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

APRUEBA ACTUALIZACIÓN Y CREACIÓN DE LOS MANUALES Y PROCEDIMIENTOS ASOCIADOS AL PRINCIPIO DE CONTROL DE ACCESO FÍSICO Y LÓGICO

RESOLUCIÓN EXENTA Nº 586

SANTIAGO, 28 SEP 2021

VISTOS:

Lo dispuesto en el DFL N° 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N°19.880, que establece las Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado; en la Ley N°20.529, sobre Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización; en la Ley N°20.285, sobre Acceso a la Información Pública; en la Ley N°19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firmas; en la Ley N°19.628, sobre Protección a la Vida Privada; en el Decreto Supremo N°83, de 2005, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en la norma chilena NCh-ISO 27001; en las Resoluciones Exenta N°s 1025, 1027, 1527, 1611 y 1616; de 2019, de la Agencia de la Calidad de la Educación; en los Memorándum N°58 y N°83, de 2019, del Secretario Ejecutivo; en la Resolución Exenta N°583, de 2021, que aprueba la actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación; en la Resolución Exenta N°584, de 2021, que aprueba la Política de Protección de Datos Personales; en la Resolución Exenta N°585, de 2021, que aprueba la actualización del Procedimiento de Respuesta ante Incidentes de la Agencia de Calidad de la Educación; en la Resolución Exenta N°218, de 2021 que aprueba medidas y procedimientos de datos personales; en la Resolución Nº7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del Trámite de Toma de Razón, y

CONSIDERANDO:

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

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

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

Que, en este sentido, dentro de las regulaciones que se dejan sin efecto, se encuentran: Resolución Exenta N°1025, de 14 de agosto de 2019, del Servicio, se aprobó la Política sobre Escritorio y Pantallas Limpios de la Agencia de Calidad de la Educación; Resolución Exenta N°1027, de 14 de agosto de 2019, del Servicio, se aprobó la Política sobre Control

de Acceso Físico y Lógico de la Agencia de Calidad de la Educación; Resolución Exenta N°1527, de 02 de diciembre de 2019, se aprobó la Política de Gestión de Activos; Resolución Exenta N°1611, de 13 de diciembre de 2019, se aprobó la Política para Transferencia y Manejo de Información; y Resolución Exenta N°1616, de 13 de diciembre de 2019, del Servicio, se aprobó la Política de Protección contra Código Malicioso de la Agencia de Calidad de la Educación.

Que, teniendo en cuenta lo expuesto, corresponde aprobar el presente acto, por medio de cual se aprueba las distintas materias asociadas al principio de control de acceso físico y logístico, dejando sin efecto las regulaciones vigentes.

RESUELVO:

PRIMERO: **APRUEBASE,** el Manual de Seguridad Física de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Entregar las directrices para la disposición de controles que resguarden los activos de información de la Agencia, de aquellas amenazas de índole física.

2. ALCANCE

Este manual aplica para las instalaciones de Agencia del nivel central y aquellas Macrozonas y oficinas regionales que se encuentren habilitadas.

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

a) ISO/IEC 27.001:2013, Control A.11.01.01 – Perímetro de Seguridad Física.

b) ISO/IEC 27.001:2013, Control A.11.01.02 – Controles de Acceso Físicos.

c) ISO/IEC 27.001:2013, Control A.11.01.03 – Seguridad de oficinas, salas e instalaciones.

d) ISO/IEC 27.001:2013, Control A.11.01.04 – Protección contra amenazas externas y del medioambiente.

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.3 relativo al principio de control de acceso físico y lógico.

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

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

4. TÉRMINOS Y DEFINICIONES

Los términos y definiciones que aplican a este y todos los documentos del SSI de la Agencia se encuentran en el Anexo I de la Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política

General de Seguridad de la Información de la Agencia de Calidad de la Educación. (SSI-POL-01).

5. ROLES Y RESPONSABILIDADES

a) **Jefatura DAG:** Responsable de velar por la correcta ejecución de los dispuesto en este manual.

b) **Jefatura de Departamento de Servicios Generales – DAG:** ejecutar las directrices entregadas en este manual, así como de gestionar lo necesario para que se cumpla su objetivo. También será el encargado de gestionar con la Administración de los Edificios en donde se encuentren oficinas y/o instalaciones críticas de procesamiento de información de la Agencia, la correcta implementación de las medidas que en este contexto se definen en este documento.

c) **Jefatura de Unidad de Tecnología – DAG:** ejecutar la correcta implementación de los controles de seguridad física en las instalaciones relacionadas con la operación de las Unidades que estén definidas en este documento.

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

e) **Jefaturas de División y Encargados de Macrozona:** como propietarios de los activos que se almacenan y procesan en las instalaciones de la Agencia, deben validar que los controles de seguridad física estén bien implementados, así como generar los requerimientos para su implementación o mejora.

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

- R: Responsable.
- E: Ejecutor.
- C: consultado.
- I: Informado.

ROL	JEFATURA DAG	JEFATURA DIVISIÓN / MACROZONAS	DPTO. SERVICIOS GENERALES- DAG	JEFATURA TIC - DAG	ENC. SI / CIBERSEGURIDAD
RESPONSABLE	X				
EJECUTOR		X	X	X	
CONSULTADO					X
INFORMADO		X			

6. LINEAMIENTOS DEL MANUAL

En función de lo definido por el principio de control de acceso físico de la Política General de Seguridad de Información (SSI-POL-01)[1], la Agencia declara las siguientes instalaciones críticas de procesamiento de información:

a) Edificios o Direcciones Físicas:

   i. Edificio Morandé 360, pisos 9 y 10, Santiago Centro, Chile.
   ii. Edificio Amunátegui 232, pisos 2 y 4, Santiago Centro, Chile.
   iii. Edificios o direcciones físicas de Macrozonas.

b) Oficinas e Instalaciones Internas de Nivel Central:

   i. Centro de Datos o Data Center, Unidad TIC – Edificio Morandé 360, Santiago de Chile.
   ii. Bodega de la Unidad de TIC – Edificio Morandé 360, Santiago de Chile.
   iii. Oficinas de la Unidad de TIC - Edificio Morandé 360, Santiago de Chile.
   iv. Accesos generales a los pisos 9 y 10 del Edificio Morandé 360, Santiago de Chile
   v. Oficinas de la División de Evaluación de Logros de Aprendizaje (DELA), considerando sus dos puertas de acceso.

Sobre estas instalaciones, se deberán aplicar las directrices definidas en los siguientes puntos de este documento, de forma de mitigar los riesgos asociados a la seguridad física de los activos de información de la Agencia.

6.1. Controles de Acceso Físico a las Instalaciones

Se deben implementar medidas de control para regular y controlar el ingreso y egreso de personas a las instalaciones críticas de procesamiento de información de la Agencia. Estas medidas están orientadas a validar de la forma más automática posible, el acceso tanto del personal de la Agencia como de personas ajenas a la institución. Para lo anterior, la Agencia deberá disponer de los siguientes mecanismos de control de acceso físico:

a) **Control de acceso físico a oficinas e instalaciones internas:** la Agencia deberá disponer un sistema de recepción de visitas en los pisos donde se encuentren sus oficinas, donde éstas deberán registrar:

   i. Nombre y apellido.

   ii. Motivo de la visita.

   iii. Persona de la Agencia que recibe la visita.

   iv. Hora de entrada y salida de la visita.

En complemento, para las oficinas e instalaciones internas definidas como críticas, las puertas de acceso deben contar con cierre magnético que autorice el acceso a usuarios autenticados mediante lectura de huella dactilar, las cuales deben permanecer cerradas y ser abiertas sólo al momento de autorizar el acceso de personas a éstas.

Adicionalmente, la Agencia deberá alinearse a los mecanismos de control de acceso físicos dispuestos por cada administración de los edificios en donde se ubiquen las instalaciones críticas de procesamiento de información, los cuales pueden incluir como mínimo, la identificación de las personas que ingresan a las instalaciones.

