluir, en función de la criticidad y/o ámbito de impacto del mismo a la Encargada de Seguridad de Información y/o a la Encargada de Ciberseguridad, para lo cual se utilizará la siguiente dirección electrónica: seguridadinformación@agenciaeducacion.cl

En caso de que el evento o anomalía sea declarado incidente de alta criticidad, la Encargada de Seguridad de Información o la encargada de Ciberseguridad, deberán notificar al Equipo de Respuesta Ante Incidentes de Ciberseguridad Gubernamental (CSIRT Gubernamental) utilizando los siguientes medios:

1. Notificación al CSIRT Gubernamental: soc@interior.gob.cl
2. Notificación telefónica al CSIRT Gubernamental: +56 2 2486 3850.
3. Registrar en el sistema del CSIRT Gubernamental el incidente: https://www.csirt.gob.cl/

Cabe destacar, que toda notificación de evento o incidente debe ser notificada con la mayor cantidad de información al respecto posible, ya que ésta facilitará y agilizará la gestión de contención y recuperación de la organización. Asimismo, todo evento o incidente debe ser notificado de forma interna, y solo aquellos de mayor relevancia o impacto se notifican al CSIRT de Gobierno.

6.2 Evaluación y Decisión sobre Eventos de Seguridad.

Una vez que la Encargada de Seguridad de Información y/o la Encargada de Ciberseguridad de la Agencia reciben la notificación de un evento por parte de un(a) usuario(a) del servicio, éste se debe clasificar según su taxonomía, utilizando como guía las definiciones establecidas en la siguiente tabla basada en los lineamientos del CSIRT de Gobierno para clasificación de incidentes:

Tabla de Clasificación de Incidentes según Taxonomía		
N°	**Clase de Incidente**	**Tipo de Incidente**
1	Contenido Abusivo	Pornografía Infantil - Sexual - Violencia
		Spam
2	Código Malicioso	Malware y Virus
3	Recopilación de Información	Scanning
		Sniffing
		Ingeniería Social
4	Intentos de Intrusión	Intentos de acceso
		Explotación de vulnerabilidades conocidas
		Nueva Firma de Ataque
5	Intrusión	Compromiso de Cuenta Privilegiada
		Compromiso de Cuenta sin privilegios
		Compromiso de Aplicación
6	Disponibilidad	Ataque de denegación de servicio (DoS / DDoS)
		Sabotaje
		Intercepción de información
7	Información de seguridad de contenidos	Acceso no autorizado a la información
		Modificación no autorizada de la información
8	Fraude	Phishing
		Derechos de Autor
		Uso no autorizado de recursos
		Falsificación de registros
		Generación y/o utilización de certificados maliciosos
9	Vulnerable	Sistemas y/o softwares desactualizados
10	Reportes de Seguridad	Uso no autorizado de administración de sistemas
		Explotación de fallas de software
		Ataque fuerza bruta
		Hombre del medio /Secuestro de sesión
		Inyección de red
		Errores de configuración
11	Solicitud	Solicitud de Información
12	Otros	Fuga de información
		Manipulación de Información
		Cross-site scripting (XSS)

Adicional a lo anterior, se debe identificar el nivel de impacto que puede tener un evento o incidente, lo cual, se determina en función de la criticidad de activos de información y/o la criticidad de el o los procesos comprometidos. Para lo anterior, los niveles de impacto a utilizar son los siguientes:

NIVELES DE IMPACTO	DESCRIPCIÓN
CATASTRÓFICO	Es posible que la amenaza se concrete de forma periódica para la organización
MUY ALTO	Es posible que la amenaza se concrete al menos una vez a la semana
ALTO	Es posible que la amenaza se concreta una vez al mes
BAJO	Es posible que la amenaza se concreta una vez al semestre
INSIGNIFICANTE	Es posible que la amenazas se concreta una vez al año o menos

De esta forma, la notificación de incidentes al CSIRT de Gobierno se define para aquellos incidentes que sean clasificados con niveles CATASTRÓFICO, y MUY ALTO. De esta forma, todos los incidentes de seguridad, incluyendo los falsos positivos, que hayan sido notificados al CSIRT, deberán ser revisados mediante análisis post-incidente, para identificar el origen de este, sus posibles implicancias, impacto en la organización, estudio de tendencias de incidentes analizados, así como también con el propósito de realizar una mejora continua sobre las acciones de control realizadas por esta unidad.

6.3 Comunicación durante incidentes.

Una vez declarado un incidente, la Agencia de Calidad de la Educación debe establecer planes de comunicación transversales, que permitan una coordinación de los esfuerzos para su mitigación, contención y recuperación. De esta forma, el plan comunicacional debe estar liderado por aquella Unidad o Departamento, en conjunto con su Jefatura de División, que sea directamente asociada a la solución del incidente, y, en caso de que el incidente sea de carácter muy alto o catastrófico, será el Comité de Seguridad de Información quien lidere la solución del mismo, incluyendo las comunicaciones, las cuales deberán ser ejecutadas en este caso, por el Departamento de Comunicaciones Internas de la Agencia.

Es importante considerar que todo incidente que tenga alto impacto en la organización deberá ser comunicado por el Departamento de Comunicaciones Internas, previa directriz por parte del Comité de Seguridad de Información, a todos los funcionarios de la Agencia, esto como parte de las medidas de mitigación y de educación de los usuarios.

6.4 Cierre de Incidentes de Seguridad.

Se considerará como cerrado un incidente, cuando la solución inmediata implementada entregue la seguridad a la Encargada de Seguridad de Información de que éste se encuentra bajo control, es decir, que fue contenido y la organización puede recuperar su operación normal.

Como cierre formal del mismo, se debe actualizar la Planilla de Incidentes de Seguridad y notificar a la organización, así como al usuario notificante, que se da por cerrado el incidente. La base de datos de incidentes que se genere al interior de la Agencia y sus unidades dependientes será revisada con intervalos no mayores a un año para verificar que los mismos no se repitan o si se han modificado las circunstancias, desarrollar una nueva medida de control que minimice la posibilidad e impacto del incidente en caso de que se diera la posibilidad de volver a presentarse.

6.5 Informe de Incidentes de Seguridad.

Como parte de la buena práctica asociada a la gestión de incidentes, se debe elaborar un informe de aquellos eventos o incidentes que sean relevantes para la organización, es decir, aquellos que tengan un nivel de impacto Alto, Muy Alto o Catastrófico. Las situaciones que se han de considerar en el informe de eventos de seguridad incluyen, al menos, las siguientes:

a) Identificación de control de seguridad ineficaz.
b) Detección de incumplimiento de la integridad, la confidencialidad, la privacidad o las expectativas de disponibilidad de la información.
c) Errores humanos.
d) Incumplimientos con las políticas o pautas.
e) Incumplimientos en las disposiciones de seguridad física.
f) Cambios no controlados en el sistema.
g) Fallas en el software o hardware.
h) Violaciones de acceso.

Las fallas u otro comportamiento anómalo del sistema pueden ser un indicador de un ataque de seguridad o un incumplimiento real de seguridad y, por lo tanto, siempre se debería informar como un evento de seguridad de la información.

Dependiendo de la magnitud del incidente para la institución se realizará un análisis post-incidente, para identificar el origen del mismo.

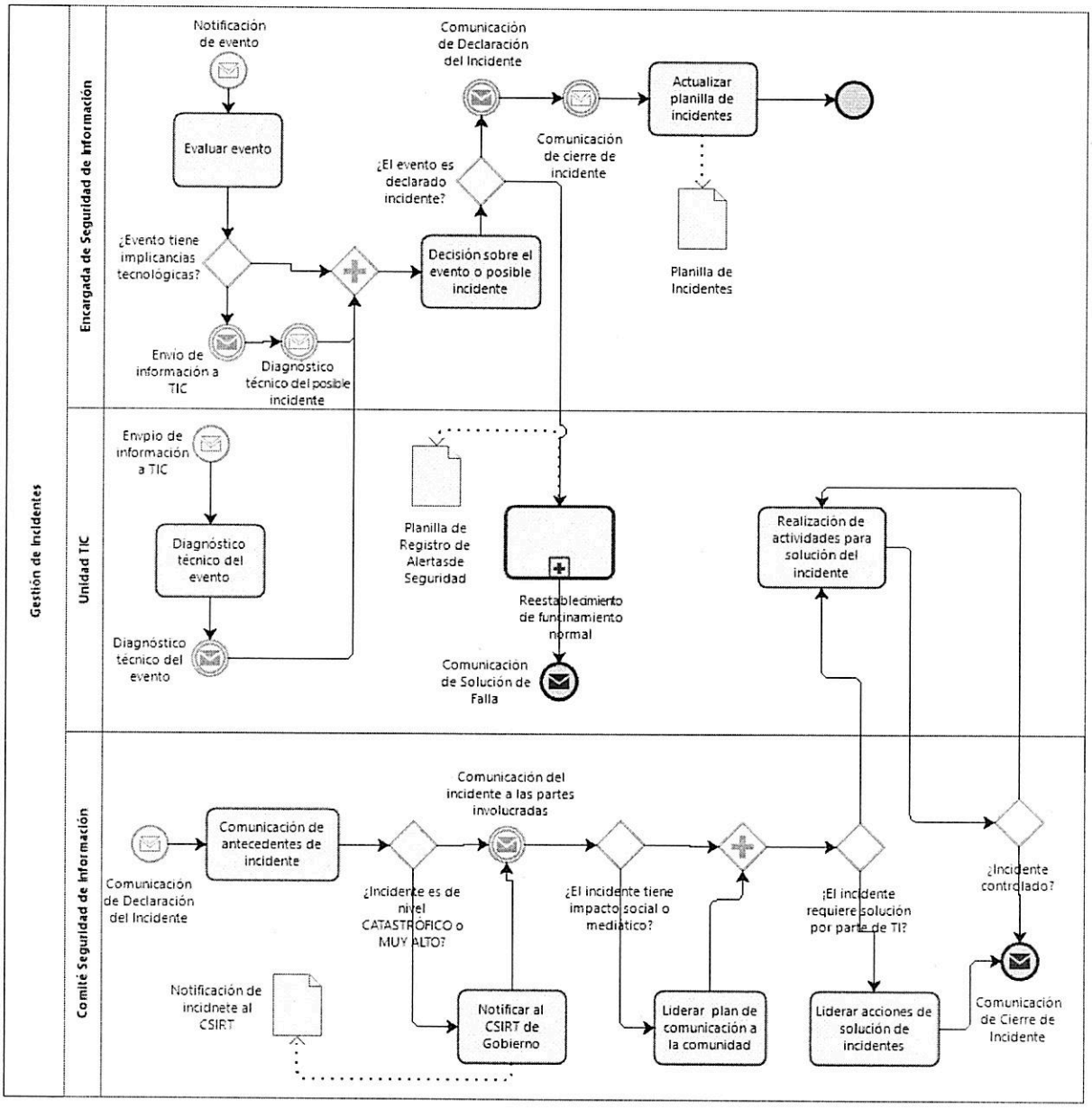
6.6 Aprendizaje de los Incidentes de Seguridad.

Se realizarán informes de evaluación de los incidentes ocurridos, de manera de poder concentrar el conocimiento obtenido de los diferentes análisis y la respectiva resolución y/o mitigación de los incidentes de seguridad de la información, para que este aprendizaje ayude a reducir la probabilidad o el impacto de incidentes futuros.

7. Modo de Operación.

A continuación, se define el procedimiento de gestión de incidentes.

7.1 Flujo de Procedimiento para Gestión de Incidentes.



7.2 Matriz del Procedimiento Gestión de Incidentes.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Notificación de evento	Se recibe la notificación de un posible evento o incidente por parte de un usuario. Esta notificación debiese incluir las consideraciones establecidas en el punto 6.5 de este documento. En caso de no poseer una especificación que permita hacer una correcta evaluación del evento, se debe contactar al usuario notificante.	Encargada de Seguridad de la Información	2
2	Evaluar evento	Con la finalidad de poder decidir qué curso de acción tomar para abordar el evento o incidente, se debe determinar la taxonomía del mismo y el nivel de impacto que tiene para la organización. Se pueden dar las siguientes alternativas: - El evento/incidente tiene implicancias tecnológicas (2A). - El evento/incidente no tiene implicancias tecnológicas (3).	Encargada de Seguridad de la Información	2A o 3
2A	Envío de información a TIC	Se deben enviar los antecedentes del evento/incidente a la Unidad de TIC para que se realice un diagnóstico técnico del mismo.	Encargada de Seguridad de la Información	2B
2B	Diagnóstico técnico del evento/incidente	Se deben realizar las actividades necesarias para determinar el nivel de impacto e implicancias del evento/incidente.	Unidad de TIC	2C
2C	Enviar diagnóstico técnico	Se debe enviar el diagnóstico técnico del evento/incidente a la Encargada de Seguridad de Información.	Unidad de TIC	3
3	Decisión sobre el evento o posible incidente	Con toda la información necesaria, se debe decidir el curso a seguir para la resolución o mitigación del evento/incidente. Se pueden dar las siguientes alternativas: - El evento no es declarado incidente (3A). - El evento es declarado incidente (4).	Encargada de Seguridad de la Información	3A o 4

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
3A	Restablecimiento de funcionamiento normal	Se deben realizar las actividades necesarias para restablecer la operación normal de la organización.	Unidad de TIC	3B
3B	Comunicación de Solución de Falla	Una vez solucionado el evento, se debe notificar a la Encargada de Seguridad de Información. Como finalización del procedimiento, se debe actualizar la Planilla de Registro de Alertas de Seguridad.	Unidad de TIC	FIN
4	Comunicación de Declaración del Incidente	Se debe comunicar formalmente que, dado el impacto potencial del incidente, éste debe ser gestionado como incidente de Seguridad. Para liderar la gestión de éste, se deben seguir los lineamientos entregados en el punto 6.3 de este procedimiento.	Encargada de Seguridad de la Información	5
5	Comunicación de antecedentes de incidente	Una vez conformado el Comité de Seguridad de Información, se deben comunicar todos los antecedentes del incidente a los miembros de éste con la finalidad de homologar la información existente y realizar gestión eficiente. En base a lo anterior, se pueden dar las siguientes alternativas: - El incidente es de tiene un nivel de impacto MUY ALTO o CATASTRÓFICO (5A). - El incidente es de criticidad inferior a MUY ALTO (6).	Comité de Seguridad de Información	5A o 6
5A	Notificar al CSIRT de Gobierno	Se debe notificar al CSIRT de Gobierno, según lo estipulado en el punto 6.1 de este documento.	Comité de Seguridad de Información	6
6	Comunicación del incidente a las partes involucradas	Se debe comunicar del incidente a todas las partes involucradas en éste, lo que puede incluir a toda la organización según la criticidad del mismo. Se pueden dar las siguientes opciones: - El incidente tiene impacto mediático o social (6A). - El incidente no tiene impacto mediático o social (7).	Comité de Seguridad de Información	6A o 7

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
6A	Liderar plan de comunicación a la comunidad	Se debe liderar un plan comunicacional para mantener informada a la comunidad sobre el incidente. Se pueden dar las siguientes opciones: - EL incidente requiere soluciones TIC (7). - El incidente no es de tipo tecnológico (8).	Comité de Seguridad de Información	7 u 8
7	Realización de actividades para solución del incidente tecnológico	Se deben llevar a cabo las actividades necesarias para recuperar la operación normal de la organización.	Unidad de TIC	9
8	Liderar acciones de solución de incidentes	Se deben liderar las acciones para mitigar o controlar el incidente. Se debe considerar el procedimiento de Contacto con la Autoridades.	Comité de Seguridad de Información	9
9	Se debe validar la solución del incidente para proceder a su cierre formal	El Comité de Seguridad de Información debe determinar que el incidente ha sido solucionado y/o controlado para volver a la normalidad operativa de la organización. Se pueden dar las siguientes alternativas: - La solución no cumple con los requisitos para proceder a su cierre (7 u 8 según tipo de incidente). - La solución cumple con los requisitos para proceder a su cierre (9).	Comité de Seguridad de Información	7/8 o 10
10	Comunicación de cierre de incidente	Se debe comunicar a todas las partes pertinentes, el cierre formal del incidente.	Comité de Seguridad de Información	11
11	Actualizar planilla de incidentes	Se debe actualizar la planilla de registro de incidente para gestionar las futuras actividades de aprendizaje o soluciones permanentes.	Encargada de Seguridad de Información	FIN

