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

APRUEBA ACTUALIZACIÓN DE POLITICA DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA DE CALIDAD DE LA EDUCACIÓN.

RESOLUCIÓN EXENTA N° 583

SANTIAGO, 28 SEP 2021

VISTOS:

Lo dispuesto en el DFL N° 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N° 19.880, que establece las Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado; en la Ley N° 20.529, sobre Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización; en la Ley N° 20.285, sobre Acceso a la Información Pública; en la Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firmas; en la Ley N° 19.628, sobre Protección a la Vida Privada; en el Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en la norma chilena NCh-ISO 27001; Resolución Exenta N°589 de 2019, que aprueba Nueva Política General de Seguridad de la Información de la Agencia de Calidad de la Educación; Resolución Exenta N° 218 de 2021 que aprueba medidas y procedimientos de datos personales; en la Resolución Nº 7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del Trámite de Toma de Razón, y

CONSIDERANDO:

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

Que, de acuerdo al Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, la norma chilena NCh-ISO 27001, y otras normativas presentes en el Sistema de Gestión de Seguridad de la Información, las exigencias y recomendaciones que se proveen, presentan desafíos en cuanto a la necesidad de garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información.
Que, de conformidad con lo señalado en el artículo 11 del decreto supremo individualizado en el considerando precedente, se deberá establecer una política que fije las directrices generales que orienten la materia de seguridad dentro de cada institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura institucional.

Que por Resolución Exenta N°589, de 16 de mayo de 2019, que aprueba Nueva Política General de seguridad de la Información de la Agencia de Calidad de la Educación, la cual establece una serie de objetivos a cumplir por el Servicio, entre los cuales se estableció la identificación y actualización permanentemente de:

- ✓ Los procesos claves, para la mantención operativa de la Agencia, con el fin de establecer la cadena de valor de procesos de la organización, con lo cual, la Agencia logrará determinar el primer alcance del SGSIC.
- ✓ Todos los activos de información que reciba, almacene, procese y emita la Agencia. Estos activos se podrán encontrar en distintos medios y formatos, tanto físicos como digitales.
- ✓ La tecnología asociada a los activos de información, con el fin de establecer la relación entre los procesos críticos de la organización y la tecnología que los

soporta. Esta identificación deberá ser gestionada a través de la implementación de un inventario actualizado de componentes tecnológicos que apalancan la operación de la organización.

- ✓ La clasificación de los activos de información identificados, bajo los parámetros de la confidencialidad, integridad, disponibilidad, autenticidad y privacidad, con el fin de lograr una categorización de los activos de información, en función de su grado de criticidad para la institución (baja, media, alta). En esta operación deberán participar todas las líneas operacionales constitutivas de la cadena de valor de la organización. Este proceso, entregará una mirada más detallada sobre cuáles son los activos de información más críticos para la Agencia, y por qué procesos fluyen durante la ejecución de la operación de la institución.
- ✓ La realización de análisis de riesgos sobre los activos de información con niveles de criticidad media y alta. Dichos análisis deberán considerar al menos los siguientes indicadores: el valor o criticidad del activo de información, el peso de las vulnerabilidades asociadas a la tecnología y el peso asociado a una tipificación de amenazas o a la captura de indicadores de amenazas para la tecnología asociada a los procesos críticos de la Agencia. Este proceso, entregará una mirada más detallada sobre donde colocar los esfuerzos para reducir o mantener el riesgo de imagen reputacional de la Agencia y de cumplimiento del PMG asociado a estas materias.
- ✓ La determinación, en base al análisis de riesgo, del alcance específico del SGSIC. Éste alcance deberá estar definido en función de los riesgos de alto impacto, o bien, que podrían afectar negativamente la consecución de los objetivos de la institución. La organización trabajará en el establecimiento de mecanismos, que se enfoquen en el crecimiento y madurez del ambiente de control que se establezca, para efectos de reducir los riesgos asociados a la operación y cumplimiento de la Agencia.
- ✓ La implementación del SGSIC alineado a las mejores prácticas del mercado en estas materias, alineado al cumplimiento derivado de regulaciones, leyes y decretos de Gobierno. En la implementación del ambiente de control para sostener el SGSIC, la Agencia declara que se enfocará en la operación de los siguientes procesos asociados a la seguridad de la información y la ciberseguridad:
    - Seguridad de la información y ciberseguridad de los recursos humanos.
    - Gestión de activos de información.
    - Gestión del riesgo de los activos de información.
    - Establecimientos de mecanismos y medidas de protección sobre los activos de información.
    - Establecimientos de mecanismos y buenas prácticas de seguridad de la información, relacionadas con el proceso de desarrollo y/o adquisición de software y tecnología.
    - Gestión de vulnerabilidades y remediación de brechas.
    - Establecimientos de mecanismos y medidas de monitoreo sobre los activos de información e identificación de posibles incidentes.
    - Establecimiento de mecanismos y medidas de contención y respuesta frente a incidentes.
    - Establecimiento de mecanismos y medidas de recuperación y vuelta a la normalidad de los procesos y sistemas frente a posibles incidentes.
    - Establecimiento de mecanismos y medidas de sensibilización y formación en estas materias, con el fin de cambiar de manera progresiva, la cultura institucional y los niveles de concientización en seguridad de la información y ciberseguridad.

Que, de igual modo la Agencia ha implementado una gobernanza para gestionar la seguridad de la información y la ciberseguridad al interior de la institución, y velar por el crecimiento en madurez de la seguridad corporativa, en base a la determinación y asignación de roles definidos para tales efectos, incorporando en el perfil de cargo, las funciones y responsabilidades que cada rol asume al interior de la organización, para garantizar una adecuada gestión de la seguridad de la información al interior de la institución.

Que, conforme a lo establecido, se deberá revisar el cumplimiento de la Política General de Seguridad de la Información, con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento y mejora continua de la misma.

Que, a la fecha se ha avanzado en cada uno de los compromisos, y en especial en el cambio cultural sobre la materia, lo que nos estar a la altura de los requerimientos del CSIRT del Gobierno y de los avances en la materia.