---

[1] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra b) sobre el principio específico de control de acceso en su dimensión física.

b) **Protección contra amenazas físicas y del medio ambiente:** Adicional a lo anterior, se establece un plan de protección contra amenazas que puedan ser de origen ambiental o industrial

   i. **Sensores de humo:** si bien este mecanismo es necesario para la protección de los activos de la Agencia, su gestión puede depender de la institución, así como de la Administración de los Edificios.

   ii. **Extintores:** se define que los tipos de extintores deben ser con dióxido de carbono (CO2) para las áreas de la Unidad de TIC y Data Center, y de polvo químico para el resto de las instalaciones.

   iii. **Red húmeda:** todos los pisos en los cuales se ubiquen oficinas e instalaciones de la agencia deben contar con mangueras de red húmeda en buen estado.

   iv. **Condiciones de temperatura especiales:** es obligatorio para el Data Center y para cualquier instalación u oficina que albergue equipamiento tecnológico con activos de información críticos, ya que la no regulación de la temperatura ambiente de estas zonas se traduce en riesgos de indisponibilidad por altas temperaturas o por daños ambientales en ésta. Se deben mantener los niveles de temperatura y humedad descritos por el fabricante de la infraestructura tecnológica que se ubique en el Data Center u otras instalaciones.

c) **Contratación de seguros:** para complementar los mecanismos preventivos, la Agencia puede implementar mecanismos mitigatorios, como contratos de seguro para todos los bienes de la Agencia a nivel nacional, por ejemplo, para casos de sismo, incendio, robo, y escenarios de riesgo similares. Estos seguros deben ser definidos y contratados de forma anual por la Agencia.

6.2. Mantención de mecanismos de control físicos

A continuación, se listan los mecanismos de control para amenazas externas y de medioambiente, junto con su respectivo detalle asociado a la mantención para su correcto funcionamiento:

CONTROL	MANTENIMIENTO
Extintores	Se realiza mantención anual planificada en función de las últimas mantenciones de cada extintor.
Huellero biométrico	La mantención se efectúa en función de los desperfectos que presenten los aparatos que conforman el control.
Edificios y direcciones físicas de la Agencia en Nivel Central y Macrozonas	Responsabilidad de la Administración del Edificio.
Sensores de Humo	Mantención cada tres (3) meses a cargo de la Administración del Edificio Morandé 360.
Aire acondicionado	La mantención contempla todos los aires acondicionados de las instalaciones de la Agencia, y se realiza un plan anual de mantención en conjunto con el proveedor considerando mantenciones al menos anuales por cada equipo de aire acondicionado.

Mangueras de red húmeda	Responsabilidad de la Administración del Edificio.

7. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-4.1—Aprobación de pólizas de seguro
MANUAL / PROCEDIMIENTO	Seguridad Física
CONTROLES ISO 27.001	
RESPONSABLE	Encargado de Administración Interna - DAG
DESCRIPCIÓN	Corresponde a la Resolución Exenta que formaliza la contratación de seguros en el contexto de la protección contra amenazas físicas y del ambiente para la Agencia.
FRECUENCIA	Anual
ALMACENAMIENTO	Digital - Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-4.1—Plan Anual de Mantención de Aire Acondicionado
MANUAL / PROCEDIMIENTO	Seguridad Física
CONTROLES ISO 27.001	• A.11.01.03 – Seguridad de oficinas, salas e instalaciones. • A.11.01.04 – Protección contra amenazas externas y del medioambiente
RESPONSABLE	Encargado de Administración Interna - DAG
DESCRIPCIÓN	Corresponde al plan anual de mantención de aire acondicionado.
FRECUENCIA	En función de lo dispuesto en el plan anual de mantención de aire acondicionado.
ALMACENAMIENTO	Digital - Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-4.1—Plan de mantención para controles específicos
MANUAL / PROCEDIMIENTO	Seguridad Física
CONTROLES ISO 27.001	• A.11.01.01 – Perímetro de Seguridad Física. • A.11.01.02 – Controles de Acceso Físicos.
RESPONSABLE	Encargado de Administración Interna - DAG
DESCRIPCIÓN	Corresponde al plan anual de mantención de controles específicos.

FRECUENCIA	En función de lo dispuesto en el plan anual de mantención de controles específicos
ALMACENAMIENTO	Digital - Google Drive del responsable

8. NO CONFORMIDADES E INCUMPLIMIENTOS

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

Así mismo, cualquier evento o incidente de seguridad de la información, deberá ser canalizado según lo estipulado en el Procedimiento de Respuesta ante Incidentes de Seguridad (SSI-PRO-5.1)[2].

SEGUNDO: APRUEBASE, el Procedimiento de Gestión de Cuentas y Accesos de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios de la Agencia de Calidad de la Educación.

2. ALCANCE

Este procedimiento es aplicable para la administración general de todas las cuentas de usuario de la Agencia, incluidos el controlador de dominio, sistemas y software.
En relación con la norma ISO/IEC 27.001:2013, este procedimiento considera dentro de su alcance los siguientes controles:

a) ISO/IEC 27.001:2013, Control A.09.01.02 – Acceso a redes y servicios de red.

b) ISO/IEC 27.001:2013, Control A.09.02.01 – Registro y cancelación de registro de usuario.

c) ISO/IEC 27.001:2013, Control A.09.02.02 – Entrega de acceso a los usuarios.

d) ISO/IEC 27.001:2013, Control A.09.02.03 – Administración de derechos de acceso privilegiados.

e) ISO/IEC 27.001:2013, Control A.09.02.04 – Administración de la información de autenticación secreta de los usuarios.

f) ISO/IEC 27.001:2013, Control A.09.02.05 – Revisión de los derechos de acceso de los usuarios.

g) ISO/IEC 27.001:2013, Control A.09.02.06 – eliminación o ajuste de los derechos de acceso

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.3 relativo al principio de control de acceso físico y lógico.

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

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

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

4. TÉRMINOS Y DEFINICIONES

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

5. ROLES Y RESPONSABILIDADES

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

6. LINEAMIENTOS DEL PROCEDIMIENTO

Para la incorporación de la seguridad en la gestión de cuentas de usuario y contraseñas, se deben considerar dos contextos:

a) **Alta general de usuarios:** corresponde al flujo procedimental para el ingreso de nuevos funcionarios y funcionarias y colaboradores a la Agencia con un vínculo contractual de cualquier naturaleza, y en donde la Unidad de TIC debe proporcionar los siguientes accesos base según el tipo de usuario:

i. Accesos y privilegios estándar:

- Acceso al dominio de la organización con mínimos privilegios, donde el usuario será agregado al grupo de usuarios del controlador de dominio dependiendo de la División de la cual dependa el perfil de cargo.
- Anexo telefónico.
- Cuenta de correo electrónico, donde en caso de corresponder, se incluirá la cuenta de correo en grupos o listas de difusión asociadas al perfil de cargo del nuevo usuario.
- Acceso a impresoras con privilegios de impresión en blanco y negro o color según corresponda.
- Acceso a redes WiFi correspondientes a su perfil de cargo.
- Hacer entrega de los recursos y equipamiento respectivos para el desempeño de las funciones según su perfil de cargo, siguiendo los principios establecidos en la Política General de Seguridad de Información sobre la asignación de recursos (SSI-POL-01)[3].
-

ii. Accesos y privilegios de administrador:

- Acceso al dominio de la institución con perfil administrador, donde el usuario será agregado al grupo de usuarios del controlador de dominio dependiendo de la División de la cual dependa el perfil de cargo.
- Acceso a sistemas o software específicos con privilegios de administración.
- Anexo telefónico.

[3] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra b), punto ii) sobre la asignación de recursos.

- Cuenta de correo electrónico, donde en caso de corresponder, se incluirá la cuenta de correo en grupos o listas de difusión asociadas al perfil de cargo del nuevo usuario.
- Acceso a impresoras con privilegios de impresión en blanco y negro o color según corresponda.
- Acceso a redes WiFi especiales o genéricas según corresponda a su perfil de cargo.
- Hacer entrega de los recursos y equipamiento respectivos para el desempeño de las funciones según su perfil de cargo, siguiendo los principios establecidos en la Política General de Seguridad de Información sobre la asignación de recursos (SSI-POL-01)[4].

iii. Para comenzar el proceso de creación de usuarios, la Unidad de TIC – DAG, debe contar con la siguiente información, provista por el Departamento de Gestión de Personas (GDP) - DAG:

- Nombre completo y rut de la persona que ingresa.
- Rol y perfil de cargo con el que ingresa.
- Jefatura directa.
- Tipo de usuario (interno / externo)
- Fecha de alta de usuario.
- Fecha de caducidad de la cuenta de usuario (sólo si aplica).

b) **Alta de usuarios en sistemas Divisionales:** corresponde al flujo procedimental en el cual cada División, a través de las Jefaturas de Departamento o Unidad, dan acceso a los usuarios nuevos o antiguos, a los sistemas que son administrados internamente en el contexto del alta y baja de usuarios.