7.3 Matriz de Responsabilidades.

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

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

De esta forma las matrices de responsabilidades asociadas a los procesos establecidos por el presente documento son las siguientes:

a) Matriz de responsabilidades para el Procedimiento de Gestión de Incidentes

ID	ACTIVIDAD	COMITÉ SI	UNIDAD TIC	ENC. SI	DUEÑO ACTIVO	USUARIO
1	Notificación de evento	-	-	I	R/E	R/E
2	Evaluar evento	-	I	R/E	C	C
2A	Envío de información a TIC	-	I	R/E	C	C
2B	Diagnóstico técnico del evento/incidente	-	R/E	C	C	C
2C	Enviar diagnóstico técnico	-	R/E	I	I	I
3	Decisión sobre el evento o posible incidente	I	I	R/E	I	I
3A	Restablecimiento de funcionamiento normal	-	R/E	I	-	-
3B	Comunicación de Solución de Falla	-	R/E	I	I	I
4	Comunicación de Declaración del Incidente	I	I	R/E	I	I
5	Comunicación de antecedentes de incidente	R	C	E	C	-
5A	Notificar al CSIRT de Gobierno	R	I	E	I	-
6	Comunicación del incidente a las partes involucradas	R/E	I	I	I	I
6A	Liderar plan de comunicación a la comunidad	R/E	C	C	C	-
7	Realización de actividades para solución del incidente tecnológico	R	E	C	I	-
8	Liderar acciones de solución de incidentes	R/E	C	C	C	-
9	Se debe validar la solución del incidente para proceder a su cierre formal	R/E	C	C	C	-
10	Comunicación de cierre de incidente	R/E	I	I	I	I
11	Actualizar planilla de incidentes	I	I	R/E	I	-

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Planilla de Registro de Incidentes (A.16.1.2; A.16.1.4; A.16.1.5; A.16.1.6)	-	Encargado(a) de Seguridad de la Información	4 años / Archivo UTIC	Digital	PC Responsable del Registro
Sistema de gestión de ticket (A.16.1.2; A.16.1.4; A.16.1.5; A.16.1.6)	-	Unidad de TIC	4 años / Archivo UTIC	Digital	Plataforma de gestión de ticket

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Registros de Operación de Event Viewer (A.12.4.1; A.12.4.3)	-	Unidad de TIC	4 años / Archivo UTIC	Digital	Event Viewer

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Procedimiento de Elaboración de Plan Anual de Capacitación, Formación y Entrenamiento (Control A.07.02.02)
2. Política de Gestión de Activos (Control A.8.1.2, A.8.1.3, A.8.3.1 Y A.8.3.3)
3. Procedimiento de Alta y Baja de Cuentas de Usuario a la Red y Servicios de Red (Control A.9.1.2, A.9.2.1, A.9.2.2 Y A.9.2.3)
4. Procedimiento de Gestión de Contraseñas (A.9.4.3, A.9.2.4 y A.9.3.1)
5. Política de Gestión de Controles Criptográficos y Contraseñas (Control A.10.1.1 y A.10.1.2)
6. Procedimiento de Gestión para el Desarrollo y Mantención de Software Seguro (A.14.1.1, A.14.1.2, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9 y A.12.1.4)
7. Procedimiento de Sincronización de Relojes (Control A.12.04.04)
8. Política de desarrollo seguro (control A.14.2.1)
9. Política de gestión de Incidentes control A.16.01.01
10. Procedimiento de Gestión de Incidentes (Control A.12.4.1, A.12.4.3, A.16.1.02, A.16.1.4, A.16.1.5 Y A.16.1.6)

Fecha: 2 de octubre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodríguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD (S)	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	María de la Luz González.	Jefa de DIEST (S)	
6	Ramón Gutiérrez P.	Jefe DAG (S)	
7	Sergio Hidalgo	Jefe Departamento de Auditoría	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Patrick Soto A.	Jefe TIC	
10	Andrea Soto Araya	Encargada de SSI	
11	Nicol Jeria O.	Encargada de Ciberseguridad	
12			

Procedimiento de Sincronización de Relojes
Control A.12.04.04

Tabla de Contenidos

Revisiones del procedimiento.....2
1. Objetivo.....3
2. Alcance.....3
3. Normas y Referencias.....3
4. Términos y Definiciones.....3
5. Roles y Responsabilidades.....4
6. Definiciones para la Sincronización de Relojes.....5
7. Modo de Operación.....5
7.1 Flujo de Procedimiento de Sincronización de Relojes para Estaciones de Trabajo5
7.2 Flujo de Procedimiento de Sincronización de Relojes para Servidores.....5
7.3 Matriz del Procedimiento de Sincronización de Relojes para Estaciones de Trabajo 6
7.4 Matriz del Procedimiento de Sincronización de Relojes para Servidores.....7
7.5 Matriz de Responsabilidades. 7
8. Registro de Operación. 8
9. Anexo.....8

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de Información y Ciberseguridad	Patrick Soto Jefe Unidad TIC	Andrea Soto Encargada de Seguridad de la Información	Comité de SGSIC

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	31/07/2019	Elaboración inicial	Todas

1. Objetivo.

En concordancia con lo establecido en la Política de Gestión de Incidentes de Seguridad de la Información y Ciberseguridad, la Agencia de Calidad de la Educación, en adelante la Agencia, debe garantizar la trazabilidad inequívoca de los eventos y registro de operación de la totalidad de sus sistemas de procesamiento de información. Para lo anterior, el presente documento tiene por objetivo el establecer la secuencia de actividades para la sincronización de los relojes tanto de los servidores como de las estaciones de trabajo de la institución.

2. Alcance.

Este procedimiento debe aplicarse para todas y cada una de las estaciones de trabajo que sean o hayan sido asignadas a funcionarios(as) de planta y contrata, y personal a honorarios de la Agencia de Calidad de la Educación y toda aquella persona natural o jurídica que preste servicios (terceros y proveedores) para ella y que, a raíz de ello, requieran acceder o procesar activos de información de la Agencia de Calidad de la Educación mediante el uso de estaciones de trabajo. Asimismo, lo establecido en este documento, debe aplicarse para todos los servidores y sistemas de procesamiento de la Agencia de Calidad de la Educación, indiferente del segmento de red al que pertenezcan.

Asimismo, este procedimiento debe ser ejecutado ante todo cambio de hora que se ajuste a la realidad del país donde la Agencia de Calidad de la Educación tenga operación.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27002:2013, el presente documento tiene su alcance sobre los siguientes controles:

- A.12.04.04 – Sincronización con relojes.

3. Normas y Referencias.

a) NCh ISO 27,001:2013.

b) NCh ISO 27,002:2013.

c) Política de Gestión de Incidentes de Seguridad de la Información y Ciberseguridad, aprobada por Resolución Exenta N° 1338, de 2019, de la Agencia de Calidad de la Educación.

4. Términos y Definiciones.

Amenaza	Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.
Riesgo	Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.
Autoridad	Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.

Evento de Seguridad de la Información	Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.
Incidente de Seguridad	Se refiere a la Identificación y materialización de una amenaza o riesgo detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.
Vulnerabilidad	Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.
Evento de Seguridad	Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia
Plan de Contingencia	Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.
Activos de Información	Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
Contactos críticos	Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o incidentes.
Red de Seguridad	Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.
Seguridad de la Información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.

5. Roles y Responsabilidades.

a) **Encargada de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC) de la Agencia, será el rol encargado de ejercer la supervisión de la correcta aplicación de este procedimiento. Por otra parte, será este rol el encargado de entregar asesorías que permitan, desde el punto de vista de la seguridad de información y ciberseguridad, impulsar mejoras al presente documento según necesidades o cambios específicos del entorno en el cual se desenvuelve la Agencia, o los requerimientos particulares que ésta experimente en el tiempo.

b) **Jefatura Unidad de Tecnologías de la Información y Comunicación, de la División de Administración General:** Como dueño funcional de este procedimiento, será este rol el encargado de velar por la correcta aplicación de lo establecido en el presente documento, ejerciendo las labores necesarias para esto. Asimismo, será este rol el encargado de proponer e impulsar mejoras y actualizaciones al procedimiento, en función tanto de los cambios que el entorno en el que se desenvuelve la Agencia pueda experimentar, así como de los requerimientos particulares que ésta experimente en el tiempo.

c) **Encargado de Plataforma, de la Unidad de Tecnologías de la Información y Comunicación:** Será este rol el principal encargado de la correcta ejecución de lo establecido en este procedimiento, asegurando así la efectividad que éste busca en relación a la seguridad de información y ciberseguridad. Será su responsabilidad el proponer mejoras que eleven el

nivel de madurez de la organización en estas temáticas mediante la aplicación de este procedimiento.

6. Definiciones para la Sincronización de Relojes.

Según lo establecido a nivel nacional, será el Servicio Hidrográfico y Oceanográfico de la Armada (SHOA), el referente oficial para efectuar los cambios de hora de los sistemas de procesamiento de información de la Agencia. De esta forma, los recursos del SHOA a utilizar para este procedimiento son los siguientes:

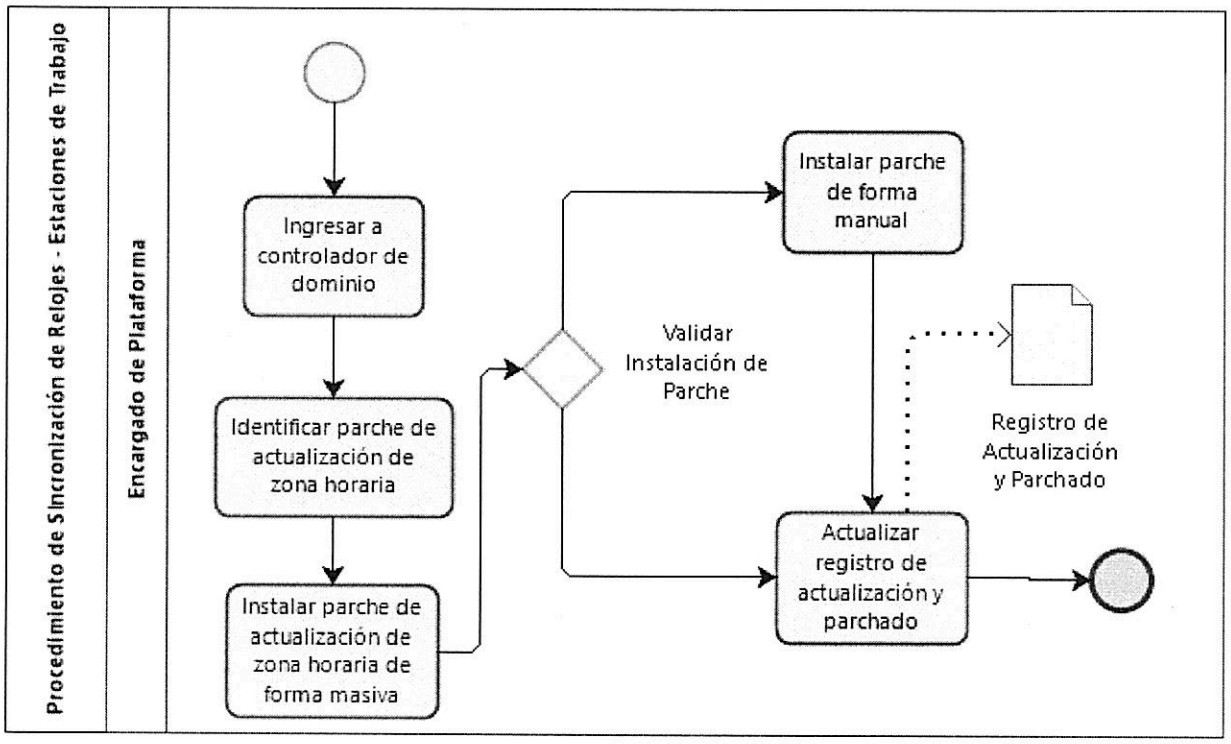
- Hora Oficial: Proporciona la hora oficial para Chile Continental, Isla de Pascua, y Región de Magallanes, así como la referencia de hora universal UCT (http://www.horaoficial.cl/).

7. Modo de Operación.

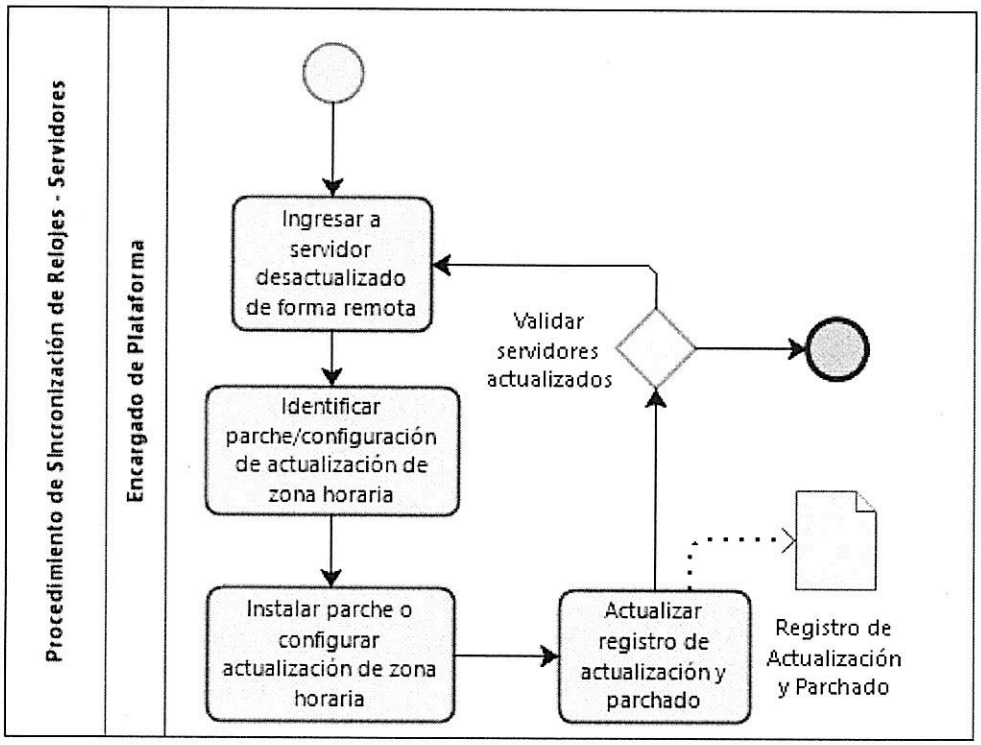
A continuación, se describen los flujos procedimentales para:

- Procedimiento de Sincronización de Relojes para Estaciones de Trabajo.
- Procedimiento de Sincronización de Relojes para Servidores.