Que, en razón de la evaluación realizada, se requiere dar un nuevo paso en la institucionalidad y gobernanza del Sistema de Seguridad de la Información y Ciberseguridad de la Agencia, recogiendo con ello la labor desarrollada por los equipos durante este año 2021 para su profundización, actualizando la política y definición de roles y responsabilidades, estableciendo los pilares institucionales sobre la materia, abarcar 16 controles ISO básicos para una estructura robusta se seguridad y que nos permitan seguir avanzando en el cambio cultural y el establecimiento de procedimientos específicos para aumentar la madurez del sistema.

RESUELVO:

PRIMERO: **APRUEBASE,** la Política General de Seguridad de Información y Ciberseguridad de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

1. DECLARACIÓN INSTITUCIONAL

El Sistema Nacional de Aseguramiento de la Calidad de la Educación, tiene por objeto propender a asegurar una educación de calidad en sus distintos niveles, y a asegurar la equidad en él, entendida como tal, que todos los estudiantes tengan las mismas oportunidades de recibir una educación de calidad.

Conforme a lo anterior, la Agencia de Calidad de la Educación, en adelante la Agencia, tiene por objeto el evaluar y orientar el 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, junto a ello debe proporcionar información a la comunidad educativa en materias de su competencia, promoviendo su correcto uso.

Dado lo anterior, se desprende que la operación central de la Agencia se basa en la recolección de información, su tratamiento para la obtención de indicadores y métricas en las materias de su competencia, y la presentación de éstos, tanto a nivel estatal para el apoyo en la toma de decisiones referentes al mejoramiento de la calidad de la educación tanto en materia de políticas públicas; en la gestión educativa de los establecimientos educacionales como a las padres y apoderados.

Es así, como la Agencia reconoce la información y los datos personales que ésta puede contener, como su activo de mayor relevancia, catalogándola como un elemento crítico de apoyo al cumplimiento del Objetivo Institucional, que por tanto, requiere ser protegida convenientemente (junto a los procesos y sistemas que la utilizan) frente a amenazas y riesgos que puedan poner en peligro la continuidad operacional, rentabilidad social y conformidad legal, necesarios para alcanzar los objetivos institucionales y preservar la reputación y transparencia de las entidades de gobierno hacia los ciudadanos.

Por lo tanto, la Agencia se encuentra estableciendo un proceso, el cual, vele por el cumplimiento y operación de mecanismos que se enfoquen en la protección, respuesta y recuperación frente a posibles incidentes que puedan afectar negativamente focos como: la transparencia, reputación, imagen y operación de la Institución, en el marco de las otras unidades de gobierno. En este contexto, la Agencia ha fortalecido su ambiente de control, con el fin de mantener el valor de la información a través del tiempo, conservando

aspectos como la confidencialidad, integridad, disponibilidad, y privacidad de los activos de información institucionales relevantes o claves para la operación de la organización. Esto, ha operado desde 2019 a través de la implementación de un Sistema de Seguridad de la Información a nivel institucional, en adelante SSI, que ha permitido aumentar de manera progresiva en el tiempo, los niveles de madurez de la organización en materia de seguridad de la información y ciberseguridad. La cual a partir de esta evaluación y actualización de la política aspira a lograr su madurez y operatividad, logrando cambios dentro de la cultura organizacional y que la seguridad de la información sea un principio transversal a la gestión de la Agencia. Ejemplo de ello, es la consideración en los convenios de desempeño de las jefaturas de división, seleccionadas por sistema de alta dirección Pública compromisos en la materia de Seguridad de la Información y Ciberseguridad.

Adicionalmente, es parte de la declaración de la Agencia ver la seguridad de la información y la ciberseguridad, como componentes claves y estratégicos para la mantención y preservación de la imagen reputacional, cumplimiento regulatorio y prestigio de la institución. En este escenario, el proceso de construcción de la seguridad de la información y la ciberseguridad en Agencia deberá ser visto como un apalancador estratégico de los objetivos de la Organización.

2. ALCANCE

Esta Política contiene los lineamientos generales de la Agencia de Calidad de la Educación en materias relativas a la Seguridad de la Información y la Ciberseguridad. Esta Política deberá ser aplicada por todos(as) los(as) funcionarios(as) de planta y contrata, personal a honorarios y toda aquella persona natural o jurídica que preste servicios (terceros y proveedores) y que, a raíz de ello, tengan acceso a los activos de información de la Institución.

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:

- ISO/IEC 27.001:2013, Control A.05.01.01 – Políticas de seguridad de información
- ISO/IEC 27.001:2013, Control A.05.01.02 – Revisión de políticas de seguridad de información
- ISO/IEC 27.001:2013, Control A.06.01.01 – Roles y responsabilidades de la seguridad de la información
- ISO/IEC 27.001:2013, Control A.06.01.02 – Segregación de funciones
- ISO/IEC 27.001:2013, Control A.06.01.04 – Contacto con grupos de interés especiales
- ISO/IEC 27.001:2013, Control A.09.01.01 – Política de control del acceso
- ISO/IEC 27.001:2013, Control A.12.01.01 – Procedimientos de operación documentados
- ISO/IEC 27.001:2013, Control A.16.01.01 – Responsabilidades y procedimientos
- ISO/IEC 27.001:2013, Control A.17.01.01 – Planificación de la continuidad de la seguridad de la información
- ISO/IEC 27.001:2013, Control A.17.01.02 – Implementación de la continuidad de la seguridad de la Información
- ISO/IEC 27.001:2013, Control A.17.01.03 – Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- ISO/IEC 27.001:2013, Control A.18.01.01 – Identificación de la legislación vigente y los requisitos contractuales
- ISO/IEC 27.001:2013, Control A.18.01.03 – Protección de registros
- ISO/IEC 27.001:2013, Control A.18.02.01 – Revisión independiente de la información de seguridad de la Información
- ISO/IEC 27.001:2013, Control A.18.02.02 – Cumplimiento con las políticas y normas de seguridad
- ISO/IEC 27.001:2013, Control A.18.02.3 – Verificación del cumplimiento técnico

3. 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 este documento.