6.1. Lineamientos generales para gestión de cuentas y accesos

Así mismo, de forma general e independiente de los contextos descritos anteriormente, se deben considerar los siguientes lineamientos para la gestión de cuentas de usuario:

a) Para la creación de identificadores únicos de usuarios, se deben seguir los principios establecidos en la Política General de Seguridad de Información referentes al control de acceso lógico (SSI-POL-01)[5].
b) Los ID de usuarios que dejan la organización deben deshabilitarse de inmediato, y cuando sea posible se debe automatizar la caducidad de una cuenta de usuario.
c) Evitar la generación de usuarios redundantes.
d) Verificar que el nivel de accesos y privilegios otorgados se condice con las definiciones establecidas por el dueño funcional del sistema, según los principios establecidos en la Política General de Seguridad de Información referentes al control de acceso lógico (SSI-POL-01) [6].
e) Validar que los accesos y privilegios no se activan hasta terminado el proceso de alta de usuarios y autorización de los propietarios o custodios de los activos de información.
f) Revisar periódicamente los accesos y privilegios concedidos.
g) La asignación de derechos de acceso privilegiados asociados a cada sistema o software debe ser controlada a través de un proceso formal que deje registro

[4] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra b), punto ii) sobre la asignación de recursos.
[5] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra a), punto ii) sobre la gestión de accesos y privilegios en los sistemas.
[6] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra a), punto ii) sobre la gestión de accesos y privilegios en los sistemas.

de su operación. Para el caso de los sistemas administrados por la Unidad de TIC, el registro de alta, baja y modificación de usuarios corresponde a los tickets de mesa de ayuda respectivos, mientras que para los sistemas cuyos dueños funcionales son las Divisiones, debe generarse un registro como el que se muestra en el Anexo I de este documento.

h) Los derechos de acceso deberán asignarse en base al mínimo privilegio, según los principios establecidos en la Política General de Seguridad de Información referentes al control de acceso lógico (SSI-POL-01) [7].

i) La asignación de accesos y privilegios deberá ser revisada de manera periódica como mínimo trimestralmente por los dueños funcionales de los sistemas de manera de evitar la generación de accesos caducos que se encuentren activos.

7. MODO DE OPERACIÓN

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

a) Procedimiento de alta de usuarios.

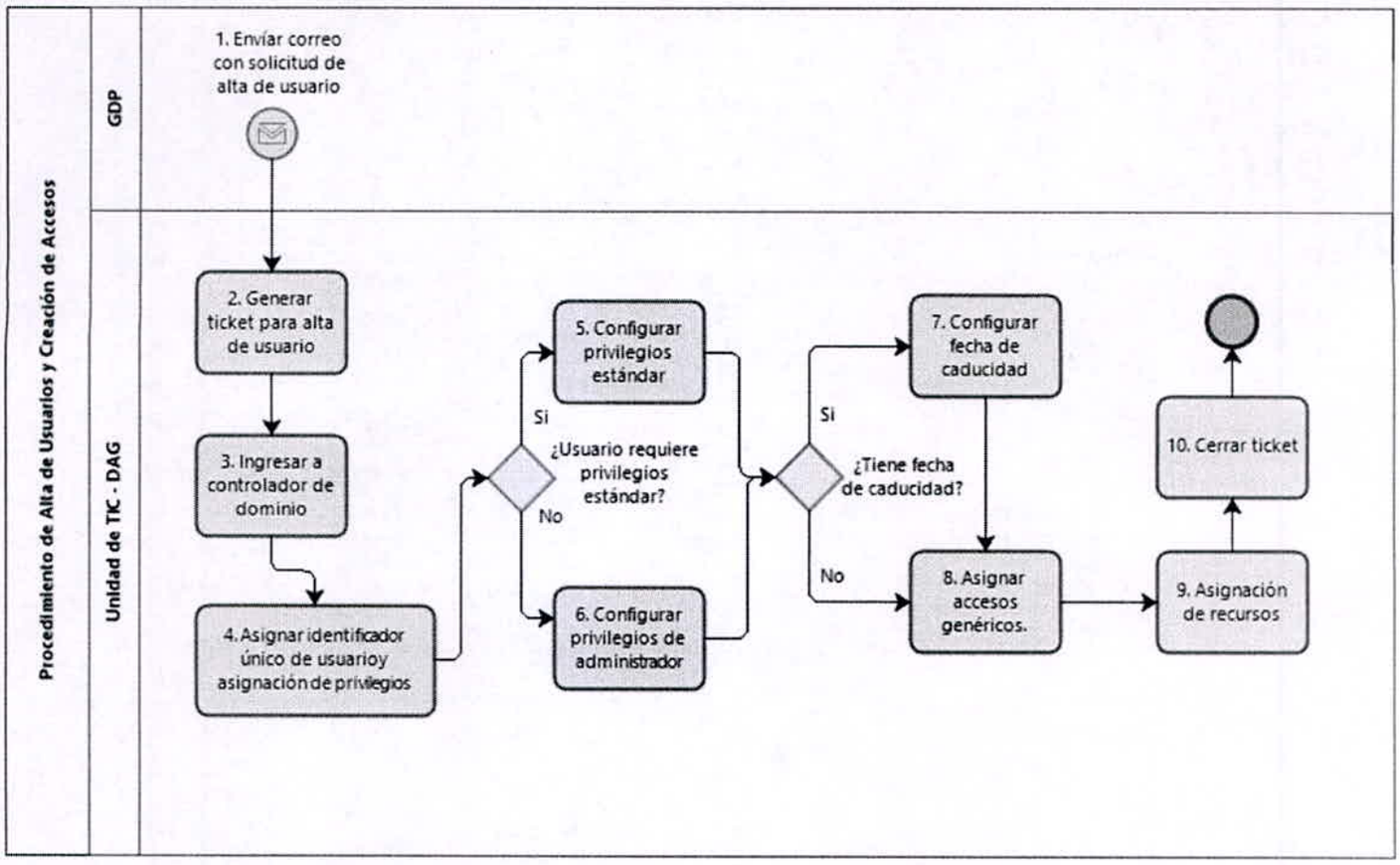
b) Procedimiento de entrega de acceso a sistemas divisionales.

c) Procedimiento de baja o modificación de usuarios.

d) Procedimiento de revisión de usuarios y accesos.

[7] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra a), punto ii) sobre la gestión de accesos y privilegios en los sistemas.