7.1 Flujo de Procedimiento de Sincronización de Relojes para Estaciones de Trabajo.



7.2 Flujo de Procedimiento de Sincronización de Relojes para Servidores.



7.3 Matriz del Procedimiento de Sincronización de Relojes para Estaciones de Trabajo.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Ingresar a controlador de dominio	Se debe ingresar en el controlador de dominio de la Agencia, a fin de comenzar con el procedimiento de sincronización de relojes en las estaciones de trabajo.	Analista de Plataforma	2
2	Identificar parche de actualización de zona horaria	Según los requerimientos del momento, se debe identificar la actualización disponibilidad por el proveedor Microsoft para cambio de hora.	Analista de Plataforma	3
3	Instalar parche de actualización de zona horaria de forma masiva	Se debe aplicar el parche antes mencionado como una tarea masiva del controlador de dominio.	Analista de Plataforma	4
4	Validar Instalación de Parche	Se debe validar que la tarea masiva de actualización de relojes en las estaciones de trabaja haya finalizado con éxito. Se pueden dar las siguientes situaciones: - La actualización NO finalizó con éxito (4A). - La actualización finalizó con éxito (5).	Analista de Plataforma	4A o 5

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
4A	Instalar parche de forma manual	Se debe realizar las actividades necesarias para sincronizar los relojes en estas estaciones de trabajo.	Analista de Plataforma	5
5	Actualizar registro de actualización y parchado	Se debe actualizar el registro de actualización y parchado.	Analista de Plataforma	FIN

7.4 Matriz del Procedimiento de Sincronización de Relojes para Servidores.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Ingresar a servidor desactualizado de forma remota	Se debe hacer ingreso de forma remota al servidor al cual se le realizar la sincronización de relojes.	Analista de Plataforma	2
2	Identificar parche/configuración de actualización de zona horaria	Dependiendo del servidor que se esté actualizando, se puede requerir una instalación de parche o una configuración de zona horaria para llevar a cabo la sincronización de relojes.	Analista de Plataforma	3
3	Instalar parche o configurar actualización de zona horaria	Se debe llevar a cabo la configuración o instalación de parche para la sincronización de relojes.	Analista de Plataforma	4
4	Actualizar registro de actualización y parchado	Se debe actualizar el registro de actualización y parchado.	Analista de Plataforma	5
5	Validar servidores actualizados	Se debe validar que no queden servidores fuera de la sincronización de relojes. Se pueden dar las siguientes opciones: - No se han sincronizado los relojes de la totalidad de servidores (1). - La totalidad de los servidores han sido sincronizados (FIN).	Analista de Plataforma	1 o FIN

7.5 Matriz de Responsabilidades.

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

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

De esta forma las matrices de responsabilidades asociadas a los procesos establecidos por el presente documento son las siguientes:

a) Matriz de responsabilidades para el Procedimiento de Sincronización de Relojes para Estaciones de Trabajo.

ID	ACTIVIDAD	ANALISTA DE PLATAFORMA	JEFE TIC	ENC. SI
1	**Ingresar a controlador de dominio**	E	R	-
2	**Identificar parche de actualización de zona horaria**	E	R	-
3	**Instalar parche de actualización de zona horaria de forma masiva**	E	R	-
4	**Validar Instalación de Parche**	E	R	-
4A	**Instalar parche de forma manual**	E	R	-
5	**Actualizar registro de actualización y parchado**	E	R	I

b) Matriz de responsabilidades para el Procedimiento de Sincronización de Relojes para Servidores.

ID	ACTIVIDAD	ANALISTA DE PLATAFORMA	JEFE TIC	ENC. SI
1	Ingresar a servidor desactualizado de forma remota	E	R	-
2	Identificar parche/configuración de actualización de zona horaria	E	R	-
3	Instalar parche o configurar actualización de zona horaria	E	R	-
4	Actualizar registro de actualización y parchado	E	R	I
5	Validar servidores actualizados	E	R	-

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Registro de actualización y parchado actualizado	-	Encargado de Plataforma	Hasta el siguiente cambio de hora	SCCM Configuration Manager	Servidor Digital

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:

1. Procedimiento de Elaboración de Plan Anual de Capacitación, Formación y Entrenamiento (Control A.07.02.02)
2. Política de Gestión de Activos (Control A.8.1.2, A.8.1.3, A.8.3.1 Y A.8.3.3)
3. Procedimiento de Alta y Baja de Cuentas de Usuario a la Red y Servicios de Red (Control A.9.1.2, A.9.2.1, A.9.2.2 Y A.9.2.3)
4. Procedimiento de Gestión de Contraseñas (A.9.4.3, A.9.2.4 y A.9.3.1)
5. Política de Gestión de Controles Criptográficos y Contraseñas (Control A.10.1.1 y A.10.1.2)
6. Procedimiento de Gestión para el Desarrollo y Mantención de Software Seguro (A.14.1.1, A.14.1.2, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9 y A.12.1.4)
7. Procedimiento de Sincronización de Relojes (Control A.12.04.04)
8. Política de desarrollo seguro (control A.14.2.1)
9. Política de gestión de Incidentes control A.16.01.01
10. Procedimiento de Gestión de Incidentes (Control A.12.4.1, A.12.4.3, A.16.1.02, A.16.1.4, A.16.1.5 Y A.16.1.6)

Fecha: 2 de octubre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodríguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD (S)	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	María de la Luz González.	Jefa de DIEST (S)	
6	Ramón Gutiérrez P.	Jefe DAG (S)	
7	Sergio Hidalgo	Jefe Departamento de Auditoría	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Patrick Soto A.	Jefe TIC	
10	Andrea Soto Araya	Encargada de SSI	
11	Nicol Jeria O.	Encargada de Ciberseguridad	
12			

1

Agencia de Calidad de la Educación Gobierno de Chile	**Procedimiento de Gestión de Vulnerabilidades Técnicas**			
	Nivel de Confidencialidad	-	Páginas	**1 de 8**
			Versión	**0**
	Fecha versión del documento	**31-10-19**	Código	**SGSIC-PRO-A.12.06.01**
	Procedimiento de Gestión de Vulnerabilidades Técnicas			

Procedimiento de Gestión de Vulnerabilidades Técnicas
Control A.12.06.01

Tabla de Contenidos

Revisiones del Procedimiento....2
1. Objetivo. 3
2. Alcance. 3
3. Normas y Referencias. 3
4. Términos y Definiciones. 3
5. Roles y Responsabilidades 3
6. Gestión de Vulnerabilidades Técnicas 4
6.1. Detección de Vulnerabilidades y Actualizaciones 4
6.2. Estudio de Parches....4
6.3. Implementación de Parches 5
7. Modo de Operación 5
7.1 Flujo de Procedimiento para la Gestión de Vulnerabilidades Técnicas 5
7.2 Matriz del Procedimiento para la Gestión de Vulnerabilidades Técnicas....6
7.3 Matriz de Responsabilidades. 7
8. Registro de Operación....8
9. Anexo....7

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC)	Patrick Soto Jefe Unidad TIC	Andrea Soto Araya Encargada Seguridad de la Información	Comité SGSIC

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	31/10/2019	Elaboración Inicial	Todas

1. Objetivo.

El presente procedimiento tiene por objetivo principal entregar los principales lineamientos, directrices y tareas que deberán ser llevadas a cabo con el objetivo de brindar niveles de protección adecuados a los sistemas tecnológicos administrados por la Agencia de Calidad de la Educación. En función de lo anterior, es importante detallar que, aunque este documento no incluye las prácticas técnicas que deberán ser llevadas a cabo para gestionar las vulnerabilidades de los sistemas, sí contiene las buenas prácticas que deberán ser consideradas para implementar dichas soluciones técnicas.

2. Alcance.

El presente procedimiento debe ser aplicado por todos los funcionarios y funcionarias, de planta, contrata, honorarios internos y/o cualquiera sea la naturaleza de su vinculación jurídicas y proveedores, que, dado el cumplimiento de sus responsabilidades, se vean involucrados en la gestión de vulnerabilidades técnicas sobre los sistemas tecnológicos de la Agencia de Calidad de la Educación.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27002:2013, el presente documento tiene su alcance sobre el siguiente control:

- A.12.06.01 – Administración de Vulnerabilidades Técnicas

3. Normas y Referencias.

- NCh ISO 27.001:2013.
- NCh ISO 27.002:2013.
- Política de Desarrollo Seguro de Software, aprobada por Resolución Exenta N° 1547, de 2019, de la Agencia de Calidad de la Educación.

4. Términos y Definiciones.

Vulnerabilidades Técnicas	Una vulnerabilidad técnica se refiere a cierto tipo de debilidad en un sistema tecnológico, la cual pudiera ser aprovechada por un individuo externo a la Agencia con intenciones maliciosas.
Parches	Hace referencias a actualizaciones de los sistemas tecnológicos, las cuales están dirigidas a solucionar vulnerabilidades técnicas asociadas a los mismos.
Parchado	Se refiere al proceso de aplicar los parches sobre los sistemas tecnológicos de la organización, con el objetivo de brindar niveles de protección adecuados para estos.
Sistemas	Hace referencia al conjunto de tecnologías de información y comunicación (TIC) que mediante la disponibilización de un servicio apalancan uno o varios procesos de la institución.

5. Roles y Responsabilidades.

a) **Jefatura Unidad Tecnologías de Información y Comunicación:** Deberá promover mejoras tecnológicas asociadas a la optimización de este procedimiento. Así mismo, deberá supervisar las acciones llevadas a cabo por los miembros de la Unidad a su cargo, con el objetivo de dar cumplimiento a los lineamientos, directrices y prácticas detalladas en el presente documento.

b) **Encargado de Plataforma de la Unidad de Tecnologías de la Información y Comunicación:** Encargado de realizar el parchado sobre los diferentes sistemas de la organización en conformidad con las directrices, tareas y buenas prácticas expresadas en el presente procedimiento, brindando así los niveles de protección adecuados a los activos de información y sistemas utilizados al interior de la Agencia.

c) **Encargada/o de Seguridad de la Información:** Rol encargado de velar por la correcta aplicación y difusión de los lineamientos aquí establecidos. Así mismo, será este el encargado de apoyar los procesos de actualización de este documento, prestando un asesoramiento activo desde la perspectiva de la seguridad de la información.

d) **Personal de la Agencia de Calidad de la Educación**: Dentro de sus responsabilidades encontramos la notificación de cualquier incidente tecnológico o sospecha asociada a la existencia de vulnerabilidades técnicas sobre los sistemas de la Agencia, entendiendo por tal todos los funcionarios y funcionarias, de planta, contrata, honorarios internos y/o cualquiera sea la naturaleza de su vinculación jurídica.

6. Gestión de Vulnerabilidades Técnicas.

En función de la importancia de la información manejada al interior de la Agencia de Calidad de la Educación, es necesario implementar métodos de protección asociados a aumentar la robustez de los sistemas tecnológicos que contienen dicha información. Así, se deberá llevar a cabo un proceso de gestión de las vulnerabilidades técnicas asociadas a dichos sistemas, el cual se enfocará en el parchado de los sistemas críticos de la organización, brindando así una protección preventiva frente a posibles acciones maliciosas que se pudieran tomar contra la Agencia. En función de las características cíclicas asociadas a la implementación de parches sobre los sistemas, se entiende que el proceso, de igual manera, es cíclico, por lo que deberá ser realizado de forma continua.

6.1. Detección de Vulnerabilidades y Actualizaciones.

Con el objetivo de garantizar que los sistemas tecnológicos de la Agencia de Calidad de la Educación funcionen correctamente, se deberá velar por la detección de vulnerabilidades, así como por el monitoreo de actualizaciones que pudiesen resolver dichos errores. A continuación, se detallan buenas prácticas a realizar en el proceso en cuestión:

a) Velar por la inclusión de alertas o recordatorios asociados a la liberación de nuevos parches para los sistemas críticos de la Agencia de Calidad de la Educación. En caso de que no sea posible la activación de alertas automáticas, esta tarea deberá ser llevada a cabo de forma manual, mediante revisiones periódicas por parte del encargado de plataforma.

b) En caso de existir errores en los sistemas o equipos de la Agencia de Calidad de la Educación, se deberá estudiar si la causa de estos se encuentra asociada fallas conocidas de cierto parche realizado sobre el sistema en cuestión, o si dichos errores pueden ser corregidos mediante la implementación de parches.

6.2. Estudio de Parches.

Con la finalidad de proteger a los sistemas tecnológicos de la Agencia de Calidad de la Eduacación en relación con posibles errores o vulnerabilidades asociadas a la implementación de parches, es necesario estudiar estos cuidadosamente. Así, es necesario seguir las siguientes buenas prácticas al llevar a cabo dichos estudios:

a) Con la finalidad de garantizar que el parche que se desea implementar en un sistema no tenga efectos negativos sobre el mismo, el Encargado de Plataforma deberá dedicar tiempo al estudio del parche en cuestión. Así, toda investigación llevada a cabo deberá ser realizada

basándose exclusivamente en estudios reales y fundamentados, o experiencias de usuarios confiables.

b) Una buena práctica asociada a la implementación y el estudio de parches sobre sistemas informáticos tiene que ver con esperar cierto tiempo antes de la implementación del mismo, luego de que este ha sido liberado, con la finalidad de evitar comprometer los sistemas de la organización en caso de que el parche en cuestión contenga algún error considerable. En función de lo anterior, se deberá esperar como mínimo una semana luego de la liberación del parche para la implementación del mismo.

c) Una vez que se hayan recopilado todos los antecedentes necesarios, se deberá lanzar el parche dentro de un sistema simulado y controlado como, por ejemplo, mediante la utilización de máquinas virtuales. El comportamiento de la máquina virtual luego de la implementación del parche deberá ser monitoreada, procurando identificar cualquier evento fuera de lo normal, en caso de ocurrir alguno.

Todas las prácticas anteriormente descritas deben ser realizadas con el principal objetivo de prevenir potenciales malfuncionamientos en los sistemas de la organización. Así, ningún parche podrá ser implementado sin realizar las tareas anteriormente descritas.

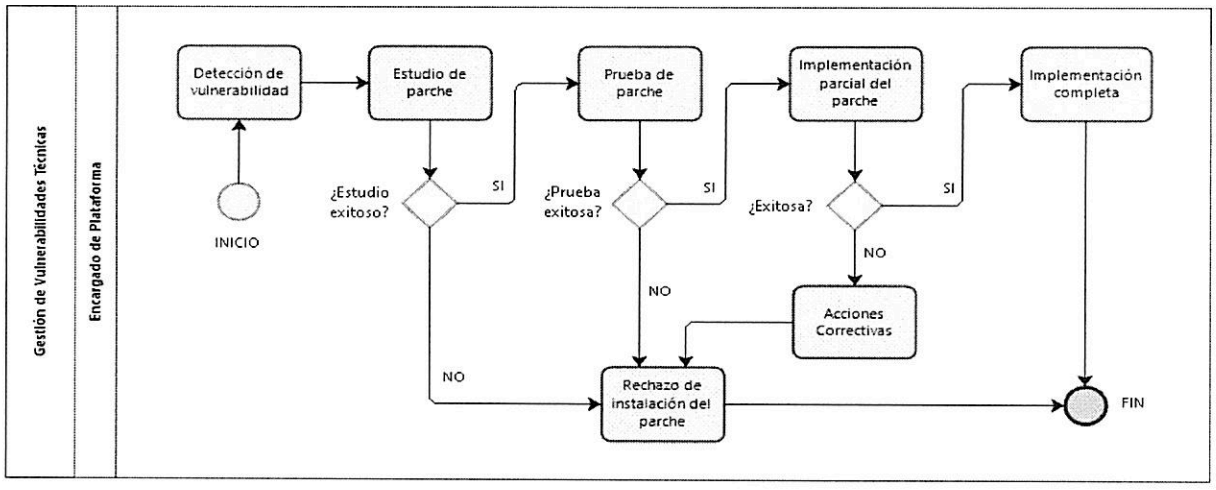
6.3. Implementación de Parches.

En función de la criticidad de los sistemas de la organización, cada parchado deberá ser debidamente estudiado y probado antes de ser implementado. En función de lo anterior, el responsable de la realización de esta tarea será el encargado de plataforma, quien deberá velar por la seguridad de los sistemas de la organización y de la información almacenada en estos bajo todo momento dado. Así, la implementación de los parches sobre los sistemas deberá ser realizada de forma progresiva, velando porque, en caso de existir fallas durante la implementación del mismo, estas solo afecten una parte de los equipos de la Agencia. Una vez que sea verificado que el proceso de parchado es seguro, se podrá realizar este sobre el resto de los equipos y sistemas de la organización.

7. Modo de Operación.

A continuación, se describen los flujos procedimentales para la gestión de vulnerabilidades técnicas.