4. ROLES Y RESPONSABILIDADES

a) **Comité de Seguridad de Información:** Aprobar en sesión lo dispuesto en este documento y apalancar su mejora continua a través de revisiones ejecutivas periódicas al SSI y el monitoreo contante de su rendimiento.

b) **Jefaturas de División:** Responsables de revisar esta política, validando la relación con los manuales y procedimientos que de ésta se desprenden. Así mismo, serán responsables del cumplimiento de lo estipulado en este documento por parte de su División, así como de apalancar su mejora continua en el tiempo.

c) **Encargada de Seguridad de Información:** Responsable asesorar en la implementación y mejora continua de los lineamientos propuestos en este documento.

d) **Auditoría Interna:** Responsable de la gestión del programa de auditoría para abordar la mejora continua de los lineamientos propuestos en este documento, así como de los manuales y procedimientos que de este se desprenden.

5. OBJETIVOS ESPECÍFICOS DEL SISTEMA DE SEGURIDAD DE INFORMACIÓN

El Sistema se sustenta en base a los siguientes objetivos a cumplir y que insuman cada una de sus acciones

a) ***Confidencialidad***, la Agencia deberá verificar la aplicación de los controles necesarios para resguardar los activos de información de cualquier acceso no autorizado, revelaciones accidentales, espionaje, violación de la privacidad y otras acciones de similares características.

b) ***Integridad***, la Agencia deberá verificar por la aplicación de los controles necesarios para resguardar los activos de información de cualquier degradación por efectos de agentes internos o externos, ambientales o manipulación que afecten su exactitud y completitud.

c) ***Disponibilidad***, la Agencia deberá verificar por la aplicación de los controles necesarios para resguardar a los activos de información de cualquier interrupción, asegurando que éstos se encuentren accesibles y utilizables por usuarios autorizados, para que no afecte la continuidad operacional.

d) ***Privacidad***, la Agencia deberá velar por la aplicación de los controles necesarios para resguardar los activos de información y mantener las características de privacidad, en cumplimiento de las garantías constitucionales, estableciendo la exigencia sobre el manejo y uso de la información conforme a la legislación vigente. Por lo tanto, Agencia deberá atender no sólo las exigencias regulatorias respecto a la información personal, sino desarrollar los mecanismos y estrategias que permitan su adecuada administración, lo que incluye aspectos como su recolección, uso, procesamiento, almacenamiento y revelación.

6. MARCO GENERAL DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En esta sección, se establecen las etapas generales que rigen a la Agencia en el tratamiento de activos, así como los principios de seguridad de información y ciberseguridad que establece esta política.

6.1. Etapas generales en el proceso de tratamiento de activos

Dadas las facultades conforme a lo establecido en el Artículo 11 de la ley 20.529, la Agencia comprende que su actividad central es la recolección y procesamiento de datos e información propia confidencial, y/o datos e información personal sensible de terceros, y que ésta, representa un pilar crítico para la medición y mejora continua de la educación a nivel nacional, por lo tanto, declara que el tratamiento de los activos

de información que fluyen por sus procesos, debe ser estructurado y seguro durante todo su ciclo de vida, donde se destacan las siguientes etapas generales:

a) **Recolección de datos**, desde la elaboración de los ítems y/o cuestionarios de los instrumentos de medición, hasta la aplicación de los mismos en las instituciones de educación a nivel nacional, tanto, la Agencia como los terceros que participan de este proceso, deben mantener y garantizar la confidencialidad de estos activos de información.
b) **Tratamiento de datos**, donde la Agencia, mediante sus divisiones, debe analizar y tratar la información recolectada mediante la aplicación de los diferentes instrumentos de medición, con especial énfasis en la integridad de ésta, para la obtención de métricas e indicadores relevantes que apoyen la consecución de sus objetivos institucionales.
c) **Elaboración de informes de resultado**, donde la Agencia, posterior al análisis de los datos obtenidos y la obtención de indicadores, genera información concerniente a su materia de competencias, la cual, representa el principal insumo de apoyo a la toma de decisiones a nivel nacional, en función de la mejora de la calidad y equidad de la educación.
d) **Disponibilización de información**, donde la Agencia debe disponibilizar a la comunidad en general, información concerniente a su materia de competencia, velando por su correcto uso y garantizando que la publicación de ésta, en caso alguno incluirá la individualización de los alumnos.

Es así, como cualquier vulneración a la seguridad de los activos de información, en cualquiera de las fases descritas anteriormente, podría suponer como consecuencia, un cuestionamiento hacia la Agencia tanto a nivel reputacional, desde el punto de vista de la administración pública, como a nivel de transparencia, desde el punto de vista del servicio público hacia los ciudadanos y ciudadanas. Dado lo anterior, y, con el fin de velar por el cumplimiento de lo establecido en la declaración institucional de este documento, la Agencia deberá establecer un Sistema de Seguridad de Información (SSI).

6.2. Principios de la Política

Para dar cumplimiento a la aplicación de esta política, la Agencia estructura el SSI a través de los siguientes principios:

1. Gestión de Riesgos
2. Gestión de Activos y Transferencia de Información
3. Control de Acceso Físico y Lógico
4. Seguridad en la Gestión de Tecnologías de Información y Comunicación (TIC)
5. Gestión de Incidentes
6. Revisión Independiente del SSI

6.2.1. Principio de Gestión de riesgos

A través del SSI, la Agencia deberá realizar al menos de forma anual, un análisis de riesgos sobre los activos de información. Dicho análisis deberá considerar al menos los siguientes indicadores:

a) el valor o criticidad del activo de información,
b) el peso de las vulnerabilidades asociadas a la tecnología y
c) el peso asociado a una tipificación de amenazas o a la captura de indicadores de amenazas para la tecnología asociada a los procesos críticos de la Agencia.

Este proceso, debe entregar la indicación en donde se deberán enfocar los esfuerzos para reducir o mantener el riesgo de imagen reputacional de la Agencia y de cumplimiento asociado a estas materias, considerando también la legislación vigente en estas materias, definida en el Anexo II de este documento. A nivel operativo, este principio debe arrojar como resultado l**a Matriz de riesgos de seguridad de información y ciberseguridad.**

6.2.2. Principio de Gestión de Activos y Transferencia de Información

En base a la criticidad que representan para la Agencia los activos de información y los datos personales que estos puedan contener, el SSI debe establecer lineamientos estratégicos y operacionales que permitan mitigar los riesgos de seguridad de información y ciberseguridad a los cuales están sujetos estos activos, abordando los aspectos relativos tanto a la manipulación segura de los activos de información, incluyendo su almacenamiento, procesamiento y transferencia, así como los aspectos relativos con la seguridad en el equipamiento que los soporta.