7.1. Flujo de Procedimiento para alta de usuarios

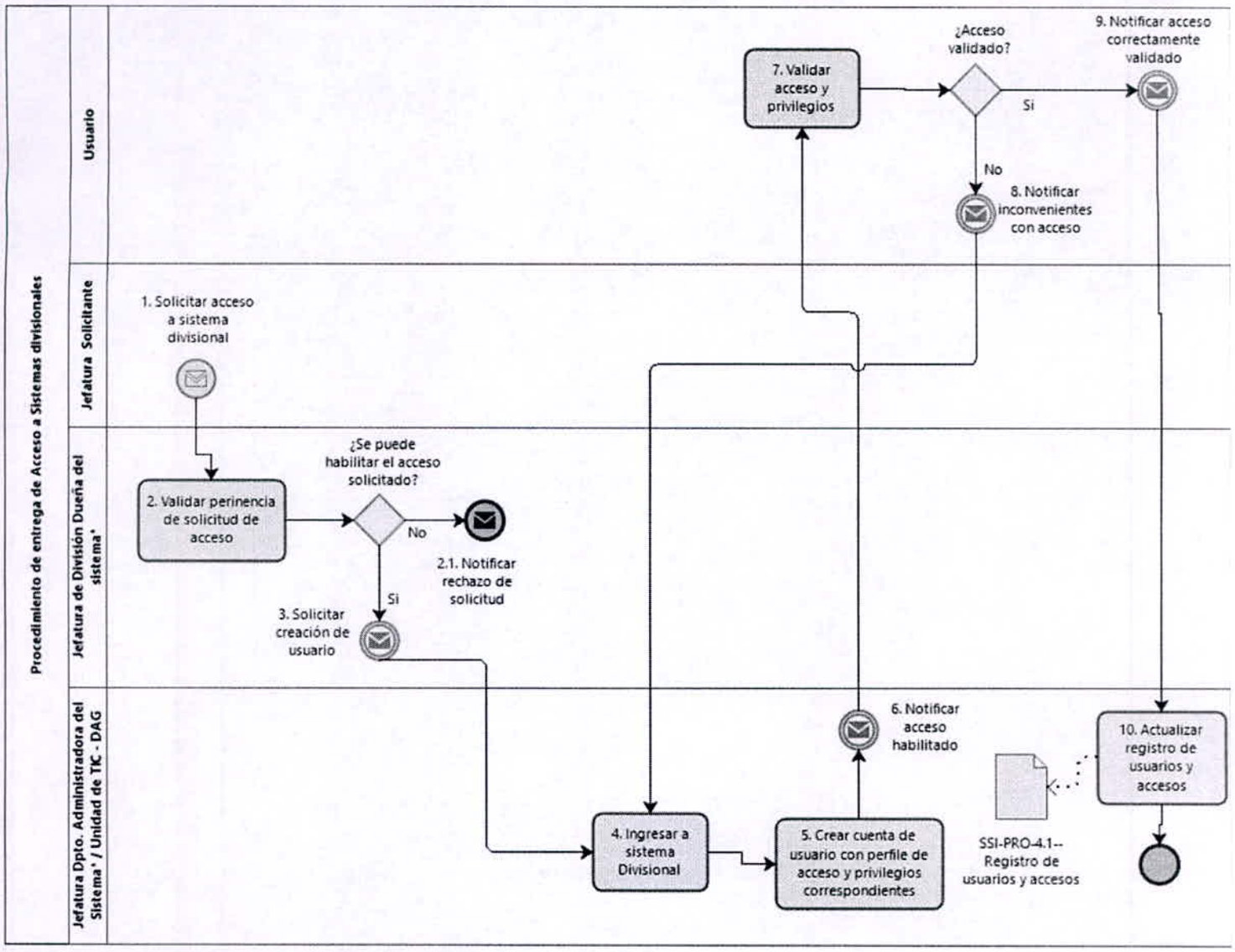


7.2. Matriz de Procedimiento para alta de usuarios

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Enviar correo con solicitud de alta de usuario.	Una vez concluido el proceso de selección o reclutamiento, se debe enviar un correo con la información de la persona que se integra a la agencia según lo dispuesto en este documento.	Departamento de Gestión de Personas.	2
2	Generar ticket para alta de usuario	Se debe crear un ticket en el sistema de mesa de ayuda para dar seguimiento al proceso de alta de usuario.	Equipo de Soporte e Infraestructura	3
3	Ingresar a controlador de dominio	Se debe ingresar al controlador de dominio para crear el usuario en el dominio de la Agencia.	Equipo de Soporte e Infraestructura	4
4	Asignar identificador único de usuario y asignación de privilegios	Se debe asignar al nuevo usuario un identificador único según los lineamientos de este procedimiento. Al momento de asignar los privilegios, se pueden dar los siguientes escenarios: - El usuario requiere privilegios estándar (5). - El usuario requiere privilegios de administrador (6).	Equipo de Soporte e Infraestructura	5 o 6

5	Configurar privilegios estándar	Se deben configurar los privilegios estándar para el usuario en el controlador de dominio. Se pueden dar los siguientes escenarios: - La cuenta de usuario tiene fecha de caducidad (7). - La cuenta de usuario no tiene fecha de caducidad (8).	Equipo de Soporte e Infraestructura	7 u 8
6	Configurar privilegios de administrador	Se deben configurar los privilegios estándar para el usuario en el controlador de dominio. Se pueden dar los siguientes escenarios: - La cuenta de usuario tiene fecha de caducidad (7). - La cuenta de usuario no tiene fecha de caducidad (8).	Equipo de Soporte e Infraestructura	7 u 8
7	Configurar fecha de caducidad	Se debe configurar la fecha de caducidad e la cuenta de usuario según corresponda.	Equipo de Soporte e Infraestructura	8
8	Asignar accesos genéricos	Una vez creado el usuario en el controlador de dominio, se debe otorgar todos los demás accesos genéricos	Equipo de Soporte e Infraestructura	9
9	Asignación de recursos	Se debe preparar y hacer entrega del equipamiento y recursos siguiendo los lineamientos establecidos en este documento.	Equipo de Soporte e Infraestructura	10
10	Cierre de Ticket	Se debe dar por cerrado el ticket de alta de usuario.	Equipo de Soporte e Infraestructura	FIN

7.3. Flujo de Procedimiento para entrega de acceso a sistemas divisionales



(*) Resolución Exenta N°583 de 2021 de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.3.1), sobre los roles y responsabilidades en el SSI.

Powered by bizagi Modeler

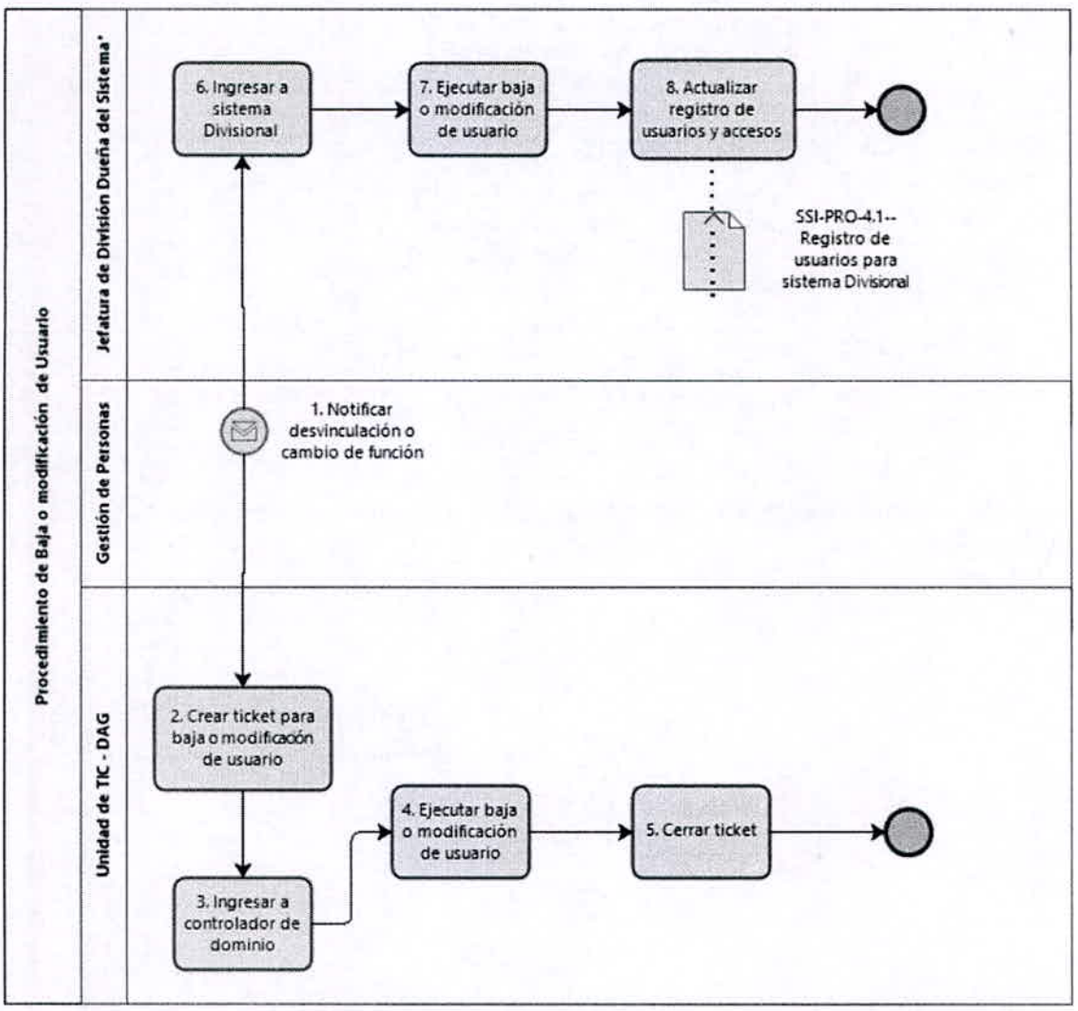
7.4. Matriz de Procedimiento para entrega de acceso a sistemas divisionales