7.1 Flujo de Procedimiento para la Gestión de Vulnerabilidades Técnicas.



Powered by bizagi Modeler

7.2 Matriz del Procedimiento para la Gestión de Vulnerabilidades Técnicas.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Detección de vulnerabilidad	En función de las directrices establecidas en el presente documento, una detección de vulnerabilidad puede responder a cualquiera de los siguientes escenarios: • Se detecta una vulnerabilidad que puede ser solucionada mediante la implementación de un parche. • Se ha liberado un parche que puede ser aplicado en los sistemas de la organización.	Encargado de Plataforma	2
2	Estudio de parche	En conformidad con las directrices establecidas en el presente procedimiento, se deberá estudiar la instalación del parche en cuestión. Así, los siguientes cursos de acción son posibles: - Se estima que el parche debe instalarse (3) - El parche no debe ser instalado (7)	Encargado de Plataforma	3 o 7
3	Prueba de parche	La instalación del parche deberá ser probada en un entorno virtual y controlado, como una máquina virtual. Durante la prueba se deberá intentar definir si la instalación del parche es exitosa, o si existe alguna complicación asociada a la implementación del mismo. Pueden darse los siguientes escenarios: - El parche pasó la prueba (4) - El parche no pasó la prueba (7)	Encargado de Plataforma	4 o 7

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
4	Implementación parcial del parche	En conformidad con lo establecido en el presente documento, en primera instancia se deberá implementar el parche de forma parcial. En función de lo anterior, pueden ocurrir los siguientes resultados: - Parche fue instalado exitosamente (5) - La instalación produjo errores (6)	Encargado de Plataforma	5 o 6
5	Implementación completa	Debido a que el parche en cuestión ha logrado superar todas las pruebas asociadas, este podrá pasar a instalarse en el resto de los equipos de la organización.	Encargado de Plataforma	FIN
6	Acciones correctivas	Debido a que la implementación parcial del parche falló, se deberán tomar acciones correctivas sobre los sistemas damnificados durante este proceso.	Encargado de Plataforma	7
7	Rechazo de instalación del parche	En función de que las pruebas realizadas sobre el parche en cuestión resultaron negativas, se estima que este no será instalado en los sistemas de la organización.	Encargado de Plataforma	FIN

7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

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

De esta forma, la matriz de responsabilidades para el Desarrollo Seguro Interno se estructura de la siguiente manera:

ID	ACTIVIDAD	Encargado Plataforma	Jefe Unidad TIC	Encargado Seguridad
1	**Detección de vulnerabilidad**	R / E / A	I	-
2	**Estudio de parche**	R / E / A	I	-
3	**Prueba de parche**	R / E / A	I	-
4	**Implementación parcial del**	R / E / A	I	-

	parche			
5	**Implementación completa**	R / E	I / C / A	I
6	**Acciones correctivas**	R / E	I / C / A	I
7	**Rechazo de instalación del parche**	R / E / A	I / C	I

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Windows Update History	-	Encargado de Plataforma	1 año / Windows Update	Digital	Windows Update

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Política de Revisión Independiente del Sistema de Gestión de Seguridad de Información y Ciberseguridad (Control A.5.1.2, A.18.2.1, A.18.2.2 y A.18.2.3)
2. Procedimiento de Segregación de Funciones (Control A. 6.1.2)
3. Política para Transferencia y Manejo de Información (A. 8.2.2, A.8.2.3, A.8.3.2, A.13.2.1 y A.13.2.3)
4. Procedimiento de Controles y Perímetro de Seguridad Física (Control A.11.1.2 y A.11.1.4)
5. Procedimiento para Documentación de los Procedimientos Operacionales (control A.12.1.1 y A.18.1.3)
6. Política de Protección Contra Código Malicioso (Control A.12.02.01, A.12.5.1 y A.12.6.2)
7. Procedimiento de Gestión de Vulnerabilidades Técnicas (A.12.6.1)
8. Política de Controles de Red (control .13.1.1 y A.13.1.2)
9. Política de Seguridad de la Información para los Proveedores (A.15,1,1 y A.15.2.1)
10. Política de Planificación de la Continuidad Operacional (control A.17.1.1, A.17.1.2 y A.17.1.3)
11. listado de legislación vigente (A.18.1.1)
12. Procedimiento de Privacidad y Protección de la Información de Identificación Personal (Control A.18.01.04)

Fecha: 5 de diciembre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodriguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	Gabriela Cares	Jefa de DIEST	
6	Ana María Concha	Jefe DAG	
7	Sergio Hidalgo	Jefe Departamento de Auditoría	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Andrea Soto Araya	Encargada de SSI	
10	Nicol Jeria O.	Encargada de Ciberseguridad	
11			
12			

1

Procedimiento de Gestión para el Desarrollo y Mantención de Software Seguro
Control A.14.01.01

Tabla de Contenidos

Revisiones del procedimiento....2
1.. Objetivo. 2
2 Alcance. 3
3. Normas y Referencias. 3
4. Términos y Definiciones. 3
5. Roles y Responsabilidades....4
6. Seguridad en el Ciclo de Desarrollo del Software 5
6.1. Análisis y Especificación de Requerimientos de Seguridad 5
6.2. Seguridad en la Fase de Diseño 6
6.3. Seguridad en la Fase de Construcción 6
6.4. Seguridad en la Fase de Pruebas 7
6.5. Seguridad en el Paso a Producción 7
7. Modo de Operación 8
7.1 Flujo de Procedimiento para Desarrollo de Software Seguro Interno 8
7.2 Flujo de Procedimiento para Desarrollo Seguro Externo....9
7.3 Flujo de Procedimiento para Mantención de Software Seguro 10
7.4 Matriz del Procedimiento para Desarrollo de Software Seguro Interno 10
7.5 Matriz del Procedimiento para Desarrollo Seguro Externo....13
7.6 Matriz del Procedimiento para Mantenimiento de Software Seguro....15
7.7 Matriz de Responsabilidades. 17
8. Registro de Operación. 20
9. Anexo....20

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de la Información y Ciberseguridad	Enrique Opazo Encargado Área Desarrollo	Andrea Soto Araya Encargada Seguridad de la Información	Comité SGSIC

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	26/08/2019	Elaboración Inicial	Todas

1. Objetivo.

El objetivo del presente documento es servir como línea base para los diferentes procesos asociados a la construcción o mantención de sistemas, llevados a cabo tanto de forma interna como con apoyo de externos a la organización, con la finalidad de garantizar la seguridad de la información durante la totalidad del ciclo de vida de desarrollo de software, generando así, productos que cuenten con estándares de calidad que velen por la confidencialidad, integridad, disponibilidad y privacidad de los activos de información que serán soportados por los nuevos y actuales desarrollos.

2. Alcance.

El presente procedimiento debe ser aplicado a todos los funcionarios y funcionarias, de planta, contrata, honorarios de la Agencia de Calidad de la Educación y a proveedores de desarrollo de software externos a la Agencia de Calidad de la Educación, que, dado el cumplimiento de sus responsabilidades, se ven involucrados en el desarrollo o mantención de sistemas que interactúan con los activos de información que habitan dentro de la Agencia de Calidad de la Educación. Asimismo, este debe ser aplicado en cada una de las fases del desarrollo de software, según sea el caso. De esta manea deberá ser considerado como parte de les especificaciones técnicas de los servicios que se adquieran para este efecto.

De esta forma, y, en concordancia con lo establecido en la NCh ISO 27001:2013, el presente documento tiene su alcance sobre los siguientes controles:

a) A.14.01.01 – Análisis y Especificaciones de Requisitos de Seguridad
b) A.14.01.02 – Aseguramiento de Servicios de Aplicaciones en Redes Públicas
c) A.14.02.02 – Control de Cambios
d) A.14.02.05 – Principios de Ingeniería de Sistema Seguro
e) A.14.02.06 – Entorno de Desarrollo Seguro
f) A.14.02.08 – Prueba de Seguridad del Sistema
g) A.14.02.09 – Prueba de Aprobación del Sistema
h) A.12.01.04 – Separación de Ambientes de Desarrollo, Pruebas y Operación

3. Normas y Referencias.

a) NCh ISO 27,001:2013.
b) NCh ISO 27,002:2013.
c) Política de Desarrollo Seguro de Software aprobada por Resolución Exenta N° 1547, de 2019, de la Agencia de Calidad de la Educación.
d) OWASP Application Security Verification Standard (ASVS) 3.0
e) OWASP Testing Guide 4.0
f) OWASP Top 10 de riesgos
g) OWASP Top 10 de controles proactivos
h) Guía Técnica de Lineamientos para Desarrollo de Software, Gobierno Digital

4. Términos y Definiciones.

Ciclo de Desarrollo Seguro de	Proceso de construcción de software, cuyo objetivo es asegurar un entregable de calidad que, a la vez, garantice la seguridad de la información en todos sus ámbitos.

Software	
Seguridad de la Información	Preservación de la confidencialidad, la integridad, la disponibilidad y la privacidad de la información.
OWASP	Comunidad mundialmente reconocida que provee artículos gratuitos, metodologías, documentación, herramientas y tecnologías en el campo de seguridad para las aplicaciones web.

5. Roles y Responsabilidades.

a) **Jefatura Unidad Tecnologías de la Información y Comunicación de la División de Administración General:** Dentro de las principales tareas llevadas a cabo por el rol, se encuentra la supervisión de la correcta aplicación de los lineamientos establecidos en el presente documento. Adicionalmente, deberá promover mejoras sobre el mismo, buscando siempre el mejoramiento continuo de la protección brindada a los activos de información mediante los sistemas que son construidos tanto dentro como fuera de la organización.

b) **Encargado Área de Desarrollo de Software, de la Unidad de Tecnologías de la Información y Comunicación:** Como principal labor, este rol deberá velar por la correcta ejecución de los lineamientos expresados en el presente documento durante todas las fases del ciclo de desarrollo de software, garantizando de esta forma un nivel aceptable de protección a los activos de información asociados a la organización involucrados en este tipo de proyectos. Complementariamente, deberá promover mejoras al presente documento tanto en función de las necesidades de la organización, como de los cambios o promulgaciones de lineamientos externos asociados con la seguridad de la información. Adicionalmente, deberá gestionar la contratación y supervisión de nuevos proveedores de desarrollo de software, en concordancia con los lineamientos aquí establecidos.

c) **Equipos de Desarrollo Internos:** Estarán encargados de dar cumplimiento a los lineamientos expresados en el presente documento durante la construcción o actualización de productos de software, con excepción de aquellos que están especificados para el trato con proveedores de servicios de software.

d) **Equipos de Desarrollo Externos:** Serán estos los encargados de aplicar activamente todos los lineamientos aquí expresados, alineándose así con los requerimientos internos para el desarrollo seguro de software y haciendo especial énfasis en aquellos puntos especificados para el trato con proveedores de servicios de software.

e) **Encargada/o de Seguridad de Información:** Será este el rol encargado de velar por la correcta aplicación de los lineamientos aquí establecidos. Así mismo, será este rol el encargado de apoyar los procesos de actualización de este documento, prestando una asesoría activa desde la perspectiva de la seguridad de la información y cómo ésta debe ser incluida de forma óptima en el ciclo de vida de los diferentes desarrollos/mantenciones de software de la Agencia.

f) **Jefatura de División Solicitante:** Hace referencia a la División de la Agencia que solicitó el desarrollo del sistema en cuestión. Es labor de esta área colaborar activamente en todos los procesos asociados con el desarrollo, haciendo principal énfasis en la fase de requerimientos y la elaboración del diseño de la solución en cuestión.

g) **Equipo de Mantención:** Equipo que puede estar conformado tanto por agentes internos o externos a la organización, cuya principal función es llevar a cabo la mantención de los sistemas de la Agencia. Así mismo deberán colaborar activamente con el Jefe de Proyectos Designado.

h) **Jefe de Proyecto:** Supervisor designado por el Encargado del Área de Desarrollo de Software para el seguimiento de los proyectos que están siendo llevados a cabo en la organización – tanto por agentes internos como externos a esta – con la finalidad de garantizar una correcta gestión sobre estos.

i) **Equipo de Pruebas:** Equipo encargada de la realización de pruebas sobre los sistemas que son construidos o mejorados para la institución. Es importante denotar que esta área puede estar conformada tanto por agentes internos como externos a la organización en cuestión.

6. Seguridad en el Ciclo de Desarrollo del Software.

La seguridad es un pilar fundamental dentro del ciclo de desarrollo del software, debido a que permite la construcción de un sistema que no solo será funcional, si no que también protegerá los activos de información que en el futuro habitarán en él. En función de lo anterior, y con la finalidad de estipular correctamente las consideraciones que cualquier desarrollo llevado a cabo por la Agencia debe tener en relación con la seguridad, independiente de la metodología de desarrollo que se utilizará, a continuación, se estipulan ciertos marcos de referencia asociados con la construcción de software seguro:

1. OWASP ASVS: Guía de OWASP para la toma de requerimientos de seguridad de información.
2. OWASP Testing Guide: Guía elaborada por OWASP, para la ejecución de las pruebas de seguridad sobre el sistema desarrollado.
3. OWASP Top 10 de riesgos: Ranking emitido por OWASP, sobre los diez (10) riegos más críticos asociadas al desarrollo de aplicaciones.
4. OWASP Top 10 de controles proactivos: Definición de los diez (10) controles proactivos a considerar durante el desarrollo de software para mitigación del Top 10 de riesgos.
5. Guía Técnica para el Desarrollo Seguro de Software, Gobierno Digital: Guía emitida por el Gobierno de Chile, en la cual se pueden encontrar consideraciones técnicas asociados al desarrollo de software seguro.

6.1. Análisis y Especificación de Requerimientos de Seguridad.

En conformidad con lo establecido en la Política de Desarrollo Seguro, los requerimientos para cualquier tipo de desarrollo o mantención de software para la Agencia deben especificar la necesidad de implementación de controles. Estas especificaciones deben incorporar tanto controles estándar como de apoyo. En conformidad con lo detallado anteriormente, se deberán tener en cuenta las siguientes especificaciones:

a) Deberá existir un proceso de evaluación de riesgos previo a la construcción o mantenimiento de sistemas en función de la criticidad de los activos de información involucrados en éste. Durante este proceso se deberá considerar como principal input la documentación asociada a los Top 10 de OWASP, tanto de riesgos como de controles, con el principal objetivo de sentar las bases mínimas de seguridad para la construcción de un sistema que no contenga las vulnerabilidades allí especificadas.

b) Los requerimientos de seguridad y controles requeridos deberán ser analizados cuidadosamente tanto en función de la criticidad de los activos de información que se desean proteger como del costo que implica la implementación de estos. Adicionalmente, los requerimientos se deberán realizar en conformidad con lo detallado en la guía OWASP ASVS 3.0, para el análisis y especificación de requerimientos de seguridad.

c) Para cualquier tipo de desarrollo o mantención de software que sea externalizado, se deberán especificar en los Términos de Referencia (TDR) consideraciones básicas de seguridad asociadas con lo especificado en la Política de Desarrollo Seguro, considerando también lo expuesto en la Guía Técnica de Desarrollo de Software dispuesto por el Gobierno. De esta forma, la Agencia garantiza que los proveedores que apoyarán los procesos de desarrollo y/o

mantención de software poseen por lo menos las mismas bases de seguridad que establece la organización.

d) Se debe considerar también, que la implementación de un control es considerablemente más efectiva y menos costosa en las fases más tempranas del desarrollo o mantención del software. En función de lo anterior, se debe velar por la correcta asignación de estos en la toma de requerimientos.

e) Cualquier proceso de toma de requerimientos que se desee llevar a cabo dentro de la organización debe incorporar de forma activa al área de negocio que hizo solicitud del desarrollo o mantención en cuestión. Así mismo, se debe contar con la Encargada de Seguridad de Información como rol asesor en estas definiciones.

6.2. Seguridad en la Fase de Diseño.

En conformidad con lo establecido anteriormente, es importante detallar que todo diseño de la solución debe ser debidamente revisado por el jefe de proyecto asignado, con el objetivo de detectar de forma temprana funcionalidades que no han sido correctamente aplicadas, o que no protegen correctamente los activos de información involucrados. De esta forma, se deberán tener en cuenta las siguientes especificaciones:

a) En caso de que la construcción del sistema sea llevada a cabo mediante el apoyo de proveedores externos a la institución, la construcción del diseño de la solución deberá ser supervisada directamente por el Jefe de Proyecto asignado, el cual podrá solicitar asesoría por parte de la Encargada de Seguridad de Información de la Agencia.

b) La construcción y la revisión de cualquier diseño deberá ser efectuada considerando los requerimientos establecidos durante el análisis y especificación de requerimientos, detallado en el punto anterior. Cabe destacar que durante esta fase la organización puede valerse del material entregado por OWASP.