Para dar cumplimiento a estos principios, el SSI de la Agencia considera la operación de los siguientes controles:

a) Sobre la manipulación segura de activos
    i. Procedimiento de elaboración y actualización del inventario de activos de información.
    ii. Manual para la transferencia y confidencialidad de información.
b) Sobre la seguridad en el equipamiento:
    i. Procedimiento de eliminación y reutilización del equipamiento.
    ii. Manual para la asignación y devolución de recursos.
    iii. Manual para administración de medios removibles.

6.2.3. Principio de Control de Acceso Físico y Lógico

De forma de mitigar los riesgos de disponibilidad, integridad, confidencialidad y privacidad sobre sus activos de información de la Agencia, el SSI debe implementar mecanismos que normen y limiten tanto el acceso como los privilegios sobre éstos. Para lo anterior, la Agencia define que estos mecanismos de control de acceso y gestión de privilegios deben abarcar tanto la dimensión física como la dimensión lógica en las cuales conviven los activos de información.

Para dar cumplimiento a estos principios, el SSI de la Agencia considera la operación de los siguientes controles:

a) Para la dimensión lógica:
    i. Procedimiento de gestión de cuentas de usuario y accesos.
    ii. Manual para la gestión de accesos y privilegios en los sistemas.
    iii. Manual para el trabajo remoto seguro.
    iv. Manual de responsabilidades del usuario en el acceso a la información.
b) Para la dimensión física:
    i. Manual de seguridad física.

6.2.4. Principio de Seguridad en la Gestión de Tecnologías de Información y Comunicación (TIC)

Las tecnologías de información y comunicación son un recurso crítico tanto para la operación de los procesos de la Agencia, como para el procesamiento, almacenamiento y transferencia de sus activos de información. Desde ahí, que la institución debe incorporar mecanismos de seguridad y ciberseguridad sobre la gestión tecnológica que aborden los aspectos de operación tecnológica propiamente tal, como aquellos aspectos relativos al desarrollo, actualización y adquisición de sistemas, de forma de mitigar los riesgos que puedan generar impactos adversos a la institución.

Para dar cumplimiento a estos principios, el SSI de la Agencia considera la operación de los siguientes controles:

a) Sobre la seguridad en la operación de las TIC:
    i. Manual para la seguridad de las operaciones TIC.
    ii. Manual para la gestión de controles criptográficos.
    iii. Manual para la protección contra código malicioso.
    iv. Procedimiento de control de cambios TIC.
    v. Procedimiento de respaldo de sistemas, software y cuentas de usuario.

vi. Procedimiento de gestión de vulnerabilidades.
vii. Procedimiento de mantención del equipamiento.

b) Sobre el desarrollo, actualización y adquisición de software:
   i. Manual de requisitos de seguridad para el desarrollo y adquisición de software.
   ii. Procedimiento de Gestión para el Desarrollo y Mantención de Software.

6.2.5. Principio de Gestión de Incidentes

Ante la inminente probabilidad de ocurrencia de un incidente de seguridad de información, se debe contar con los lineamientos y directrices necesarias para generar una adecuada y eficaz respuesta institucional que le permita contener, mitigar, responder y recuperarse minimizando los impactos que este tipo de sucesos puedan generar. Para dar cumplimiento a estas acciones, el SSI de la Agencia considera la operación de un Procedimiento de respuesta ante incidentes.

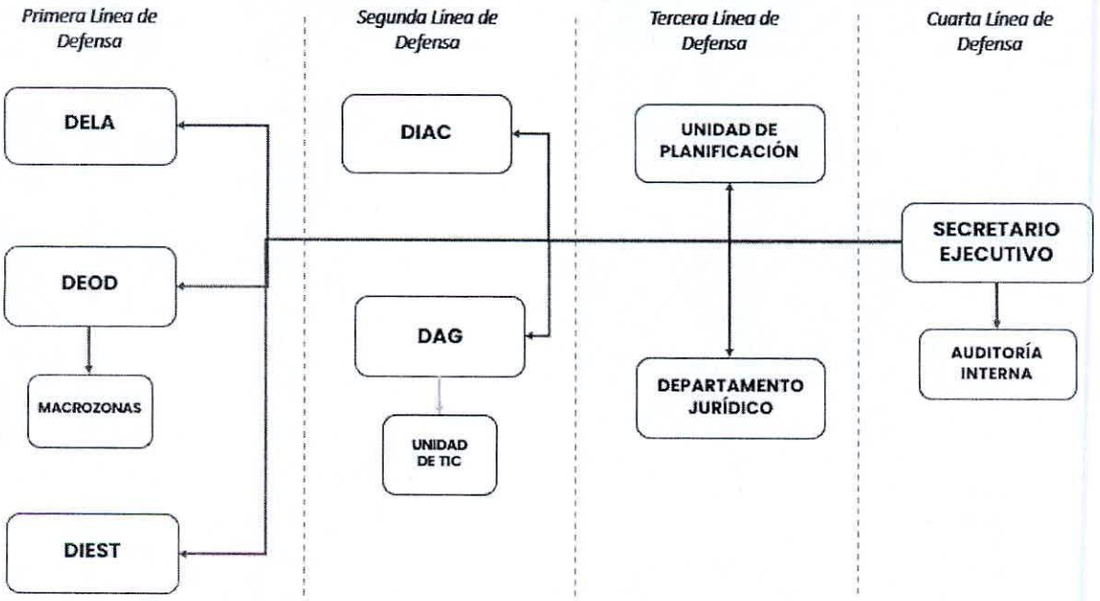
6.2.6. Principio de Revisión Independiente del SSI

Se establece la mejora continua del SSI como parte de los compromisos adquiridos por los Roles Administrativos de las cuatro (4) líneas de defensa que lo componen. Se define así que la ejecución de auditorías y revisiones independientes sobre el Sistema de Seguridad de la Información es una de las actividades más relevantes para que, de forma imparcial, se identifiquen aspectos de mejora que generen iniciativas para optimizar la mitigación de los riesgos de la Agencia en estas materias, así como los aspectos que pongan en riesgo la operación y cumplimiento de los objetivos del SSI.

De esta forma, para dar cumplimiento a este principio, la Agencia realizará revisiones independientes sobre el SSI al menos con periodicidad anual, las cuales pueden ser realizadas de forma interna o externa.