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Solicitar acceso a sistema divisional	La Jefatura de División o Departamento (en sus roles de propietarios y custodios de los activos	Jefatura Solicitante	2

		de información[8]) del usuario que requiere el acceso, debe enviar una solicitud al dueño funcional del mismo.		
2	Validar pertinencia de solicitud	Se debe validar la pertinencia y aplicabilidad de la solicitud en función de la criticidad de los activos involucrados y el perfil del cargo del solicitante, considerando los lineamientos de este documento. Se pueden dar los siguientes escenarios: - La solicitud es rechazada (3). - La solicitud es aceptada (4).	Jefatura de División Dueña del Sistema	2.1 o 3
2.1	Notificar rechazo de la solicitud	Se debe notificar a la Jefatura Solicitante y al Usuario el rechazo de la solicitud y los motivos.	Jefatura de División Dueña del Sistema	FIN
3	Solicitar creación de usuario	Se debe solicitar al Administrador del Sistema Divisional que cree el usuario con los privilegios y accesos solicitados.	Jefatura de División Dueña del Sistema	4
4	Ingresar al sistema divisional	Se debe ingresar al sistema divisional para configurar el usuario y otorgar los accesos solicitados.	Jefatura Dpto. Administradora del Sistema / Unidad de TIC - DAG	5
5	Crear cuenta de usuario con perfil de acceso y privilegios correspondientes	Se debe crear el usuario y asignar los accesos según los lineamientos establecidos en este documento.	Jefatura Dpto. Administradora del Sistema / Unidad de TIC - DAG	6
6	Notificar acceso habilitado	Una vez creado el usuario y otorgado el acceso y privilegios se debe notificar al usuario para que los valide.	Jefatura Dpto. Administradora del Sistema / Unidad de TIC - DAG	7
7	Validar accesos y privilegios	Se debe validar que los accesos y privilegios coinciden con lo solicitado. Se pueden dar los siguientes escenarios: - El acceso es validado por el usuario (9). - El acceso no cumple con lo solicitado (8).	Usuario	8 o 9
8	Notificar inconvenientes con el acceso	Se debe notificar el dueño funcional del sistema que hay inconvenientes con el acceso solicitado.	Usuario	4
9	Notificar acceso correctamente validado	Se debe notificar que el acceso cumple con lo requerido.	Usuario	10
10	Actualizar registro de usuarios y accesos	Se debe actualizar el registro de usuarios y accesos para el sistema divisional respectivo.	Jefatura Dpto. Administradora del Sistema / Unidad de TIC - DAG	FIN

[8] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.3.1), sobre los roles y responsabilidades en el SSI.

7.5. Flujo de Procedimiento para baja o modificación de usuarios



(*) Resolución Exenta N°583 de 2021 de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.3.1), sobre los roles y responsabilidades en el SSI.

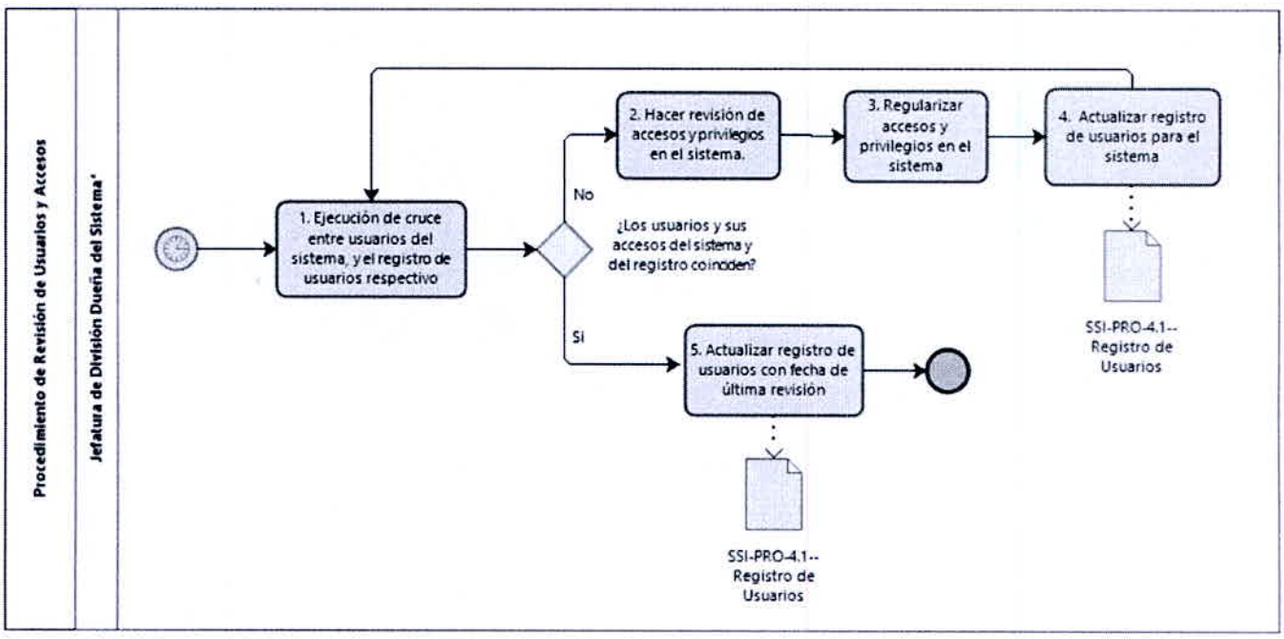
Powered by bizagi Modeler

7.6. Matriz de Procedimiento para baja o modificación de usuarios

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Notificar desvinculación o cambio de función	El proceso se gatilla con una notificación formal que indique una desvinculación o cambio de función de un usuario, que requiera dar de baja su usuario o modificar los accesos y privilegios de este respectivamente.	Departamento de Gestión de Personas	2 y 6
2	Crear ticket para baja o modificación de usuario	Se debe crear un ticket en el sistema de mesa de ayuda para dar seguimiento al proceso de baja o modificación de usuario.	Unidad de TIC – DAG	3
3	Ingresar a controlador de dominio	Se debe ingresar al controlador de dominio para dar de baja o modificar el usuario en el dominio de la Agencia.	Unidad de TIC – DAG	4

4	Ejecutar baja o modificación de usuario	En el controlador de dominio, se debe dar de baja el usuario o modificar sus privilegios de acceso según el cambio en las funciones de este.	Unidad de TIC – DAG	5
5	Cerrar ticket	Una vez dado de baja o modificado el usuario según las indicaciones, se debe dar por cerrado el ticket, dejando registro así del procedimiento.	Unidad de TIC – DAG	FIN
6	Ingresar a sistema divisional	Se debe ingresar a el sistema divisional para dar de baja el usuario o cambiar sus accesos y privilegios.	Jefatura de División Dueña del Sistema	7
7	Ejecutar baja o modificación de usuario	Se deben ejecutar los cambios o la baja del usuario en el sistema divisional.	Jefatura de División Dueña del Sistema	8 o 9
8	Actualizar el registro de usuarios y accesos del sistema divisional	Se debe actualizar la baja o cambio de privilegios del usuario en el sistema divisional.	Jefatura de División Dueña del Sistema	FIN

7.7. Flujo de Procedimiento para revisión de usuarios y accesos



(*) Resolución Exenta N°583 de 2021 de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.3.1), sobre los roles y responsabilidades en el SSI.

Powered by bizagi Modeler

7.8. Matriz de Procedimiento para revisión de usuarios y accesos

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	ID ACTIVIDAD SIGUIENTE
1	Ejecución de cruce entre usuarios del sistema y el registro de usuarios respectivo	En función de la periodicidad definida para la revisión de los accesos y usuarios del sistema, se debe hacer una revisión para validar que los usuarios y accesos correspondan con el registro que se lleva de éstos. Se pueden dar los siguientes escenarios: - Los usuarios del sistema y el registro no coinciden (2). - Los usuarios del sistema y del registro coinciden (5).	Jefatura de División Dueña del Sistema	2 o 5
2	Hacer revisión de accesos y privilegios en el sistema	Se debe cruzar la información referente a las altas, bajas y modificaciones de cuentas de usuario en el sistema para regularizar el registro y/o los usuarios del sistema.	Jefatura de División Dueña del Sistema	3
3	Regularizar usuarios y accesos en sistema	Se deben dar de baja o modificar los usuarios que sean necesarios para que coincida con los usuarios activos del sistema.	Jefatura de División Dueña del Sistema	4
4	Actualizar registro de usuarios para el sistema	Una vez regularizados los usuarios en el sistema, se debe regularizar el registro de este. Para el caso de sistemas administrados por la unidad de TIC, se debe actualizar el sistema de tickets. Para el caso de sistemas administrados por las Divisiones se debe actualizar el Registro de usuarios para sistema divisional.	Jefatura de División Dueña del Sistema	1
5	Actualizar registro de usuarios con fecha de última revisión	Se debe actualizar el registro de usuarios con la última fecha de revisión. Para el caso de sistemas administrados por la unidad de TIC, se debe actualizar el sistema de tickets. Para el caso de sistemas administrados por las Divisiones se debe actualizar el Registro de usuarios para sistema divisional.	Jefatura de División Dueña del Sistema	FIN

7.9. Matriz de Responsabilidades

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

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

De esta forma, la matriz de responsabilidades para el procedimiento de alta de usuarios se distribuye de la siguiente forma:

ID	ACTIVIDAD	JEFATURA DAG	GDP	UNIDAD TIC - DAG	ENC. SI / CIBER.
1	Enviar correo con solicitud de alta de usuario	I	R	I	I
2	Generar ticket para alta de usuario	I	I	R/E	-