6.3. Seguridad en la Fase de Construcción.

La seguridad debe de ser considerada como un elemento fundamental tanto en el desarrollo del sistema como en el ambiente en el que este será llevado a cabo. Así mismo, es necesario tener en cuenta las siguientes especificaciones:

a) Cualquier desarrollo o mantención llevada a cabo para la agencia deberá estar en conformidad con lo establecido tanto en la Guía Técnica de Desarrollo de Software dispuesta por el Gobierno, como en la Política de Desarrollo Seguro. En caso de que este proceso este siendo llevado a cabo por proveedores externos de la institución, el Jefe de Proyecto asignado por el Encargado del Área de Desarrollo de Software, deberá asegurarse de que los proveedores estén siguiendo los lineamientos especificados en los documentos anteriormente mencionados.

b) Se deberán tener en consideración todas las definiciones establecidas en etapas anteriores del proceso (análisis y especificación de requerimientos, y diseño).

c) Los desarrollos internos deberán incorporar la utilización de repositorios de código fuente con la capacidad de versionar el mismo que contemplen control de acceso y asignación de privilegios sobre el mismo en función de las responsabilidades del rol en el proyecto.

d) Así mismo, deberán contemplar consideraciones asociadas a la seguridad de los ambientes de desarrollo, principalmente aquellas asociadas con la separación estricta de los ambientes de prueba y productivos, además del control de acceso a éste solo para roles de desarrollo.

e) Se deben considerar las buenas prácticas asociadas a él o los lenguajes de programación a utilizar en el desarrollo de software, según lo propuesto por la Guía Técnica de Lineamientos para Desarrollo de Software.

- En caso de que el sistema sea desarrollado externamente, el jefe de proyecto asignado deberá supervisar que esto sea llevado a cabo con las debidas consideraciones de seguridad asociadas al ambiente de desarrollo.

6.4. Seguridad en la Fase de Pruebas.

La seguridad como concepto debiese ser considerada como un elemento de gran importancia en la realización de pruebas sobre los sistemas que están bajo construcción o mantenimiento, con el principal objetivo de construir un sistema que no solo garantice calidad desde el punto de vista funcional, sino que también desde el punto de vista no funcional, aspecto en el cual se debe considerar la seguridad de información de forma integral. En función de lo anterior, es necesario tener en cuenta las siguientes especificaciones:

a) Cualquier tipo de prueba a realizar debe estar en estricta conformidad con lo establecido en la fase de Requerimientos y Diseño.

b) Según lo establecido en la Política de Desarrollo seguro, se deberá restringir el uso de datos productivos para el ambiente de pruebas. En caso de requerir este tipo de datos para la realización de pruebas, se debe excepcionar mediante un proceso riguroso que considere la autorización del dueño de estos activos de información.

c) Como principal INPUT para esta fase, se deberá considerar la OWASP Testing Guide 4.0. De la misma manera, las pruebas llevadas a cabo deberán estar planteadas en función de la validación del Top 10 de controles proactivos que este propone, con la finalidad de evitar que un software con los riesgos especificados pase a la fase de producción.

d) En el caso de que el desarrollo este siendo llevado de forma externa, se deberá solicitar y validar el plan de pruebas, con el objetivo de asegurar la correcta realización de éstas.

e) Las pruebas no deben ser realizadas por el mismo equipo o personas que efectuaron las labores de desarrollo.

f) Para el caso de desarrollos externos, las pruebas deben desarrollarse en un ambiente específico, dedicado a estas actividades y separado de los ambientes de desarrollo y producción.

6.5. Seguridad en el Paso a Producción.

Es esencial poder verificar la seguridad de los sistemas antes de que estos sean puestos en producción, con la finalidad de proteger los activos que habitarán en estos. En función de lo anterior, es necesario tener en cuenta las siguientes consideraciones:

a) Cualquier tipo de paso a producción debe estar en estricta concordancia con lo establecido en la Política de Desarrollo Seguro de la Agencia. En función de lo anterior, en caso de que un sistema no cumpla con el plan de pruebas antes mencionado, no podrá ser puesto en producción.

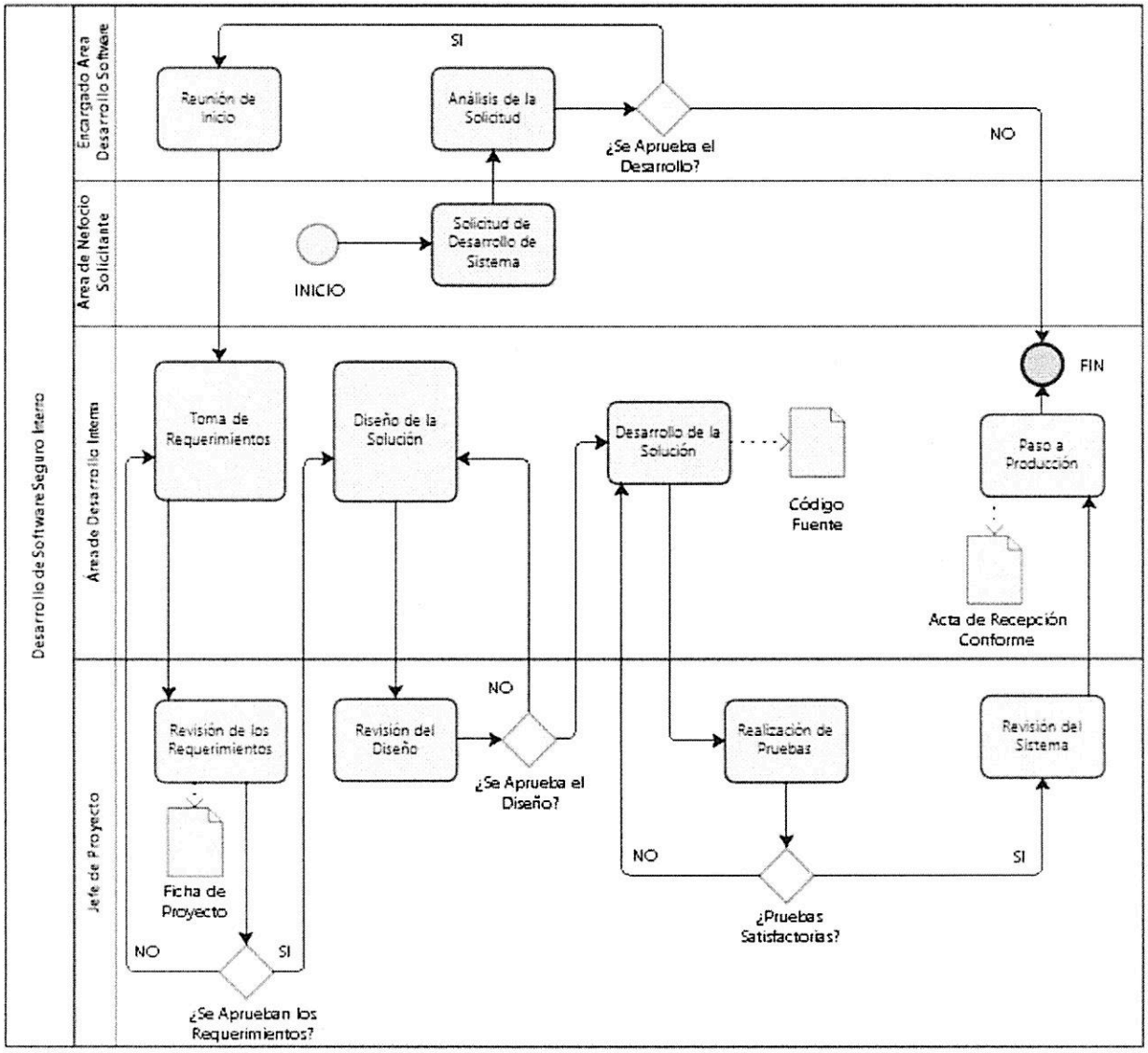
b) El Jefe de Proyecto asignado deberá revisar el desarrollo antes de que este pase a producción. Es importante detallar que, en caso de ser necesario, este podría solicitar la colaboración de ciertos roles para llevar a cabo este proceso.

c) Así mismo, deberán contemplar consideraciones asociadas a la seguridad del ambiente de producción, principalmente aquellas asociadas con la separación estricta de los ambientes de desarrollo y pruebas, además del control de acceso a éste solo para roles asociados a producción y plataforma.

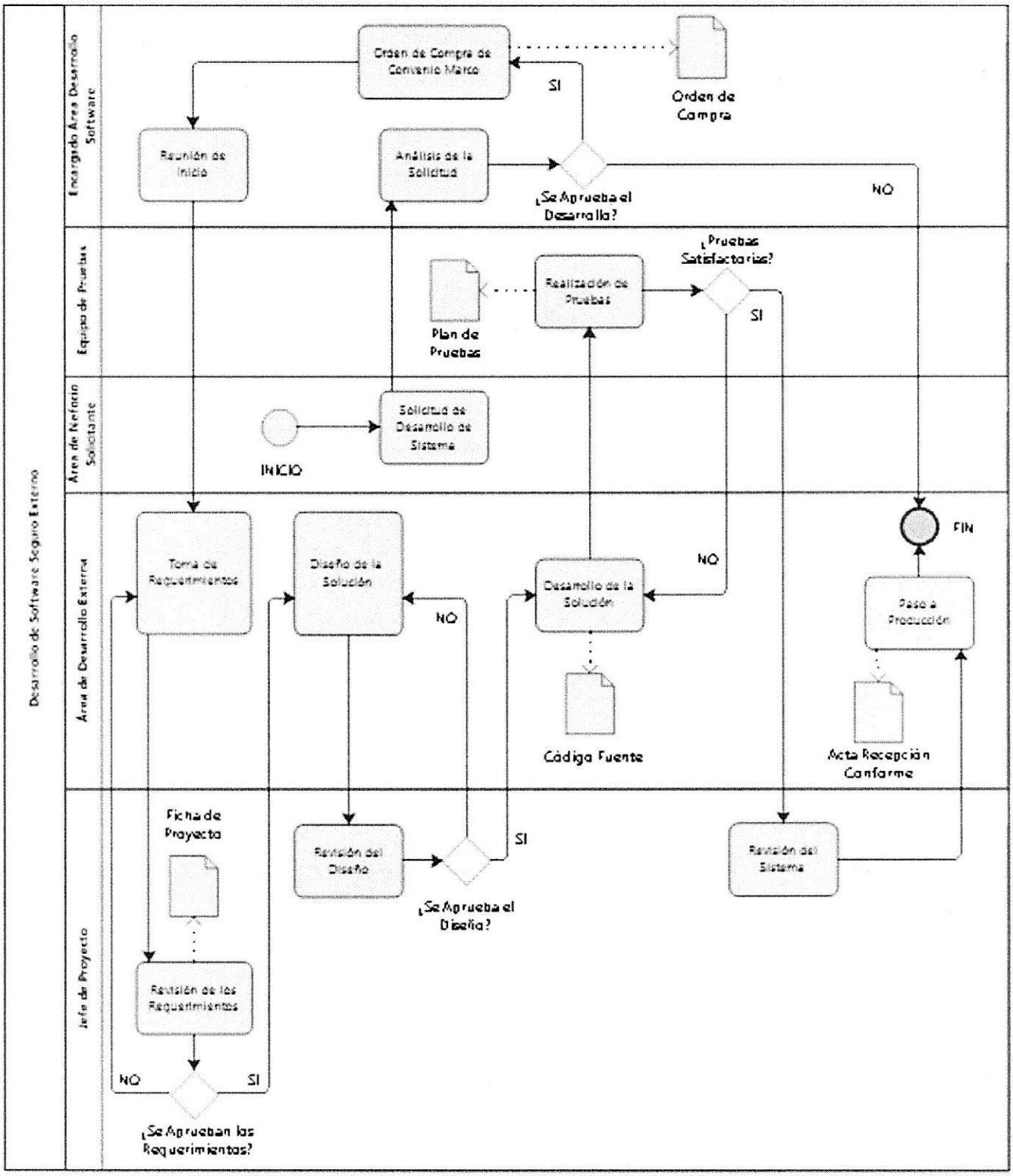
7. Modo de Operación.

A continuación, se describen los flujos procedimentales para la gestión para el desarrollo y mantención de software seguro.

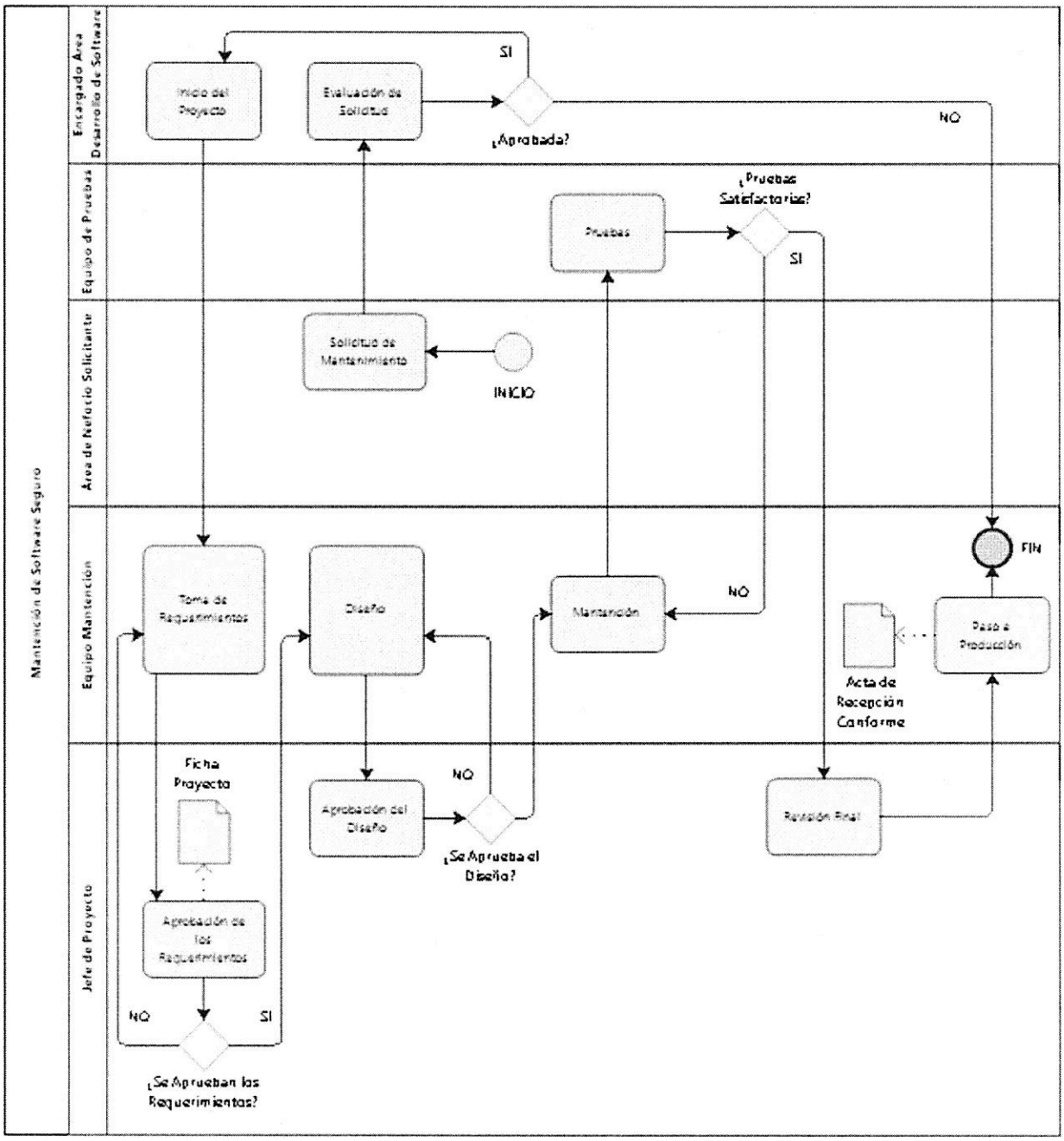
7.1 Flujo de Procedimiento para Desarrollo de Software Seguro Interno.