6.3. Estructura Funcional del SSI

Para la gobernanza y gestión efectivos de la seguridad de información y ciberseguridad a través del SSI, la Agencia establece una estructura funcional conformada por cuatro (4) líneas de defensa, las cuales serán conformadas a su vez por roles Ejecutivos, Administrativos, Operativos, de Equipo, Usuarios y/o Instancias, que, velando por mantener una correcta segregación de funciones, busca potenciar la operación del SSI. El Esquema de la estructura funcional es el siguiente:



Esquema 1. Estructura funcional institucional del SSI

6.3.1. Roles y Responsabilidades

La Primera y Segunda Línea de Defensa corresponden a la operación propiamente tal de la Agencia, donde la primera Línea estará conformada por las Divisiones DELA, DIEST y DEOD incluyendo Macrozonas, y se caracterizan por focalizar su operación en la recolección, generación y procesamiento de información y datos críticos para el cumplimiento de la misión de la Agencia. Así mismo, la Segunda Línea de Defensa estará conformada por las Divisiones DAG y DIAC, que focalizan su operación en la gestión de activos de información críticos generados por las Divisiones de Primera Línea para el cumplimiento de la misión de la Agencia. De esta forma, los roles y responsabilidades que componen estas líneas de defensa son los siguientes:

I.- Primera y Segunda Línea de Defensa.

a) **Jefaturas de División:** Deberán desempeñarse dentro de sus respectivas Divisiones, debiendo cumplir las siguientes responsabilidades:

i. Asumir el rol de Propietario de los Activos de Información involucrados en la operación de los procesos de la División.
ii. Asumir el rol de Dueño Funcional de los Sistemas y Aplicaciones que soportan la gestión de los activos de información y la operación de los procesos de la División.
iii. Asegurar la incorporación de la seguridad de información y ciberseguridad en la operación de la División, mediante la adopción y cumplimiento de las políticas, manuales y procedimientos del SSI.
iv. Facilitar las gestiones y apoyo necesarios, desde un enfoque Administrativo, para la mejora continua del SSI.
v. Garantizar la colaboración de su División con los procesos de auditoría interna y revisión independiente del SSI.
vi. Garantizar las gestiones, apoyo y participación necesarias para la implementación de soluciones tanto transitorias como de la causa raíz de no conformidades, incumplimientos, y potenciales eventos o incidentes de seguridad.
vii. Así mismo, aquellas Jefaturas de División de la Segunda Línea de Defensa, deberán establecer una comunicación fluida con las Jefaturas de División Primera Línea de Defensa, de forma de identificar aquellos activos de información críticos que son transferidos entre las Divisiones, para alinear los mecanismos de control necesarios para mantener su seguridad.

b) **Líder(es) Interno(s) del SSI:** Corresponde a las jefaturas de aquellos Departamentos, que poseen una mayor exposición al riesgo dada la criticidad de los activos de información que manejan. Se desempaña(n) como Rol(es) Operativo(s) de la Primera Línea de Defensa dentro del contexto de la División a la que pertenecen, debiendo cumplir con las siguientes responsabilidades:

i. Liderar desde la operación, así como apoyar a las demás jefaturas de departamento, en la incorporación de la seguridad y ciberseguridad en los procesos de la División mediante la adopción de los lineamientos propuestos en las políticas, manuales y procedimientos del SSI.
ii. Dada la visión transversal de la seguridad que tendrán estos roles, deberán apalancar la mejora continua del SSI mediante la detección de mejoras y posibles optimizaciones en las políticas, manuales y procedimientos que éste dispone.
iii. Ser la contraparte interna del SSI al interior de la División, de forma de canalizar requerimientos e iniciativas que apalanquen la mejora continua del mismo.

iv. Apoyar con una visión operativa y transversal de la División, en la implementación de soluciones tanto transitorias como de la causa raíz de potenciales no conformidades, eventos de seguridad, e incidentes de seguridad.
v. Así mismo, aquellos Líder(es) Interno(s) del SSI de la Segunda Línea de Defensa, deberán establecer una comunicación directa con los Líder(es) Interno(s) del SSI de las Divisiones del Primera Línea, de forma de generar un ambiente de control integral para la transferencia y acceso a la información crítica de éstas.

c) **Jefaturas de Departamento:** Desempeñan como Roles Operativos de la Primera y Segunda Línea de Defensa, debiendo cumplir con las siguientes responsabilidades:
i. Asumir el rol de Custodio de los Activos de Información involucrados en la operación de los procesos del Departamento.
ii. Asumir el rol de Administrador Funcional de los Sistemas y Aplicaciones que soportan la gestión de los activos de información y la operación de los procesos del Departamento.
iii. Asegurar la incorporación de la seguridad de información y ciberseguridad en la operación de su Departamento mediante la adopción y cumplimiento de las políticas, manuales y procedimientos del SSI.
iv. Facilitar las gestiones y apoyo necesarios, desde un enfoque Operativo, para la mejora continua del SSI.
v. Participar de forma activa en los proyectos de desarrollo, actualización y adquisición de sistemas y aplicaciones que involucren almacenamiento y/o procesamiento de los activos de información del Departamento, así como de aquellas que sean administradas por el Departamento.
vi. Tomar parte activa en el diseño e implementación de soluciones tanto transitorias como de la causa raíz de no conformidades, incumplimientos, y potenciales eventos o incidentes de seguridad.
vii. Establecer una comunicación directa con el o los Líder(es) Interno(s) del SSI para su División, de forma de apalancar la inclusión integral de la seguridad de información y ciberseguridad en la División.