3	Ingresar a controlador de dominio	R	-	E	-
4	Asignar identificador único de usuario y asignación de privilegios	R	C	E	C
5	Configurar privilegios estándar	R	-	E	C
6	Configurar privilegios de administrador	R	-	E	C
7	Configurar fecha de caducidad	R	C	E	C
8	Asignar accesos genéricos	R	-	E	C
9	Asignación de recursos	R	C	E	C
10	Cierre de ticket	R	I	E	I

Adicionalmente, la matriz de responsabilidades para el procedimiento de entrega de acceso a sistemas divisionales se distribuye de la siguiente manera:

ID	ACTIVIDAD	JEFATURA SOLICITA	USUARIO	JEFATURA DIVISIÓN DUEÑA SISTEMA	JEFATURA DPTO. ADMIN. SISTEMA	UNIDAD TIC - DAG	ENC. SI / LÍDER SSI
1	Solicitar acceso a sistema divisional	R/E	I	I	I	-	I
2	Validar pertinencia de solicitud	C	-	R	C	C	C
2.1	Notificar rechazo de la solicitud	I	I	R	-	-	-
3	Solicitar creación de usuario	I	I	R	I	I	I
4	Ingresar al sistema divisional	-	-	-	R/E	R/E	-
5	Crear cuenta de usuario con perfil de acceso y privilegios correspondientes	C	-	-	R/E	R/E	-
6	Notificar acceso habilitado	I	I	I	R/E	R/E	I
7	Validar accesos y privilegios	R	E	I	C	C	-
8	Notificar inconvenientes con el acceso	R	E	I	I	I	I
9	Notificar acceso correctamente validado	R	E	I	I	I	I
10	Actualizar registro de usuarios y accesos	-	-	I	R/E	R/E	C

Adicionalmente, la matriz de responsabilidades para baja o modificación de usuarios se distribuye de la siguiente manera:

ID	ACTIVIDAD	JEFATURA DPTO. ADMIN. SISTEMA	GDP	JEFATURA DIVISIÓN DUEÑA SISTEMA	UNIDAD TIC - DAG	ENC. SI / LÍDER SSI	JEFATURA DAG
1	Notificar desvinculación o cambio de función	I	E	I	I	I	R
2	Crear ticket para baja o modificación de usuario	-	I	-	E	-	R
3	Ingresar a controlador de dominio	-	-	-	E	-	R
4	Ejecutar baja o modificación de usuario	-	-	-	E	-	R
5	Cerrar ticket	-	I	-	E	I	R
6	Ingresar a sistema divisional	E	-	R	-	-	-
7	Ejecutar baja o modificación de usuario	E	I	R	-	I	-
8	Actualizar el registro de usuarios y accesos del sistema divisional	E	-	R	-	C	-

Adicionalmente, la matriz de responsabilidades para revisión de usuarios y accesos se distribuye de la siguiente manera:

ID	ACTIVIDAD	JEFATURA DIVISIÓN DUEÑA SISTEMA	JEFATURA DPTO. ADMIN. SISTEMA	UNIDAD TIC - DAG	ENC. SI / LÍDER SSI
1	Ejecución de cruce entre usuarios del sistema y el registro de usuarios respectivo	R	E	E	C
2	Hacer revisión de accesos y privilegios en el sistema	R	E	E	C
3	Regularizar usuarios y accesos en sistema	R	E	E	C
4	Actualizar registro de usuarios para el sistema	R	E	E	C
5	Actualizar registro de usuarios con fecha de última revisión	R	E	E	C

8. REGISTROS DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-4.1—Registro de usuarios para sistema divisional
MANUAL / PROCEDIMIENTO	Acceso a sistemas divisionales Baja o modificación de usuarios y acceso Revisión de usuarios y acceso
CONTROLES ISO 27.001	• A.09.02.01 – Registro y cancelación de registro de usuario. • A.09.02.03 – Administración de derechos de acceso privilegiados. • A.09.02.04 – Administración de la información de autenticación secreta de los usuarios. • A.09.02.05 – Revisión de los derechos de acceso de los usuarios. • A.09.02.06 – eliminación o ajuste de los derechos de acceso
RESPONSABLE	Jefatura de División Dueña del Sistema, o quien ésta designe
DESCRIPCIÓN	Corresponde al documento de registro de usuarios para los sistemas divisionales.
FRECUENCIA	Dependerá de las definiciones establecidas para la revisión de usuarios y accesos y la demanda de alta, baja y modificación de usuarios.
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-PRO-4.1—Consolidado de tickets de alta, baja y modificación de usuarios
MANUAL / PROCEDIMIENTO	Alta general de usuarios Baja o modificación de usuarios y acceso Revisión de usuarios y acceso
CONTROLES ISO 27.001	• A.09.01.02 – Acceso a redes y servicios de red.

	• A.09.02.02 – Entrega de acceso a los usuarios.
RESPONSABLE	Jefatura Unidad de TIC – DAG
DESCRIPCIÓN	Corresponde al consolidado de tickets del sistema de mesa de ayuda que funciona como registro de las altas, bajas y modificaciones de usuario, que deben coincidir con los usuarios y privilegios vigentes.
FRECUENCIA	Dependerá de las definiciones establecidas para la revisión de usuarios y accesos y la demanda de alta, baja y modificación de usuarios.
ALMACENAMIENTO	Digital – Google Drive del responsable

9. NO CONFORMIDADES E INCUMPLIMIENTO

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

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

10. ANEXOS

10.1. Anexo I: Planilla para asignación de derechos de acceso privilegiados en sistemas y softwares

	Registro de Operación			
	Nivel de Confidencialidad	*Medio Uso Interno*	Páginas	1 de 1
			Versión	0
	Fecha versión del documento	TBD	Código	SSI-RO-PRO-4.1
	Procedimiento de Gestión de Cuentas y Accesos			

REGISTRO DE USUARIOS PARA SISTEMA DIVISIONAL

Nombre Sistema	
Descripción Funcional:	
Administrador/a:	
Dueño de Activos:	

Nombre y Apellido	ID Usuario	Rol Institucional	Perfil en el Sistema	Fecha de entrega de acceso	Fecha de cierre de acceso (solo si aplica)	Observaciones

TERCERO: APRUEBASE, el Manual para Gestión de Accesos y Privilegios en Sistemas de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. OBJETIVO

Prevenir el acceso no autorizado a los sistemas y aplicaciones.

2. ALCANCE

Estos lineamientos deben ser aplicados a todos los sistemas y software de la Agencia, ya sea administrado por la Unidad de TIC o por alguna de las Divisiones.

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

a) ISO/IEC 27001:2013, Control A.09.04.01 – Restricción de acceso a la información.

b) ISO/IEC 27001:2013, Control A.09.04.02 – Procedimiento de inicio de sesión segura.

c) ISO/IEC 27001:2013, Control A.09.04.03 – Sistema de gestión de contraseñas.

d) ISO/IEC 27001:2013, Control A.09.04.04 – Uso de programas utilitarios privilegiados.

e) ISO/IEC 27001:2013, Control A.09.04.05 – Control de acceso al código fuente de los programas.

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, en donde se aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.3 relativo al principio de control de acceso físico y lógico.

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

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

4. TÉRMINOS Y DEFINCIONES

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

5. ROLES Y RESPONSABILIDADES

a) **Jefaturas de División:** responsable de determinar los privilegios de acceso a la información y sistemas de la Agencia, así como de velar por el cumplimiento y correcta aplicación de lo estipulado en este manual para aquellos sistemas y software que sean administrados por alguno de los Departamentos o Unidades que conforman la División en el contexto de acceso a la información (Dueño funcional del sistema), así como de facilitar la implementación de las medidas necesarias para cumplir con su objetivo y alcance.

b) **Líder(es) Interno(s) del SSI:** responsables de liderar la adopción de los dispuesto en este manual al interior de su División.

c) **Jefatura de la Unidad de TIC – DAG:** ejecutar correctamente lo estipulado en este manual para aquellos sistemas y software que sean administrados por la Unidad de TIC en el contexto de acceso a la información (Dueño funcional del sistema), así como de facilitar la implementación de las medidas necesarias para cumplir con su objetivo y alcance.

d) **Jefaturas de Departamento:** ejecutar correctamente lo estipulado en este manual para aquellos sistemas y software que sean administrados por el Departamento en el contexto de acceso a la información (Dueño funcional del sistema), así como de facilitar la implementación de las medidas necesarias para cumplir con su objetivo y alcance.