7.2 Flujo de Procedimiento para Desarrollo Seguro Externo.



7.3 Flujo de Procedimiento para Mantención de Software Seguro.



7.4 Matriz del Procedimiento para Desarrollo de Software Seguro Interno.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Solicitud de Desarrollo de Sistema	Al identificar una necesidad que puede ser satisfecha mediante el desarrollo de un sistema, el área de negocio deberá comunicar dicha necesidad a TIC.	Área de Negocio Solicitante	2

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
2	Análisis de la Solicitud	La solicitud en cuestión es analizada tomando en cuenta los factores asociados, luego de lo cual, pueden ocurrir dos posibles escenarios: - Se aprueba la solicitud (3) - Se rechaza la solicitud (FIN)	Encargado de Desarrollo de Software	3 o FIN
3	Reunión de Inicio	Una vez que han sido asignados los recursos que serán parte del proyecto en cuestión, se procede a sostener una reunión de Inicio en la que participarán todos los involucrados.	Encargado Área de Desarrollo de Software / Jefe de Proyecto	4
4	Toma de requerimientos	Los requerimientos deberán ser tomados con las debidas consideraciones de seguridad pertinentes, con principal énfasis en el OWASP ASVS, para la toma de requerimientos segura. En función de lo anterior, se deberán seguir las consideraciones en este documento detalladas. Así mismo, la participación del área de negocio solicitante es de gran importancia para el proceso.	Equipo de Desarrollo Interno / Área de Negocio Solicitante	5
5	Revisión de los Requerimientos	Una vez se hayan construido los requerimientos del sistema en cuestión, estos deberán ser revisados por el Jefe de Proyecto. A partir de esto se generará la Ficha de Proyecto, la cual hace referencia a los requerimientos del área de negocio solicitante y como estos serán abordados durante el proyecto. En función de lo anterior, pueden ocurrir dos posibles escenarios: - La toma de requerimientos fue aprobada (6) - La toma de requerimientos es insuficiente (4)	Jefe de Proyecto	4 o 6

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
6	Diseño de la solución	El diseño de la solución debe ser llevado a cabo en conformidad con las consideraciones detalladas en el presente documento, y con el apoyo activo del área de negocio solicitante.	Equipo de Desarrollo Interno / Área de Negocio Solicitante	7
7	Revisión del Diseño	El diseño de la solución deberá ser revisado por el Jefe de Proyectos designado. De esta forma, pueden ocurrir dos posibles escenarios: - El diseño es aprobado (8) - El diseño es insuficiente (6)	Jefe de Proyectos	6 o 8
8	Desarrollo de la solución	Se deberá llevar a cabo la construcción de la solución en conformidad con lo previamente establecido en el documento, haciendo principal énfasis en la Guía Técnica para el Desarrollo Seguro, emitida por el Estado.	Equipo de Desarrollo Interno	9
9	Pruebas	Las pruebas deberán ser realizadas haciendo énfasis en la seguridad, y en consideración de los lineamientos aquí establecidos. Así mismo, se deberá considerar la OWASP Testing Guide como principal fuente de información para la realización de las pruebas asociadas con la seguridad de la información. En función de lo anterior, pueden ocurrir dos posibles escenarios: - Resultados suficientes (10) - Resultados insuficientes (8)	Jefe de Proyecto	8 o 10
10	Revisión del Sistema	Una vez que han concluido las pruebas a realizar sobre el sistema en cuestión, este debe ser revisado, con el objetivo de determinar si este puede ser pasado a producción o no.	Jefe de Proyectos	11

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
11	Paso a Producción	Una vez han concluido correctamente todos los procesos, es posible hacer el paso a producción con las debidas consideraciones. Finalmente, es emitida el acta de recepción conforme, la cual involucra la entrega del producto final al área de negocio solicitante.	Equipo de Desarrollo Interno	FIN

7.5 Matriz del Procedimiento para Desarrollo Seguro Externo

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Solicitud de Desarrollo de Sistema	Al identificar una necesidad de gran importancia que puede ser solucionada mediante el desarrollo de un sistema, el área de negocio eleva una solicitud a TIC para que su caso sea analizado.	Área de Negocio Solicitante	2
2	Análisis de la Solicitud	La solicitud en cuestión es analizada tomando en cuenta los factores asociados, luego de lo cual, pueden ocurrir dos posibles escenarios: - Se aprueba la solicitud (3) - Se rechaza la solicitud (FIN)	Encargado Área de Desarrollo de Software	3 o FIN
3	Orden de Compra de Convenio Marco	En conformidad con lo establecido en la Política de Desarrollo Seguro de la Agencia, es necesario que existan ciertas consideraciones iniciales previas al contrato relacionadas con la seguridad de la información.	Encargado de Área de Desarrollo de Software	4
4	Reunión de Inicio	Una vez que se ha contratado un proveedor para la realización del proyecto, se sostiene una reunión con todos los participantes en este.	Encargado de Área de Desarrollo de Software	5

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
5	Toma de Requerimientos	Los requerimientos deberán ser tomados con una estricta colaboración con el área de negocio solicitante. Adicionalmente, este proceso deberá ser supervisado activamente por el Jefe de Proyecto designado para el trabajo. Cualquier toma de requerimiento deberá ser llevada a cabo en estricta conformidad con lo establecido en este procedimiento.	Equipo de Desarrollo Externo / Área de Negocio Solicitante / Jefe de Proyecto	6
6	Aprobación de los Requerimientos	Los requerimientos deberán ser aprobados por el Jefe de Proyecto. A partir de esto se generará la Ficha de Proyecto, la cual hace referencia a los requerimientos del área de negocio solicitante y como estos serán abordados durante el proyecto. En función de lo anterior, pueden darse los siguientes escenarios: - La toma de requerimientos fue aprobada (7) - La toma de requerimientos no fue aprobada (5)	Jefe de Proyecto	5 o 7
7	Diseño de la Solución	Cualquier diseño deberá contar con las debidas consideraciones de seguridad de la información, en conformidad con lo establecido en este procedimiento.	Equipo de Desarrollo Externo / Jefe de Proyecto / Área de Negocio Solicitante	8
8	Aprobación del Diseño de la Solución	La solución en cuestión deberá ser aprobada por el Jefe de Proyecto designado. En función de lo anterior, pueden darse los siguientes escenarios: - El diseño es aprobado (9) - El diseño no es aprobado (7)	Jefe de Proyecto	7 o 9

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
9	Desarrollo de la Solución	La solución deberá ser desarrollada en conformidad con lo establecido tanto en este documento como con la Guía de Desarrollo Seguro, emitida por el Estado. Adicionalmente, el desarrollo deberá ser activamente supervisado por el Jefe de Proyecto designado.	Jefe de Proyecto / Equipo de Desarrollo Externo	10
10	Pruebas	Las pruebas deberán ser realizadas en conformidad con lo aquí establecido. Adicionalmente, el Jefe de Proyecto designado deberá procurar la ejecución de pruebas asociadas con la seguridad de la información, con la OWASP Testing Guide como base para esto. En función de lo anterior, pueden ocurrir dos posibles escenarios: - El sistema pasa las pruebas (11) - El sistema no pasa las pruebas (9)	Jefe de Proyecto / Equipo de Pruebas	9 o 11
11	Revisión Final del Sistema	Una vez se han llevado a cabo todos los demás procesos, el sistema debe ser revisado por el Jefe de Proyecto, quien procurará que este se encuentre en condiciones para pasar a producción, en conformidad con lo establecido en el presente documento.	Jefe de Proyecto	12
12	Paso a Producción	Cualquier paso a producción deberá ser realizado en conformidad con las consideraciones expresadas en el presente documento. Así mismo, este proceso deberá ser debidamente supervisado por el Jefe de Proyectos en designado. Finalmente, es emitida un acta de recepción conforme, la cual involucra la correcta entrega del producto final al área de negocio solicitante.	Jefe de Proyecto / Equipo de Desarrollo Externo	FIN

7.6 Matriz del Procedimiento para Mantenimiento de Software Seguro

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Solicitud de Mantenimiento	El área de negocio eleva una solicitud asociada a una necesidad de mantenimiento de la herramienta de software en cuestión.	Área de Negocio Solicitante	2

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
2	Evaluación de Solicitud	El Encargado del Área de Desarrollo de Software debe analizar la solicitud, en función de esto, pueden ocurrir dos posibles cursos de acción: - Se aprueba la solicitud (3) - Se rechaza la solicitud (FIN)	Encargado Área de Desarrollo de Software	3
3	Inicio del Proyecto	Al inicio del proyecto el Encargado del Área de Desarrollo de Software asigna un Jefe de Proyecto, quien estará encargado de supervisar las labores llevadas a cabo por el equipo. En función de lo anterior, es importante notar que el equipo puede estar formado por personal interno o externo a la Agencia.	Jefe de Proyecto	4
4	Toma de Requerimientos	Los requerimientos serán tomados siguiendo los lineamientos expresados en el presente documento.	Equipo de Mantenimiento / Área de Negocio Solicitante	5
5	Aprobación de los Requerimientos	Los requerimientos deberán ser aprobados por el Jefe de Proyecto. En función de lo anterior, será liberada una ficha de proyecto, la cual hace referencia a los requerimientos iniciales solicitados por el área de negocio en cuestión. En función de lo anterior, pueden darse los siguientes escenarios: - La toma de requerimientos fue aprobada (6) - La toma de requerimientos no fue aprobada (4)	Jefe de Proyecto	4 o 6
6	Diseño	El diseño debe ser llevado a cabo en conformidad con lo expresado en el presente documento	Equipo de Mantenimiento / Área de Negocio Solicitante	7

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
7	Aprobación del Diseño	El diseño del mantenimiento en cuestión deberá ser aprobado por el Jefe de Proyecto designado. En función de lo anterior, pueden darse los siguientes escenarios: - El diseño es aprobado (8) - El diseño no es aprobado (6)	Jefe de Proyecto	6 o 8
8	Mantención	El mantenimiento deberá ser llevado a cabo en conformidad con lo establecido tanto en este documento como con la Guía de Desarrollo Seguro.	Jefe de Proyecto / Equipo Mantenimiento	9
9	Pruebas	Las pruebas deberán ser realizadas en conformidad con lo aquí establecido. Adicionalmente, el Jefe de Proyecto designado deberá procurar la ejecución de pruebas asociadas con la seguridad de la información, con la OWASP Testing Guide como base para esto. En función de lo anterior, pueden ocurrir dos posibles escenarios: - El sistema pasa las pruebas (10) - El sistema no pasa las pruebas (8)	Jefe de Proyecto / Equipo de Pruebas	8 o 10
10	Revisión Final	La revisión final del sistema sobre el que se ha hecho mantenimiento debe ser llevada a cabo por el Jefe de Proyecto en cuestión.	Jefe de Proyecto	11
11	Paso a Producción	Cualquier paso a producción deberá ser realizado en conformidad con las consideraciones expresadas en el presente documento. Así mismo, este proceso deberá ser debidamente supervisado por el Jefe de Proyectos en designado.	Jefe de Proyecto / Equipo de Mantenimiento	FIN

7.7 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

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

De esta forma, la matriz de responsabilidades para el Desarrollo Seguro Interno se estructura de la siguiente manera:

ID	ACTIVIDAD	Desarrollo Interno	Área Negocio	Jefe de Proyecto	Encargado Seguridad	Jefatura TIC	Encargado Desarrollo
1	**Solicitud de Desarrollo**	-	R / E	-	I	I	I
2	**Análisis de la Solicitud**	-	I	-	I	I / C / A	R / E
3	**Reunión de Inicio**	I	I	I	I	I	R / E
4	**Toma de Requerimientos**	R / E	C / A	I	I / C	I	I
5	**Revisión de los Requerimientos**	C	C	R / E / A	I	I	I
6	**Diseño de la Solución**	R / E	C / A	I	I / C	I	I
7	**Revisión del Diseño**	C	C	R / E / A	I	I	I
8	**Desarrollo de la Solución**	R / E	I	I	I	I	I
9	**Pruebas**	C	I	R / E/ A	I / C	I	I
10	**Revisión del Sistema**	R / E / A		R / E / A	I / C	I	I / C
11	**Paso a Producción**	R / E	C	A	I	I	I

Así mismo, la matriz de responsabilidades asociada al Desarrollo Seguro Externo se estructura de la siguiente manera:

ID	ACTIVIDAD	Desarrollo Externo	Área Negocio	Equipo Pruebas	Jefe Proyecto	Encargado Desarrollo	Encargado Seguridad	Jefatura TIC
1	**Solicitud de Desarrollo**	-	R / E	-	-	I	I	I
2	**Análisis de Solicitud**	-	I	-	-	I	I	I / C / A
3	**Licitación y Consideraciones Iniciales**	-	-	-	-	R / E / A	I / C	I
4	**Reunión de Inicio**	I	I	I	I	R / E	I	I
5	**Toma de Requerimientos**	R / E	C / A	-	A	I	I / C	I
6	**Aprobación de los Requerimientos**	C	C	-	R / E / A	I	I	I
7	**Diseño de la Solución**	R / E	C / I	-	A	I	I / C	I
8	**Aprobación del Diseño de la Solución**	C	C	-	R / E / A	I	I	I
9	**Desarrollo de la Solución**	R / E	I	-	A	I	I	I
10	**Pruebas**	C	-	R / E / A	A	I	I / C	I
11	**Revisión Final del Sistema**	C	C	-	R / E / A	I	I / C	I
12	**Paso a Producción**	R / E	I	-	A	I	I	I

Finalmente, la matriz de responsabilidades asociada al Mantenimiento de Software Seguro se estructura de la siguiente manera:

ID	ACTIVIDAD	Equipo Mantenn.	Área Negocio	Equipo Pruebas	Jefe Proyecto	Encargado Desarrollo	Encargado Seguridad	Jefatura TIC
1	**Solicitud de Mantenimiento**	-	R / E / A	-	-	-	-	I
2	**Evaluación de Solicitud**	-	C / I	-	-	R / E / A	I	I
3	**Inicio del Proyecto**	I	I	-	I	R / E / A	-	I
4	**Toma de Requerimientos**	R / E	C / A	-	A	I	I / C	I
5	**Aprobación de los Requerimientos**	C	C	-	R / E / A	I	I	I
6	**Diseño**	R / E	C / I	-	A	I	I / C	I
7	**Aprobación del Diseño**	C	C	-	R / E / A	I	I	I
8	**Mantención**	R / E	I	-	A	I	I	I
9	**Pruebas**	C	-	R / E / A	A	I	I / C	I
10	**Revisión Final**	C	C	-	R / E / A	I	I / C	I
11	**Paso a Producción**	R / E	I	-	A	I	I	I

8. Registro 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 (solo para desarrollos externos) (A.14.2.8; A.14.2.9)	-	Jefe de Proyecto	2 años / Google Drive	Digital	Google Drive, Documentación por Proyecto
Código Fuente (solo para desarrollos internos) (A.14.2.2; A.14.2.6)	-	Jefe de Proyecto	3 años / Repositorios	Digital	GitLab
Pantalla de AWS Console (Solo desarrollos internos) (A.12.1.4)	-	Encargado Área Desarrollo	1 año / Google Drive	Digital	Google Drive Unidad de TIC

9. Anexo.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Procedimiento de Elaboración de Plan Anual de Capacitación, Formación y Entrenamiento (Control A.07.02.02)
2. Política de Gestión de Activos (Control A.8.1.2, A.8.1.3, A.8.3.1 Y A.8.3.3)
3. Procedimiento de Alta y Baja de Cuentas de Usuario a la Red y Servicios de Red (Control A.9.1.2, A.9.2.1, A.9.2.2 Y A.9.2.3)
4. Procedimiento de Gestión de Contraseñas (A.9.4.3, A.9.2.4 y A.9.3.1)
5. Política de Gestión de Controles Criptográficos y Contraseñas (Control A.10.1.1 y A.10.1.2)
6. Procedimiento de Gestión para el Desarrollo y Mantención de Software Seguro (A.14.1.1, A.14.1.2, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9 y A.12.1.4)
7. Procedimiento de Sincronización de Relojes (Control A.12.04.04)
8. Política de desarrollo seguro (control A.14.2.1)
9. Política de gestión de Incidentes control A.16.01.01
10. Procedimiento de Gestión de Incidentes (Control A.12.4.1, A.12.4.3, A.16.1.02, A.16.1.4, A.16.1.5 Y A.16.1.6)

Fecha: 2 de octubre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodriguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD (S)	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	María de la Luz González.	Jefa de DIEST (S)	
6	Ramón Gutiérrez P.	Jefe DAG (S)	
7	Sergio Hidalgo	Jefe Departamento de Auditoría	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Patrick Soto A.	Jefe TIC	
10	Andrea Soto Araya	Encargada de SSI	
11	Nicol Jeria O.	Encargada de Ciberseguridad	
12			

1

Procedimiento para Documentación de los Procedimientos Operacionales Control A.12.1.1

Tabla de Contenidos

Revisiones del Procedimiento 2
1. Objetivo. 2
2. Alcance. 3
3. Normas y Referencias. 3
4. Términos y Definiciones. 3
5. Roles y Responsabilidades. 4
6. Definiciones para la Documentación de Procedimientos Operacionales 4
7. Modo de Operación 5
7.1 Flujo de Procedimiento para Documentación de Procedimientos Operacionales. 5
7.2 Matriz Procedimiento para Documentación de Procedimientos Operacionales ...7
7.3 Matriz de Responsabilidades 6
8. Registro de Operación. 8
9. Anexo 8

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de Información y Ciberseguridad	Nicol Jeria Encargada de Ciberseguridad	Andrea Soto Encargada de Seguridad de Información	Comité de Seguridad de Información

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	31/10/2019	Elaboración inicial	Todas

1. Objetivo.

El presente procedimiento tiene por objetivo el entregar las definiciones asociadas a los procedimientos operacionales que se encuentran documentados y, a su vez, forman parte del alcance del Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC) de la Agencia de Calidad de la Educación, en adelante, la Agencia. Así mismo, define los roles y responsabilidades asociados a la gestión de esta documentación abarcando todo su ciclo de vida, desde su creación, hasta su revisión de cumplimiento a lo largo del tiempo.