II.- Segunda Línea de Defensa

a) **Jefatura de Unidad de TIC - DAG:** Corresponde a un operativo de la Segunda Línea de Defensa que lidera la gestión de las Tecnologías de Información y Comunicación (TIC) de la Agencia, y debe cumplir con las siguientes responsabilidades:
i. Velar por que la gobernanza de las TIC incluya de forma inherente la seguridad de información y ciberseguridad.
ii. Asumir el rol de Custodio Tecnológico de los Activos de Información de la Agencia que son gestionados a través de las TIC. De esta forma, todo cambio o nuevo proyecto tecnológico, deberá contar con la participación del Propietario y/o Custodio de los Activos de Información involucrados.
iii. Velar por una segregación de funciones efectiva en lo que respecta a la seguridad de las TIC.
iv. Asegurar la adopción y cumplimiento de las políticas, normas y procedimientos del SSI relacionados con la seguridad en las TIC, cuando la definición de roles y responsabilidades en cada documento lo especifique.
v. Mantener actualizados los procedimientos y manuales de seguridad de información que tengan directa relación con su ámbito de responsabilidad.

vi. Mantener la continuidad operativa de la infraestructura TIC de la Agencia.
vii. Delegar actividades y tareas con los equipos internos de la Unidad de TIC, garantizando el cumplimiento sobre lo dispuesto en las políticas, manuales y procedimientos del SSI, así como la mitigación de los riesgos asociados a la tecnología de la Agencia.
viii. Mantener la seguridad asociada a los procesos ejecutados por proveedores tecnológicos de la Agencia.
ix. Administrar y entregar cuando corresponda los Registros de Operación asociados al cumplimiento y correcta ejecución de los manuales y procedimientos del SSI.

b) **Equipos Internos Unidad de TIC – DAG:** Desde un ámbito operativo, se desempañan como Rol de Equipo de la Segunda Línea de Defensa dentro del contexto TIC, debiendo cumplir con las siguientes responsabilidades:
   i. Ejecutar de forma correcta lo dispuesto en las políticas, normas y procedimientos del SSI que tengan directa relación con el ámbito TIC de la Agencia, así como las actividades designadas por la Jefatura de Unidad TIC - DAG en este contexto.
   ii. Ejecutar las actividades necesarias para mantener la continuidad de los servicios tecnológicos de la Agencia.
   iii. Recolectar y custodiar los Registros de Operación de las normas y procedimientos del SSI que se encuentran bajo el ámbito de responsabilidades de la Unidad TIC.

III.- Tercera Línea de Defensa

Está conformada por los siguientes roles y responsabilidades:

a) Encargada de Seguridad de Información: Corresponde a un Administrativo y líder del SSI de la Agencia, cuyas responsabilidades son:
   i. Desarrollar y promover cambios y actualizaciones apropiadas sobre las políticas, normativas, y procedimientos de seguridad de información apropiados para la Agencia.
   ii. Liderar el proceso de gestión de riesgos de seguridad de información y ciberseguridad en la Agencia.
   iii. Proporcionar asesoría al Comité de Seguridad de Información y al Secretario Ejecutivo relacionadas con la seguridad de la información.
   iv. Coordinar iniciativas, actividades y proyectos transversales o focalizados que permitan apalancar la operación y mejora continua del SSI.
   v. Liderar el proceso de gestión y respuesta ante incidentes de seguridad de información y ciberseguridad.

b) Encargada de Ciberseguridad: Corresponde a un Rol Operativo y líder subrogante del SSI de la Agencia, cuyas responsabilidades son:
   i. Seguir las directrices de la Encargada de Seguridad de Información en lo que respecta a la operación y mejora continua del SSI.
   ii. Participar de forma activa en la ejecución del proceso de gestión de riesgos de seguridad de información y ciberseguridad de la Agencia.
   iii. Actualizar las políticas y los procedimientos del SSI conforme a la evolución de los riesgos y la periodicidad que éstos indican.
   iv. Proporcionar asesoría tanto a la Encargada de Seguridad de la Información como a los Líderes Internos del SSI y a las Jefaturas de Departamento de cada División, en temáticas referentes a la operación y mejora continua de las políticas, manuales y procedimientos del SSI.

v. Consolidar y administrar los Registros de Operación de las políticas, normas y procedimientos cuando aplique.

IV.- Cuarta Línea de Defensa

Está conformada por los siguientes roles y responsabilidades:

a) **Auditoría Interna:** Corresponde a un Rol Administrativo del SSI que forma parte de la Tercera Línea de Defensa, cuyas responsabilidades son las siguientes:
   a. Formular y ejecutar un calendario anual de auditoría de controles de seguridad de información y ciberseguridad.
   b. Ejecutar el plan antes mencionado, recopilando la evidencia necesaria para validar de forma ineludible la implementación de estos controles.

b) **Secretario Ejecutivo:** Corresponde al Jefe Superior del Servicio, y proporcionar orientación y apoyo de la Dirección para la seguridad de información, de acuerdo con los requisitos institucionales y con las regulaciones y leyes pertinentes.

c) **Comité de Seguridad de Información:** Corresponde a la máxima Instancia del SSI, cuya conformación será la siguiente:
   i. Secretario ejecutivo o quien este designe, quien presidirá las sesiones del comité.
   ii. Jefes(as) de División, o quien éstos designen.
   iii. Jefe/a del Departamento Jurídico, o quien ésta designe.
   iv. Encargado(a) de Seguridad de la Información, cargo al cual le corresponde liderar las sesiones
   i. Encargado de Ciberseguridad, llevando registro de las actas de las sesiones ordinarias y extraordinarias.

   De esta forma, las responsabilidades del Comité serán las siguientes:
   i. Sesionar de forma ordinaria al menos bimensualmente para realizar seguimiento tanto del funcionamiento del SSI, como de las iniciativas en curso asociadas a su mejora continua.
   ii. Realizar, al menos una vez al año, una revisión general y transversal al funcionamiento del SSI, haciendo seguimiento a la implementación y efectividad del ambiente de control de seguridad que posee la Agencia.
   iii. Aprobar y aplicar medidas de mejora que permitan una evolución apropiada del SSI, según la evolución tanto de la organización como de los riesgos que a ésta pudiesen afectar.
   iv. Aplicar las medidas que correspondan y sean necesarias para asegurar la continuidad operativa de los procesos críticos de la Agencia ante la concreción de un riesgo u ocurrencia de incidentes de seguridad.
   v. Aprobar en sesión las políticas, normas y procedimientos que comprometan mejoras, actualizaciones y nuevas implementaciones al SSI.

   El Comité de Seguridad de la Información podrá sesionar de forma extraordinaria, caso en el cual, la sesión puede ser convocada por el Encargado/a de Seguridad de la Información cuando lo estimen procedente, con sus respectivos controles de asistencia. En caso de ausencia, el Comité designará a un reemplazante para llevar a cabo dicha función.