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

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

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

6. LINEAMIENTO DEL MANUAL

Para una correcta gestión del acceso a la información contenida, almacenada y procesada a través de sistemas y software de la Agencia, se deben tener en cuenta que las restricciones de acceso a la información deben basarse en los requisitos individuales de los usuarios y otros sistemas para el cumplimiento de su ámbito de responsabilidades o el objetivo para el cual fueron concebidos respectivamente. Para facilitar la definición de restricciones en el acceso a la información se deben tener en cuenta los siguientes lineamientos:

a) Proporcionar, en cada sistema o software de la Agencia, menús para el control de acceso a las funciones del sistema o software.

b) Controlar mediante definiciones propias de los administradores de los sistemas y software en el ámbito del acceso a la información y privilegios, qué datos pueden ser accedidos por un usuario o rol determinado. Para esto tener en consideración la plantilla provista en el Anexo 1 de este documento.

c) Controlar qué derechos de acceso o privilegios se otorga a los usuarios que requieren acceso a la información de acuerdo con lo estipulado en el punto anterior, por ejemplo, privilegios de lectura, escritura, ejecución, borrado, etc. Para esto tener en consideración la plantilla provista en el Anexo 1 de este documento.

d) Controlar los derechos de acceso de otros sistemas y softwares bajo la misma lógica de los dos puntos descritos anteriormente.

e) Proporcionar controles de acceso físico y lógicos para aislar aplicaciones sensibles, los datos de aplicación o los sistemas, para lo cual debe considerarse el principio de seguridad en la operación TIC dispuesto en la Política General de Seguridad de Información (SSI-POL-01)[9].

f) Validar la información de inicio de sesión sólo cuando se hayan completado todos los datos de entrada. Si se detecta algún error, el sistema no debería indicar qué parte de la información de autenticación es correcta o incorrecta.

g) Todos los sistemas y softwares de la Agencia deben incorporar mecanismos de inicio de sesión seguros, que consideren como mínimo un factor de autenticación. Para sistemas de alta criticidad o que apoyen al almacenamiento y/o procesamiento de activos de información críticos se debe implementar doble factor de autenticación. Adicionalmente, para la implementación de este punto se debe tener en cuenta lo siguiente:

    i. No mostrar identificadores del sistema o software hasta que el proceso de inicio de sesión se haya completado con éxito.

[9] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.4), letra b), punto i) sobre los requisitos de seguridad para el desarrollo y mantención de software.

ii. No proporcionar mensajes de ayuda durante el proceso de autenticación que puedan ayudar a usuarios no autorizados.

iii. Se deberán registrar eventos y monitorear los intentos de inicio de sesión exitosos y fallidos, de forma de proteger los sistemas contra intentos de fuerza bruta y generar alertas de seguridad cuando se detecten intentos potenciales o con éxito de violación de los controles de inicio de sesión. Para lo anterior, se debe considerar principio de seguridad en la operación TIC dispuesto en la Política General de Seguridad de Información (SSI-POL-01)[10].

iv. No mostrar la contraseña que se está introduciendo ni transmitirlas por la red sin cifrar, como lo indica el principio de seguridad en la operación TIC dispuesto en la Política General de Seguridad de Información (SSI-POL-01) [11].

6.1. Sistemas de Gestión de Contraseñas

Los sistemas de gestión de contraseñas deberán ser interactivos y proveer de contraseñas seguras y robustas. Por lo anterior, un sistema de gestión de contraseñas deberá:

a) Aplicar el uso de identificadores de usuario (ID) y contraseñas individuales que lo identifiquen y lo hagan responsable de sus acciones. Sólo deberá permitirse el uso de IDs compartidos cuando fuera necesario por razones institucionales o de operación, y deberían ser aprobados y quedar documentado. El ID de usuario debe seguir la siguiente nomenclatura:

   i. Para usuarios internos de la Agencia: nombreapellido.

   ii. Para usuarios externos de la agencia: nombreapellidoext.

b) En caso de requerirse el uso de cuentas genéricas o compartidas, deberá reforzarse la seguridad sobre la información de autenticación secreta por ejemplo, cambiando con mayor frecuencia las contraseñas de acceso, y de inmediato cuando uno de los usuarios deja la organización.

c) Permitir a los usuarios escoger y cambiar sus propias contraseñas e incluir mecanismos de confirmación que tenga en cuenta los errores de entrada.

d) Imponer la selección de contraseñas de calidad, considerando como mínimo para el cumplimiento de este punto que ésta sea de al menos siete (7) caracteres alfanuméricos.

e) Forzar a los usuarios a cambiar su contraseña tras el primer inicio de sesión, así como forzar los cambios regulares de contraseña cada tres (3) meses.

f) Mantener un registro de las últimas cinco (5) contraseñas utilizadas para evitar su reutilización.

g) Los usuarios serán responsables de mantener la confidencialidad de su información de autenticación secreta según el principio de control de acceso

[10] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.4), letra a), punto i) sobre la seguridad en las operaciones TIC.

[11] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.4), letra b), punto i) sobre los requisitos de seguridad para el desarrollo y mantención de software.

lógico establecido en la Política General de Seguridad de Información (SSI-POL-01)[12].

7. REGISTRO DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-4.2—Definición de roles y perfiles para acceso a sistemas y software.
MANUAL / PROCEDIMIENTO	Gestión de accesos y privilegios a sistemas y aplicaciones
CONTROLES ISO 27.001	• A.09.04.01 – Restricción de acceso a la información. • A.09.04.04 – Uso de programas utilitarios privilegiados. • A.09.04.05 – Control de acceso al código fuente de los programas.
RESPONSABLE	Dueños funcionales de sistemas y aplicaciones: - Jefaturas de División, o a quienes éstos designen. - Jefatura Unidad TIC-DAG
DESCRIPCIÓN	Corresponde a una matriz en la cual se definen los roles o tipos de usuario y que funcionalidades o acceso a la información deben asignarse para el cumplimiento de ámbito de responsabilidades.
FRECUENCIA	Anual o en función de cambios en la definición de roles y perfiles de acceso.
ALMACENAMIENTO	Digital – Google Drive del responsable

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-7.2—Configuración en sistemas y aplicaciones para la gestión de contraseñas.
MANUAL / PROCEDIMIENTO	Gestión de accesos y privilegios a sistemas y aplicaciones
CONTROLES ISO 27.001	• A.09.04.02 – Procedimiento de inicio de sesión segura. • A.09.04.03 – Sistema de gestión de contraseñas.
RESPONSABLE	Jefe Unidad TIC - DAG
DESCRIPCIÓN	Corresponde a las capturas de pantalla de las configuraciones de los sistemas y software que exigen la utilización de contraseñas según lo definido en este procedimiento.
FRECUENCIA	Anual
ALMACENAMIENTO	Digital – Google Drive del responsable

8. NO CONFORMIDADES E INCUMPLIMIENTOS

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

[12] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.3), letra a), punto iv) sobre las responsabilidades del usuario en el acceso a la información.

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

9. ANEXOS

9.1. Anexo I: Definición de roles y perfiles para acceso a sistemas y software

Agencia de Calidad de la Educación	Registro de Operación			
	Nivel de Confidencialidad:	Media Uso Interno	Páginas:	1 de 1
			Versión:	1
	Fecha versión del documento:	TBD	Código:	SI-RO-MAN-4
	Manual para la Gestión de Roles y Perfiles en Sistemas y Software			

Nombre del Sistema:	
Descripción funcional:	
Administradora:	
Dueño de Activos:	

OL INSTITUCIONA	PERFIL EN EL SISTEMA O SOFTWARE																															
	PERFIL 1	PERFIL 2	PERFIL 3	PERFIL 4	PERFIL 5	PERFIL 6	PERFIL 7	PERFIL 8	PERFIL 9	PERFIL 10	PERFIL 11	PERFIL 12	PERFIL 13	PERFIL 14	PERFIL 15	PERFIL 16	PERFIL 17	PERFIL 18	PERFIL 19	PERFIL 20	PERFIL 21	PERFIL 22	PERFIL 23	PERFIL 24	PERFIL 25	PERFIL 26	PERFIL 27	PERFIL 28	PERFIL 29	PERFIL 30	PERFIL 31	PERFIL 32	PERFIL 33	PERFIL 34
Rol 1	X	X				X			X				X				X															X		
Rol 2	X	X		X	X						X																					X		
Rol 3	X																															X		
Rol 4	X																															X		
Rol 5	X	X		X	X	X									X														X			X		
Rol 6																																X		
Rol 7	X	X			X	X	X				X						X	X				X								X		X		
Rol 8																																X		
Rol 9	X																															X		X
Rol 10				X	X																													
Rol 11	X			X	X	X																										X		
Rol 12	X	X		X	X	X				X	X		X			X	X	X					X									X		
Rol 13	X				X	X																										X	X	

CUARTO: APRUEBASE, el Manual de Responsabilidad del Usuario en el Acceso a la Información de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. ANEXOS

Establecer las responsabilidades de los usuarios de la Agencia para evitar vulneraciones a la información de la institución mediante el correcto uso de sus privilegios de acceso a la información.