2. Alcance.

Las definiciones vertidas en este procedimiento abarcan todos los procedimientos de operación que se encuentran documentados y forman parte del alcance del SGSIC de la Agencia de Calidad de la Educación, sus registros de operación para dar cumplimiento al Programa de Mejoramiento de la Gestión (PMG) asociado a estas temáticas, así como las evidencias de auditoría si es que aplican.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27001:2013, el presente documento tiene su alcance sobre los siguientes controles:

- A.12.01.01 – Procedimientos de operación documentados.
- A.18.01.03 – Protección de registros.

3. Normas y Referencias.

- NCh ISO 27,001:2013.
- NCh ISO 27,002:2013.
- Política General de Seguridad de la Información y Ciberseguridad, aprobada mediante Resolución Exenta N° 589, de 2019, de la Agencia de Calidad de la Educación.
- Estructura Funcional del Sistema de Gestión de Seguridad de Información y Ciberseguridad, aprobada por Resolución Exenta N° 1024, de 2019, de la Agencia de Calidad de la Educación.

4 Términos y Definiciones.

Contraseña	Una contraseña (también conocida como clave o password), es una forma de autenticación que hace utilización de información secreta para controlar el acceso hacia algún recurso. Esta es de uso personal, y debe mantenerse en secreto. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.
Activos de Información	Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
Seguridad de la Información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.
Active Directory (AD)	Repositorio de cuentas de usuarios y equipos asociados a la organización en cuestión.

5. Roles y Responsabilidades.

a) **Validador(a) Técnico(a):** Si bien el dueño o dueña funcional del mismo es aquel rol que de forma práctica ejecuta el flujo procedimental, la responsabilidad de aprobación o validación técnica corresponde al Rol Ejecutivo encargado de la correcta ejecución del procedimiento.

b) **Aprobador(a) Administrativo(a):** El o la Aprobadora Administrativa corresponde al rol Líder del sistema de gestión dentro del cual circunscribe su alcance el procedimiento. De esta forma, para el caso del Sistema de Gestión de Seguridad de Información, será el rol de Encargada(o) de Seguridad de Información el aprobador Administrativo, o en casos de ausencia de éste, la responsabilidad caerá sobre la Encargada(o) de Ciberseguridad.

c) **Usuario:** Hace referencia al funcionario/a que cuenta – o debe contar – con acceso a los sistemas o recursos tecnológicos de la agencia según su ámbito de responsabilidades. Tiene la responsabilidad de mantener secreta la información de autenticación que se le ha hecho disponible.

d) **Comité Aprobador:** Corresponde a la instancia institucional mediante la cual se realiza la aprobación formal del procedimiento.

e) **Revisor Interno:** Corresponde al rol encargado de velar que los procedimientos se ejecuten de forma correcta más allá de la validación de funcionamiento operativo que entrega(n) su(s) registro(s) de operación.

6. Definiciones para la Documentación de Procedimientos Operacionales

La Agencia de Calidad de la Educación define, en el siguiente apartado del documento, que todos los procedimientos de operación que se encuentran dentro del alcance del SGSIC, deben estar documentados y aprobados por su validador técnico, revisor de tipo directivo y por el Comité de Seguridad de Información de la institución.

Adicional a lo anterior, tanto los registros de operación asociados a cada uno de éstos, así como las evidencias procedimentales internas, deben ser almacenadas en medios y/o lugares específicos donde se resguarde su confidencialidad, integridad, privacidad y disponibilidad, siendo estos considerados como activos de información que se encuentran bajo la gestión de los dueños funcionales de los procedimientos que le correspondan.

6.1 Registros de Operación.

Los registros de operación deberán ser almacenados de forma segura, considerando que se deben mantener medidas de control ad hoc a la criticidad que presenten por cada uno de sus atributos (confidencialidad, disponibilidad, integridad y privacidad), indicada en el inventario de activos de cada Dueño/Custodio de los Activos.

De esta forma, los registros de operación se almacenan en los siguientes medios:

a) **Registros de Operación para procedimientos sobre tecnologías de la información y comunicación:** Repositorio de Google Drive de la Unidad de Tecnologías de la Información y Comunicación.

b) **Registros de operación para procedimientos del SGSIC:** Repositorio de Google Drive de Seguridad de Información.

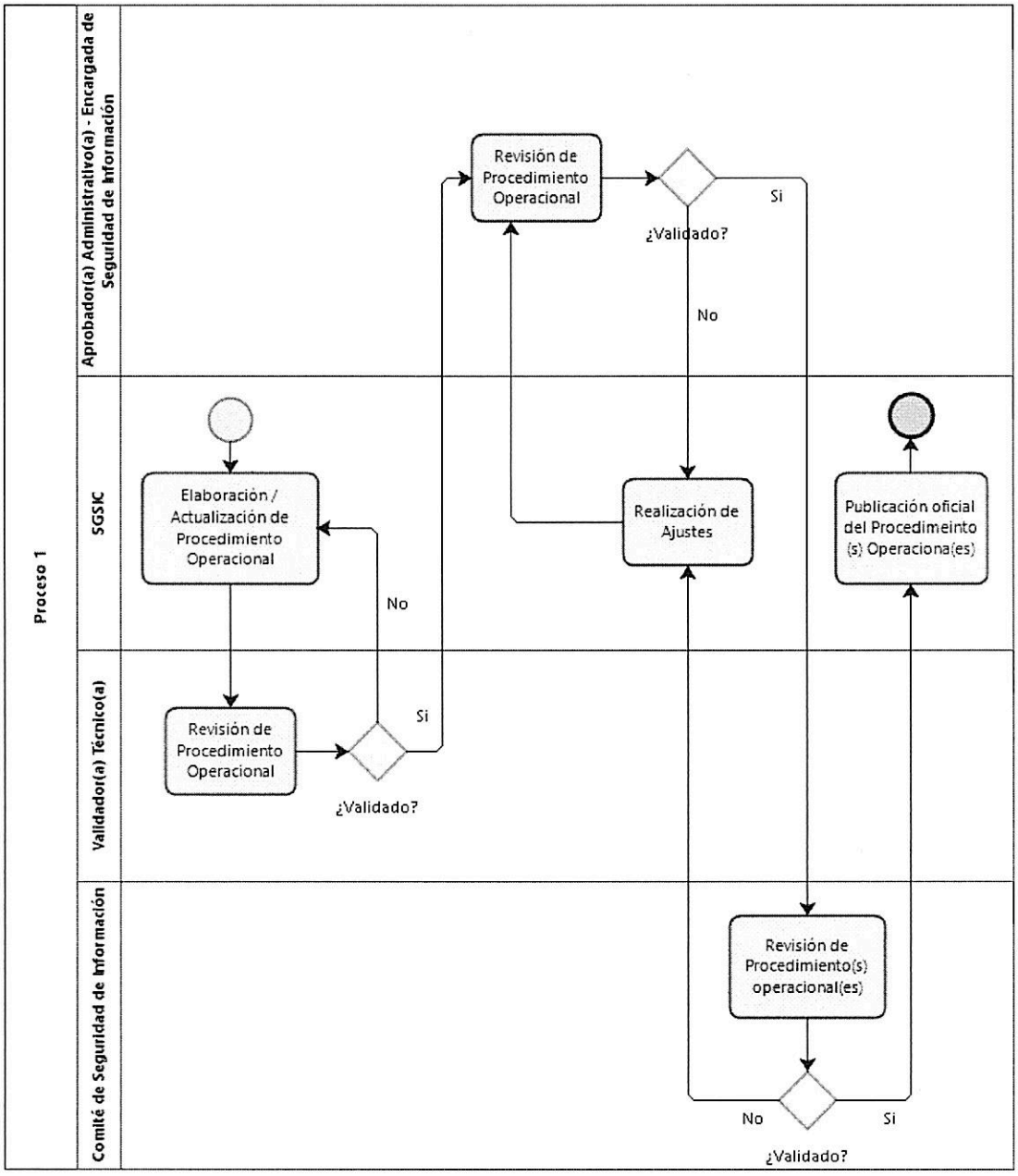
c) **Registros de Operación para Procedimientos de Gestión y Desarrollo de las Personas:** Repositorio Google Drive de Departamento de Gestión y Desarrollo de las Personas.

d) **Registros de Operación para procedimientos de privacidad de datos e información personal:** Repositorio de Google Drive de la División de Estudios.

7. Modo de Operación.

A continuación, se describen los flujos procedimentales para la documentación de procedimientos operacionales:

7.1 Flujo de Procedimiento para Documentación de Procedimientos Operacionales.



7.2 Matriz del Procedimiento para Documentación de Procedimientos Operacionales.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Elaboración / Actualización de Procedimiento Operacional	Según sea el caso, se deberá elaborar o realizar modificaciones de actualización uno o más procedimientos de operación que se encuentran dentro del alcance del SGSIC de la Agencia. Este deberá ser elaborado en estrecha interacción con el Dueño Funcional del mismo, es decir, con su validador técnico.	SGSIC	2
2	Revisión de Procedimiento Operacional	Una vez elaborado(s) el/los Procedimiento(s) Operacional(es) en cuestión, se deberán enviar formalmente vía correo electrónico al Validador Técnico para obtener su Visto Bueno. Se pueden dar las siguientes opciones: - El o los procedimientos de operación obtienen el Visto Bueno por parte del Validador Técnico (3). - El o los procedimientos de operación no obtienen el Visto Bueno por parte del Validador Técnico (1).	Validador(a) Técnico(a)	1 o 3
3	Revisión de Procedimiento Operacional	Una vez validado(s) técnicamente, el o los procedimientos de operación documentados deben ser revisados y validados por su Aprobador(a) Administrativo(a). A diferencia de la revisión ejercida en la actividad anterior, esta revisión tiene un foco en el alineamiento del procedimiento con los objetivos de la seguridad de información. Se pueden dar las siguientes opciones: - El o los procedimientos de operación obtienen el Visto Bueno por parte del Aprobador Administrativo (5). - El o los procedimientos de operación no obtienen el Visto Bueno por parte del Aprobador Administrativo (4).	Aprobador(a) Administrativo(a)	4 o 5

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
4	Realización de Ajustes	Se deberán realizar los ajustes necesarios según la retroalimentación entregada por el Validador(a) Administrativo(a).	SGSIC	3
5	Revisión de Procedimiento(s) operacional(es)	Una vez validado(s) administrativamente, el o los procedimientos de operación documentados deben ser revisados y validados por el Comité de Seguridad de Información. A diferencia de la revisión ejercida en la actividad anterior, esta revisión tiene un foco en el alineamiento del procedimiento con los objetivos institucionales, así como en el impacto de alto nivel que pueda tener su implementación. Se pueden dar las siguientes opciones: - El o los procedimientos de operación obtienen el Visto Bueno por parte del Comité de Seguridad de Información (6). - El o los procedimientos de operación no obtienen el Visto Bueno por parte del Comité de Seguridad de Información (4).	Comité de Seguridad de Información	4
6	Publicación oficial del Procedimiento(s) Operacional(es)	Una vez aprobado(s) el o los procedimientos considerados en el alcance de la iteración, deberán ser publicados y difundidos mediante los canales institucionales.	SGSIC	FIN

7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

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

De esta forma, la matriz de responsabilidades para el alta de usuarios en la red y los sistemas de red de la Agencia se estructura de la siguiente manera:

ID	ACTIVIDAD	SGSIC	Validador Técnico	Aprobador Administrativo	Comité SI
1	**Elaboración / Actualización de Procedimiento Operacional**	R/E	C	I	-
2	**Revisión de Procedimiento Operacional**	C	R/E	I	-
3	**Revisión de Procedimiento Operacional**	C	C/I	R/E	-
4	**Realización de Ajustes**	R/E	C	C	-
5	**Revisión de Procedimiento(s) operacional(es)**	C	C	C	R/E
6	**Publicación oficial del Procedimiento(s) Operacional(es)**	R/E	I	I	I

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Documento de Procedimientos de Operación Documentados	-	Encargada de Seguridad de Información	1 año / Google Drive	Digital	Repositorio Google de Seguridad de Información

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Política de Revisión Independiente del Sistema de Gestión de Seguridad de Información y Ciberseguridad (Control A.5.1.2, A.18.2.1, A.18.2.2 y A.18.2.3)
2. Procedimiento de Segregación de Funciones (Control A. 6.1.2)
3. Política para Transferencia y Manejo de Información (A. 8.2.2, A.8.2.3, A.8.3.2, A.13.2.1 y A.13.2.3)
4. Procedimiento de Controles y Perímetro de Seguridad Física (Control A.11.1.2 y A.11.1.4)
5. Procedimiento para Documentación de los Procedimientos Operacionales (control A.12.1.1 y A.18.1.3)
6. Política de Protección Contra Código Malicioso (Control A.12.02.01, A.12.5.1 y A.12.6.2)
7. Procedimiento de Gestión de Vulnerabilidades Técnicas (A.12.6.1)
8. Política de Controles de Red (control .13.1.1 y A.13.1.2)
9. Política de Seguridad de la Información para los Proveedores (A.15,1,1 y A.15.2.1)
10. Política de Planificación de la Continuidad Operacional (control A.17.1.1, A.17.1.2 y A.17.1.3)
11. listado de legislación vigente (A.18.1.1)
12. Procedimiento de Privacidad y Protección de la Información de Identificación Personal (Control A.18.01.04)

Fecha: 5 de diciembre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodriguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	Gabriela Cares	Jefa de DIEST	
6	Ana María Concha	Jefe DAG	
7	Sergio Hidalgo	Jefe Departamento de Auditoría	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Andrea Soto Araya	Encargada de SSI	
10	Nicol Jería O.	Encargada de Ciberseguridad	
11			
12			

Procedimiento de Privacidad y Protección de la Información de Identificación Personal
Control A.18.01.04

Tabla de Contenidos

Revisiones del Procedimiento.....2
1. Objetivo. 3
2. Alcance. 3
3. Normas y Referencias. 3
4. Términos y Definiciones. 3
5. Roles y Responsabilidades.....3
6. Privacidad y Protección de Información de Identificación Personal 4
6.1. Consideraciones Generales para la Manipulación de Información Privada.....4
6.2. Métodos de Enmascaramiento de Datos Aceptados 5
6.3. Consideraciones para la Entrega de la Información.....5
7. Modo de Operación 5
7.1 Flujo de Procedimiento para el Enmascaramiento y la Entrega de Información..6
7.2 Matriz del Procedimiento para Privacidad y Protección de Información de Identificación Personal 6
7.3 Matriz de Responsabilidades. 7
8. Registro de Operación. 8
9. Anexo.....8

ELABORADO POR	VALIDACIÓN TÉCNICA	APROBADO POR	APROBADO POR
Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC)	Gabriela Cares **Gabriela Cares** **Jefa División Estudios**	**Andrea Soto Araya** **Encargada Seguridad de la Información**	**Comité SGSIC**

REVISIONES DEL PROCEDIMIENTO			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
Cero (0)	31/10/2019	Elaboración Inicial	Todas

1. Objetivo.

El objetivo del presente procedimiento es servir como línea base para la protección de la información de carácter personal frente a posibles solicitudes asociadas al cumplimiento de la Ley de acceso a la información pública o ley de Transparencia. En función de lo anterior, se hará referencia a diferentes directrices, tareas y lineamientos relacionados con la protección de toda información de carácter individualizable, es decir, privada. Es importante destacar que, aunque este documento no indica los criterios a seguir para la aprobación de solicitudes, si indica los mínimos estándares que deben ser cumplidos referentes a la privacidad y la seguridad de la información asociadas al proceso en cuestión.