   Los acuerdos a los que arribe el Comité quedarán documentados a través de actas de reunión llevadas a cabo por su secretaria/o, y serán adoptados por los miembros presentes en cada sesión. En caso de desacuerdo o empate, dirimirá el presidente.

   El Comité de Seguridad de la Información podrá, si así los estima, invitar a terceros a sus sesiones, quienes solo tendrán derecho a voz.

Finalmente, las diferentes líneas de defensa del SSI, y conforme la información entregada en el Anexo III de esta política, deberán tener contacto con diversos grupos de interés especiales de forma de apalancar la mejora continua del SSI.

6.3.2. Segregación de Funciones

Para asegurar el cumplimiento de las obligaciones relacionadas con la seguridad de la información y ciberseguridad en los perfiles de cargo que se indican, se considera parte integrantes de las responsabilidades de los cargos que se indican, las siguientes:

a) **Responsabilidad en Seguridad de la Información Transversal a todos los perfiles de cargo:** Corresponde a la definición de responsabilidad en estas temáticas a incorporar en la descripción de la totalidad de las responsabilidades del personal de la Agencia de Calidad de la Educación, cualquiera sea su vínculo contractual con el servicio, 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) **Responsabilidad en Seguridad de la Información para Jefaturas de División y de Oficinas Macrozonales, que corresponde** a 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 (SSIC). 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) **Responsabilidad en Seguridad de la Información para Jefaturas de Departamento/Unidad**, a saber:
"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 (SSIC). 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."

Será responsabilidad del Jefe(a) del Departamento de Gestión de Personas, dar a conocer esta responsabilidad al personal existentes, así como incorporarlos en los procesos de selección respectivos.

7. ANÁLISIS Y EVALUACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Política General de Seguridad de la Información deberá ser evaluada por el Comité de Seguridad de la Información al menos una vez al año o cuando se produzca un cambio o incidente significativo que la impacte, con la finalidad de revisar y evaluar su contenido y

orientación. Lo anterior, para asegurar la continua idoneidad, eficiencia y efectividad del Sistema de Seguridad de la Información.
Los cambios a la Política General de Seguridad de la Información serán aprobados por el Secretario Ejecutivo de la Agencia.

8. REVISIÓN DEL CUMPLIMIENTO DE LA POLÍTICA

Anualmente, y a través de auditorías, ya sean internas o externas, se revisará el cumplimiento de la presente Política General de Seguridad de la Información, con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento y mejora continua de la misma.

9. NO CONFORMIDADES E INCUMPLIMIENTOS

Los riesgos y no conformidades derivadas del incumplimiento o necesidad de mejora de los lineamientos establecidos en este documento deberán ser comunicados directamente tanto al Propietario y/o Custodio de los activos de información involucrados, como a las Encargadas de Seguridad de Información y Ciberseguridad, de forma de establecer e implementar las acciones correctivas necesarias.
Así mismo, cualquier evento o incidente de seguridad de la información, deberá ser canalizado según lo estipulado en el Procedimiento de Respuesta ante Incidentes de Seguridad (SSI-PRO-5.1).

10.COMUNICACIÓN DE LA POLÍTICA

La Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, deberá ser informada, mediante los canales de comunicación oficiales del servicio, a su personal y a todo aquel que tenga acceso a sus activos de información.

11.SANCIONES

Conforme a la ley 20.529, el personal de la Agencia deberá guardar absoluta reserva y secreto de las informaciones de las cuales tome conocimiento en el cumplimiento de sus labores, sin perjuicio de las informaciones y certificaciones que deba proporcionar de conformidad a la ley.

Asimismo, tendrá prohibición absoluta de prestar al as entidades sujetas a su evaluación otros servicios que los señalados en la ley, ya sea en forma directa o indirecta.

12. ANEXOS

12.1. Anexo I: Glosario del SSI

Se presenta los términos más utilizados en el SSI, para efectos de su cabal comprensión:

Activo de Información	Corresponde a la información como tal, independiente del formato o medio en el que se encuentre.
Acuerdo de Nivel de Servicio (SLA)	Un acuerdo de nivel de servicio (SLA, por sus siglas en inglés) corresponde a un convenio entre un proveedor de servicios y su cliente, en donde se definen compromisos para el servicio en cuestión, con respecto a su calidad, disponibilidad, entre otros campos.
Autenticación	Corresponde al proceso mediante el cual se verifica que alguien o algo es quien dice ser.
Autorización	Corresponde al proceso mediante el cual se define qué, cómo y cuándo un usuario autenticado puede acceder a las instalaciones / sistemas, o utilizar los recursos de la organización
Borrado Seguro (Wimping)	Proceso mediante el cual se sobrescribe varias veces cada segmento de la superficie del disco del equipo en cuestión con cadenas aleatorias de ceros y unos.
Cadena de Custodia	Secuencia de pasos y registros que evidencian una correcta manipulación de un activo de información o equipamiento.