2. ALCANCE

Este manual debe ser aplicado por todos los funcionarios de la Agencia, de planta, contrata y honorarios, así como a proveedores externos y toda persona que por cumplimiento de su ámbito de responsabilidades se le asigne un usuario dentro de los sistemas informáticos de la Agencia.

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

a) ISO/IEC 27.001:2013, Control A.08.01.03 – Uso aceptable de activos

b) ISO/IEC 27.001:2013, Control A.08.02.03 – Manejo de activos

c) ISO/IEC 27.001:2013, Control A.09.03.01 – Uso de información de autenticación secreta.

d) ISO/IEC 27.001:2013, Control A.11.02.09 – Política de escritorio y pantalla limpios.

3. NORMAS Y REFERENCIAS

a) Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, incluyendo el punto 6.2.3 relativo al principio de control de acceso físico y lógico.

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

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

4. TÉRMINOS Y DEFINICIONES

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

5. ROLES Y RESPONSABILIDADES

a) **Jefaturas de División:** como propietarios de los activos de información que soportan los procesos de la División, serán los responsables de velar por la correcta adopción de lo dispuesto en este documento por parte de los usuarios de su División.

b) **Líder(es) Interno(s) del SSI:** responsables de liderar la correcta aplicación y adopción de los lineamientos dispuestos en este documento al interior de su División.

c) **Jefaturas de Departamento:** como custodios de los activos de información, deben ejecutar los lineamientos de este documento al interior de su Departamento.

d) **Encargada de Seguridad de Información y Encargada de Ciberseguridad**: ejerce como rol asesor a nivel administrativo y operativo, respectivamente, la mejora continua de los lineamientos dispuestos en ese Manual.

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

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

6. LINEAMIENTOS DEL MANUAL

Los usuarios, como parte del cumplimiento de su ámbito de responsabilidades públicas en función de sus privilegios de acceso y tratamiento sobre la información y datos de la Agencia, deberán aplicar los siguientes lineamientos:

6.1. Uso de información secreta de autenticación

Se deberá requerir a los usuarios que sigan las siguientes prácticas:

a) Mantener en estricta confidencialidad la información de autenticación a los sistemas y software de la Agencia, asegurando que no se divulgue a cualquier otra parte, incluyendo personas con autoridad.

b) No se debe guardar la información de autenticación secreta a menos que ésta pueda ser almacenada de forma segura y que el método de almacenamiento sea aprobado por la institución.

c) Cambiar la información secreta de autenticación siempre que haya indicios de su posible compromiso, si la contraseña es por defecto, o cuando la organización lo disponga.

d) Al momento de seleccionar contraseñas, éstas deben ser fáciles de recordar y difícil de adivinar por otros usuarios o agentes externos.

e) No usar la misma información de autenticación secreta en el ámbito laboral y personal.

f) La utilización de cuentas de usuario genéricas debe limitarse lo más posible, pero, de utilizarse cuentas de usuario genéricas, el rol propietario o custodio de los activos de información debe llevar un registro estricto de los usuarios que la utilizarán, así como asumir la responsabilidad en caso de algún incidente relacionado con el uso compartido de cuentas.

6.2. Escritorio y pantalla limpios

Dentro del contexto de la operación con información de la Agencia, se deben seguir los siguientes lineamientos de minimización de accesos no autorizados en base al escritorio y pantallas limpias, las cuales son extensivas al contexto de teletrabajo:

a) La información crítica, ya sea en formato físico o almacenada en medios extraíbles de almacenamiento, debe estar guardada, sobre todo cuando la oficina o lugar de trabajo está vacía.

b) El equipamiento como notebooks o laptops deberá ser apagado o bloqueada su pantalla si no se estará trabajando en ellos.

c) Los soportes o documentos críticos de la Agencia deben ser retirados de manera inmediata de fotocopiadoras e impresoras.

6.3. Uso aceptable de activos y equipamiento

Adicional a lo anterior, los usuarios de la Agencia serán responsables de la correcta manipulación y uso de los activos de información y tecnología, ya sea a nivel físico o lógico, a la cual tienen acceso como parte del cumplimiento de su ámbito de responsabilidades. Para lo anterior, se deben considerar los siguientes lineamientos:

a) Ser conscientes y estar en conocimiento de la definición de activos de información críticos de su División, los cuales se encuentran definidos en el Inventario de Activos de Información respectivo.

b) En caso de pertenecer a una División de la segunda línea de defensa, además de lo dispuesto en el punto anterior, los usuarios deben estar en conocimiento de los activos de información críticos de las Divisiones de primera línea a los cuales tienen acceso como parte del cumplimiento de su ámbito de responsabilidades.
c) La transferencia de información y datos de la Agencia deberá estar alineada con lo dispuesto en el principio de gestión de activos y transferencia de información establecido en la Política General de Seguridad de Información (SSI-POL-01)[13].

d) Para evitar pérdidas de información asociadas a su ámbito de responsabilidades, los usuarios deben almacenar la información y datos pertenecientes a la Agencia únicamente en Google Drive como el único repositorio autorizado por la Agencia.

e) En caso de no existir una clasificación de criticidad para algún activo de información, será responsabilidad del usuario manipular el activo cumpliendo con las dimensiones de confidencialidad, disponibilidad, integridad y privacidad, según lo dispuesto por el principio de gestión de activos y transferencia de información establecido en la Política General de Seguridad de Información (SSI-POL-01). Así mismo, deberá comunicarse con el propietario y/o custodio de este para su inclusión en el Inventario de Activos en caso de resultar crítico[14].

f) Los usuarios serán responsables de cerrar cualquier sesión activa en sus equipos o sistemas y software de la Agencia una vez terminadas las actividades relacionadas con ésta.

g) Los usuarios serán responsables de la toma de decisiones que pueda afectar a los activos de información que manejan para cumplir con su ámbito de responsabilidades, debiendo ser conscientes del impacto que puedan tener éstas para la Agencia.

h) Será responsabilidad de los usuarios, notificar al rol administrador de los sistemas o en su defecto al Líder Interno del SSI de su División, sobre cualquier acceso que no corresponda a su ámbito de responsabilidades, así como de aquellos accesos especiales que ya han caducado, para que el administrador de este proceda a su cancelación.

i) Notificar al propietario o custodio de los activos de información, así como al Líder Funcional del SSI respectivo, sobre cualquier incumplimiento o no conformidad sobre la ejecución de uno o varios de los manuales y procedimientos del SSI.

---

[13] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra a), punto ii) sobre la transferencia y confidencialidad de información.
[14] Resolución Exenta N°583, de 2021, de la Agencia de Calidad de la Educación, que aprueba la Actualización de la Política General de Seguridad de la Información, numeral 6.2.2), letra a), punto i) sobre la elaboración y actualización del inventario de activos de información de la Agencia.

7. REGISTRO DE OPERACIÓN

INFORMACIÓN DEL REGISTRO	DESCRIPCIÓN
NOMBRE	SSI-RO-MAN-4.3—Resultados de revisión de responsabilidades del usuario
MANUAL / PROCEDIMIENTO	Responsabilidad del usuario en acceso a la información
CONTROLES ISO 27.001	• A.08.01.03 – Uso aceptable de activos • A.08.02.03 – Manejo de activos • A.09.03.01 – Uso de información de autenticación secreta. • A.11.02.09 – Política de escritorio y pantalla limpios
RESPONSABLE	Jefaturas de División, o a quien éstas designen.
DESCRIPCIÓN	Corresponde a los resultados de la revisión de los puestos de trabajo físicos de los usuarios, donde se deberá verificar que no exista información sensible a simple vista, que los equipos desatendidos estén bloqueados, que no haya contraseñas anotadas físicamente, entre otros a fin con los lineamientos de este manual.
FRECUENCIA	Anual
ALMACENAMIENTO	Digital – Google Drive del responsable

8. NO CONFORMIDADES E INCUMPLIMIENTOS

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

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

QUINTO: DÉJASE SIN EFECTO la Resoluciones Exenta N°s 1025, 1027, 1527, 1611 y 1616, de 2019, de la Agencia de Calidad de la Educación.

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

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

PUBLÍQUESE la presente resolución en el Portal Transparencia.

DANIEL RODRÍGUEZ MORALES
SECRETARIO EJECUTIVO
AGENCIA DE CALIDAD DE LA EDUCACIÓN

ABA/GCL/NJO/CBR

Distribución:

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