2. Alcance.

El presente procedimiento debe ser aplicado a todos los funcionarios y funcionarias, de planta, contrata, honorarios, cualquiera sea la naturaleza de su régimen contractual, y a proveedores de desarrollo de software externos a la Agencia de Calidad de la Educación, que, dado el cumplimiento de sus responsabilidades, se vean involucrados en la manipulación y/o generación de información de carácter personal.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27.002:2013, el presente documento tiene su alcance sobre el siguiente control:

- A.18.01.04 – Privacidad y Protección de la Información de Identificación Personal.

3 Normas y Referencias.

- NCh ISO 27.001:2013.
- NCh ISO 27.002:2013.
- Política de Desarrollo Seguro de Software, aprobada por Resolución Exenta N° 1547, de 2019, de la Agencia de Calidad de la Educación.

4. Términos y Definiciones.

Información de Identificación Personal	Hace referencia a cualquier tipo de información que permite la individualización de una persona, ya sea natural o jurídica. En función de lo anterior, son consideradas como información de identificación personal, elementos tales como el número de Rol Único Tributario (RUT) y otro tipo de identificadores únicos asociados a personas, entidades u organizaciones.
Privacidad de la Información	Hace referencia a la protección de la información, desde el punto de vista de proteger la identidad de la persona a la que dicha información corresponde, es decir, velando por que esta no pueda ser relacionada con un individuo en específico.
Enmascaramiento de la Información	Se refiere a los métodos utilizados para la modificación u ocultamiento de cierto tipo de información.

5. Roles y Responsabilidades.

a) **Jefatura Unidad de Tecnologías de la Información y Comunicación – TIC:** Dentro de las principales tareas llevadas a cabo por el rol en cuestión, se encuentra aquellas asociadas al cumplimiento técnico del procedimiento de protección de datos personales. Adicionalmente,

deberá promover mejoras tecnológicas asociadas a la protección de la privacidad de la información.

b) **Jefa División de Estudios:** Es la encargada de supervisar el cumplimiento de los estándares contenidos en el presente documento. Adicionalmente, debe hacer las gestiones pertinentes para que las respuestas a las solicitudes de información asociadas a la Ley N° 20.285 se encuentren debidamente resguardadas.

c) **Equipo División de Estudios:** Encargados de dar cumplimiento a los estándares, lineamientos y tareas expresadas en el presente procedimiento, asociados con los niveles mínimos de protección de la privacidad y seguridad de la información frente a posibles solicitudes por la ley de transparencia.

d) **Encargada/o de Seguridad de la Información:** Rol encargado de velar por la correcta aplicación de los lineamientos aquí establecidos. Así mismo, será este el encargado de apoyar los procesos de actualización de este documento, prestando un asesoramiento activo desde la perspectiva de la seguridad de la información.

e) **Personal de Agencia**: En función del tipo de información que es manejada y generada al interior de la organización, es responsabilidad de todos las personas que prestan servicios en la Agencia. Cualquiera sea la naturaleza de su régimen contractual de brindar la debida protección y confidencialidad a la información de tipo personal en cuestión.

6. Privacidad y Protección de Información de Identificación Personal.

En vista de la cantidad y tipo de información que es manejada por la Agencia, así como de las solicitudes recibidas en cumplimiento de la ley de transparencia, es necesario tener consideraciones asociadas a la protección de la privacidad de la información. En función de lo anterior, es necesario aclarar que el presente documento no hace referencia a los criterios que deberán ser utilizados en relación con la aprobación o el rechazo de solicitudes asociadas a dicha ley, más bien, indica los principales métodos y consideraciones que deberán ser puestos en práctica para asegurar la privacidad de la información de identificación personal tanto al atender dichas solicitudes, como en la manipulación de los activos de información asociados.

6.1. Consideraciones Generales para la Manipulación de Información Privada.

Con la finalidad de brindar la debida protección a la información de carácter privada, se deberá velar por la aplicación de las siguientes consideraciones:

a) El acceso a bases de datos que contengan información privada deberá ser controlado. Así, el propietario de dicho activo deberá supervisar que solo individuos que cuenten con los debidos permisos puedan acceder a estos.

b) Las bases de datos que contengan información de carácter privado, y que adicionalmente sean críticas para la organización, deberán ser debidamente resguardadas mediante la utilización de discos duros, los cuales serán resguardados por la Unidad TIC.

c) En caso de que se deba transmitir información de carácter privada entre las diferentes divisiones de la Agencia, se deberá realizar mediante la asistencia de herramientas de gestión de archivos en la nube, eliminando los accesos una vez que estos ya no sean requeridos. Así, y de forma adicional, cualquier tipo de transmisión de información deberá ser realizada en conformidad con lo establecido en la Política de Gestión de Activos, aprobada por Resolución Exenta N° 1527, de 2019 ,de la Agencia de Calidad de la Educación. .

6.2. Métodos de Enmascaramiento de Datos Aceptados.

Con la finalidad de garantizar que cualquier tipo de información entregada debido a solicitudes asociadas con el cumplimiento de la ley de transparencia brinde la debida protección a la información de tipo confidencial, se deberá hacer uso de métodos de enmascaramiento de la información, velando así por que los solicitantes no puedan hacer uso de la información facilitada con el objetivo de individualizar los datos contenidos en esta. Así, tanto los métodos de enmascaramiento, como la información que deberán proteger son listados a continuación:

a) MRUN: Se deberá hacer uso de este método de enmascaramiento de la información sobre los runes de los individuos contenidos en la base de datos. Lo anterior, deberá realizarse con el objetivo de que el archivo resultante no pueda ser individualizable, es decir, que los resultados o las filas de la base de datos no puedan ser relacionadas a individuos específicos.

b) MRBD: El presente método de enmascaramiento deberá ser utilizado para proteger la privacidad y el anonimato de los establecimientos educacionales contenidos en la base de datos en cuestión. En función de lo anterior, la verdadera identidad de los establecimientos no debería poder ser deducida a partir de la información contenida en la base de datos.

En relación con los métodos de enmascaramiento anteriormente señalados, es de importancia especificar que estos son utilizados de forma transversal por el Ministerio de Educación (MINEDUC) y los organismos públicos dependientes de este. Adicionalmente, es necesario aclarar que, al utilizar cualquiera de los métodos anteriormente especificados, se deberá velar por la eliminación de todo tipo de información que permita la individualización de los datos.

6.3. Consideraciones para la Entrega de la Información.

Referente a cualquier tipo de entrega de información de tipo privada a individuos ajenos a la institución debido al cumplimiento de ley de transparencia, es necesario especificar las siguientes directrices, orientadas a la protección de la información de identificación personal:

a) Toda entrega de información relacionada con el cumplimiento de la ley de transparencia deberá ser realizada mediante la utilización de herramientas de gestión de archivos en la nube. En función de lo anterior, con la finalidad de brindar la debida protección a los archivos entregados, se deberá velar por la utilización de contraseñas, así como de periodos de caducidad, con la finalidad de prevenir que individuos no autorizados tengan acceso a dicha información.

b) Dependiendo de la naturaleza de la información a ser entregada, esta deberá estar enmascarada, con la finalidad de prevenir que dicha información pueda ser individualizada. De forma adicional a la implementación de dichos métodos, se deberá velar por la eliminación de cualquier tipo de información adicional que permita la vulneración de la privacidad de la misma.

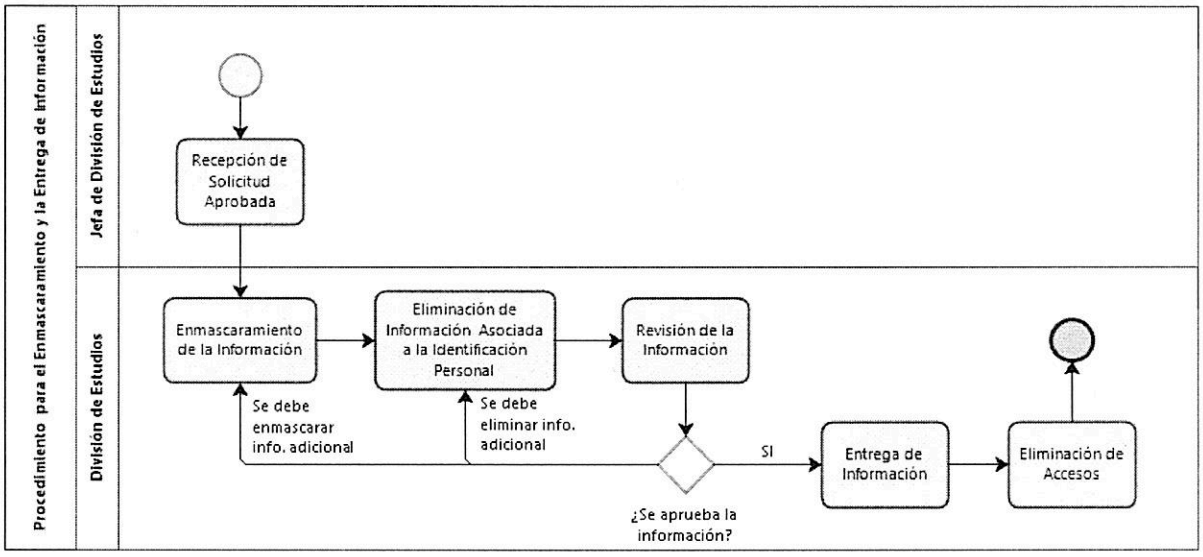
c) Cualquier tipo de entrega de información deberá ser respaldada mediante la utilización de un correo electrónico, en donde se detalle la información entregada, así como los plazos en los que estará disponible el link para acceder a la misma.

7. Modo de Operación.

A continuación, se describen los flujos procedimentales para el enmascaramiento y entrega de la información.

s

7.1 Flujo de Procedimiento para el Enmascaramiento y la Entrega de Información.



7.2 Matriz del Procedimiento para Privacidad y Protección de Información de Identificación Personal.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Recepción de solicitud aprobada	Una vez la solitud de información referente al cumplimiento de la ley de transparencia sea debidamente aprobada, esta deberá ser comunicada a la División de Estudios para ser atendida.	Jefa División de Estudios	2
2	Enmascaramiento de la información	En conformidad con las directrices establecidas en el presente documento, se deberá enmascarar todo tipo de información de identificación personal que permita la individualización del archivo a entregar. Referente a los métodos a utilizar para llevar a cabo esta tarea, se deberá hacer uso exclusivo de aquellos detallados en el presente procedimiento.	Equipo División Estudios	3

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
3	Eliminación de información asociada a la identificación personal	Se deberá eliminar cualquier tipo de información adicional que permita la vulneración de la privacidad de la misma. Así elementos como nombres, direcciones, y/o apellidos no deberán estar contenidos en el entregable final.	Equipo División Estudios	4
4	Revisión de la Información	Con la finalidad de asegurar la protección de la información de identificación personal, se deberá revisar el archivo a entregar. En virtud del resultado de dicha revisión, es posible tomar los siguientes cursos de acción: - Se debe enmascarar información adicional (2) - Se debe eliminar información adicional (3) - El archivo brinda una adecuada protección a la privacidad (5)	Equipo División Estudios	2, 3 o 5
5	Entrega de Información	La entrega de los archivos asociados al cumplimiento de la ley de transparencia deberá ser realizada en conformidad con las directrices expresadas en el presente procedimiento, velando en todo momento por la protección de dicha información.	Equipo División Estudios	6
6	Eliminación de Accesos	Una vez pase el periodo de disponibilidad establecido, se deberá revisar el link asociado, con la finalidad de verificar que este se encuentra eliminado. En caso contrario, se deberá eliminar dicho acceso.	Equipo División Estudios	FIN

7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

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

De esta forma, la matriz de responsabilidades para el presente procedimiento se estructura de la siguiente manera:

ID	ACTIVIDAD	Jefa División Estudios	Equipo Div. Estudios	Encargado Seguridad
1	**Recepción de solicitud aprobada**	R / E / A	I	I
2	**Enmascaramiento de la información**	A / I	R / E	C
3	**Eliminación de información asociada a la identificación personal**	A / I	R / E	C
4	**Revisión de la información**	A / I	R / E	C
5	**Entrega de información**	A / I	R / E	C / I
6	**Eliminación de accesos**	A / I	R / E	C / I

8. Registro de Operación.

REGISTRO	ID	RESPONSABLE/DUEÑO DEL REGISTRO	TIEMPO RETENCIÓN	SOPORTE	LUGAR
Base de datos enmascaradas entregadas	-	Jefa División de Estudios	1 año / Google Drive	Digital	Google Drive

9. Anexo.

Se adjunta lista de asistencia Comité de Seguridad de Información.

LISTA DE ASISTENCIA
Comité de Seguridad de la Información
Implementación PMG- Sistema de Seguridad de la Información

I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Política de Revisión Independiente del Sistema de Gestión de Seguridad de Información y Ciberseguridad (Control A.5.1.2, A.18.2.1, A.18.2.2 y A.18.2.3)
2. Procedimiento de Segregación de Funciones (Control A. 6.1.2)
3. Política para Transferencia y Manejo de Información (A. 8.2.2, A.8.2.3, A.8.3.2, A.13.2.1 y A.13.2.3)
4. Procedimiento de Controles y Perímetro de Seguridad Física (Control A.11.1.2 y A.11.1.4)
5. Procedimiento para Documentación de los Procedimientos Operacionales (control A.12.1.1 y A.18.1.3)
6. Política de Protección Contra Código Malicioso (Control A.12.02.01, A.12.5.1 y A.12.6.2)
7. Procedimiento de Gestión de Vulnerabilidades Técnicas (A.12.6.1)
8. Política de Controles de Red (control .13.1.1 y A.13.1.2)
9. Política de Seguridad de la Información para los Proveedores (A.15,1,1 y A.15.2.1)
10. Política de Planificación de la Continuidad Operacional (control A.17.1.1, A.17.1.2 y A.17.1.3)
11. listado de legislación vigente (A.18.1.1)
12. Procedimiento de Privacidad y Protección de la Información de Identificación Personal (Control A.18.01.04)

Fecha: 5 de diciembre de 2019

N°	Nombre	Cargo	Firma
1	Daniel Rodríguez Morales	Secretario Ejecutivo	
2	Gino Cortez B.	Jefe de DEOD	
3	Cristóbal Alarcón B.	Jefe de DIAC	
4	Juan Bravo M.	Jefe DELA	
5	Gabriela Cares	Jefa de DIEST	
6	Ana María Concha	Jefe DAG	
7	Sergio Hidalgo	Jefe Departamento de Auditoría	
8	Gabriel Cáceres	Encargado de Unidad de Planificación (s)	
9	Andrea Soto Araya	Encargada de SSI	
10	Nicol Jeria O.	Encargada de Ciberseguridad	
11			
12			

1