Código Malicioso (Malware)	Software con fines maliciosos, como la vulneración de la confidencialidad, integridad y disponibilidad de los activos de información.
Configuration Manager Database (CMDB)	Herramienta utilizada para registrar las herramientas de hardware que la organización administra, lo cual facilita la gestión, asignación y mantención de los recursos tecnológicos de la institución.
Cuarta Línea de Defensa	Corresponde a los roles o instancias de más alto nivel en la institución asociada a la seguridad de información, cuya responsabilidad es hacer seguimiento y monitoreo del SSI de forma de apalancar la mejora continua con un enfoque estratégico.
Custodio de Activos de Información	Corresponde a un rol designado por el Propietario / Dueño de los Activos de Información, quien comúnmente es miembro de su equipo de trabajo y por ende participa en uno o varios procesos que lidera éste y sobre el cual se delega la ejecución de actividades de control cuya responsabilidad se mantiene asignada al Propietario / Dueño.
Custodio Tecnológico de los Activos de Información	Corresponde al rol responsable de la tecnología que soporta el almacenamiento y procesamiento de los activos de información de la Agencia.
CSIRT de Gobierno	Equipo de Gestión y Respuesta ante Incidentes de Ciberseguridad del Ministerio de Interior, Gobierno de Chile. Apoya en la implementación de la ciberseguridad en los organismos públicos, así como de colaborar en la respuesta ante incidentes.
Evento de Seguridad	Suceso que indica una posible brecha en la seguridad de la información o falla en el control de ésta.
Dueños Funcionales de Sistemas y Aplicaciones	Corresponde a los roles propietarios de los activos que gestiona, procesa y/o almacena un sistema o software de la Agencia.
Equipamiento o equipos	Corresponde al hardware utilizado para procesar, gestionar y/o almacenar activos de información críticos de la Agencia.
Equipos Resolutores	Corresponde a los equipos que ejecutan las actividades operacionales para la resolución de intermitencias, eventos e incidentes de seguridad de información.
Ethical Hacking	Proceso mediante el cual se emulan actividades maliciosas sobre la infraestructura tecnológica de la Agencia, de forma de identificar posibles brechas de seguridad que catalicen un incidente de seguridad.
Evento de Seguridad	Suceso que indica una posible brecha de seguridad de información o una falla en un control.
Factor(es) de Autenticación	Corresponde a los mecanismos utilizados para verificar que algo o alguien es efectivamente quien dice ser.
Grupos de Interés Especiales	Instituciones externas generadoras de información y/o conocimiento de interés para la operación y mejora del SSI, asociado al ámbito de responsabilidades propio de algún rol del SSI.
Incidente de seguridad	Uno o varios eventos de seguridad identificados que puedan vulnerar la confidencialidad, disponibilidad, integridad y/o privacidad de los activos de información de Agencia.
Indicador Clave del SSI	Corresponde a una métrica que indica si el funcionamiento de uno o varios controles de seguridad de información está de acuerdo a la tolerancia al riesgo institucional.
Información de Autenticación Secreta	Corresponde a la información que utilizan los usuarios para autenticarse en los sistemas de la Agencia. Ésta es de carácter personal e intransferible.
Inventario de Activos de Información	Corresponde al consolidado de Activos de Información clasificados según su criticidad en los ámbitos de confidencialidad, disponibilidad, integridad y privacidad.

Inventario de Sistemas	Corresponde al consolidado de sistemas informáticos de la Agencia que se encuentran en producción.
Medio de soporte extraíble	Corresponde a hardware utilizado para almacenar y transportar información. Incluyen más no se limitan a dispositivos USB, discos duros externos y CDs.
No Conformidades	Corresponde a fallas en la aplicación de procedimientos y/o manuales que ponen en riesgo el correcto funcionamiento del SSI.
Operación TIC	Procesos de ligados a la administración de la tecnología de información y comunicación (TIC) que soportan los procesos operacionales de la primera y segunda línea de defensa.
Perfil de Usuario	
Primer Factor de Autenticación	Corresponde a los métodos de autenticación basados en algo que el usuario sabe, como, por ejemplo, una contraseña o PIN de acceso.
Primera Línea de Defensa	Corresponde a las Divisiones de la Agencia que se focalizan su operación en la recolección, generación y procesamiento de información y datos críticos para el cumplimiento de la misión de la Agencia.
Propietario de Activos de Información	Corresponde a aquellos roles que son responsables de un conjunto de procesos específicos, y por ende de la seguridad de los Activos de Información que por éstos forman parte. Se asigna este rol a los roles de Jefatura de División. Puede delegar la ejecución de actividades asociadas a su rol de Dueño / Propietario de los Activos de Información de sus procesos en los denominados Custodios de los Activos de Información, pero no la responsabilidad que éstas conllevan.
Registro de Operación (RO)	Corresponde a la evidencia generada al momento de ejecutar un procedimiento o los lineamientos de una norma del SSI, y es utilizado para verificar su cumplimiento ante auditorías o solicitudes del regulador. Los Registros de Operación deben estar asociados a un Indicador de Seguridad de Información, de forma de apalancar la toma de decisiones basadas en riesgo.
Repudio	Es la acción de desconocer la generación, adición y/o eliminación sobre uno o varios activos de información.
Respaldo Completo	Es aquel que considera el respaldo de la totalidad de la información de interés para la Agencia. Incluye una copia de archivos de información de acuerdo con las extensiones de archivo que puedan contener información relevante para la Agencia, ofreciendo un respaldo por extensión de archivo sobre el perfil del usuario.
Respaldo Incremental	Copia los archivos creados o modificados desde la última copia de seguridad total (completa) o incremental.
Rol	Perfil de cargo de los
Roles Administrativos	Corresponden a los roles del SSI que se enfocan en las tareas asociadas con la Gestión de la Seguridad de Información y Ciberseguridad según lo delineado por los Roles Ejecutivos.
Roles Ejecutivos	Corresponden a los roles del SSI que se enfocan en las tareas asociadas con el Gobierno de la Seguridad de Información y Ciberseguridad.
Roles de Equipo	Corresponde a aquellos roles del SSI que tienen asignadas responsabilidades que deben ser llevadas a cabo por un grupo determinado y definido de Roles de Usuario.
Roles Operativos	Corresponden a los roles del SSI que ejecutan las actividades y tareas operativas para aplicar la seguridad de información, según lo delineado por los Roles Administrativos.
Segregación de Funciones	Corresponde a la distribución de las tareas y responsabilidades dentro de la Agencia, una División y/o un Departamento, mediante la cual se mitiga el conflicto de interés en la aplicación de controles de seguridad. Ejemplo de esto es la revisión cruzada de actividades, o la doble validación / autorización de acciones.

Segunda Línea de Defensa	Corresponde a las Divisiones de la Agencia que se focalizan su operación en la gestión de activos de información críticos generados por la Primera Línea de Defensa para el cumplimiento de la misión de la institución.
Segundo Factor de Autenticación	Corresponde a los métodos de autenticación basados en algo que el usuario tiene, como un código QR, token, o tarjeta de coordenadas.
Trabajo Remoto	El teletrabajo o trabajo remoto se refiere a todas las formas de trabajo fuera de la oficina, incluyendo entornos de trabajo no tradicionales tales como aquellos denominados "trabajo a distancia", "lugar de trabajo flexible", "trabajo en remoto" y "entornos virtuales de trabajo".
Tercer Factor de Autenticación	Corresponde a los métodos de autenticación basados en algo que el usuario es, como, por ejemplo, aspectos biométricos como la huella dactilar,
Tercera Línea de Defensa	Corresponde a los roles que lideran el SSI mediante la gestión de riesgos, implementación de controles y apoyo institucional para la incorporación de la seguridad de información y ciberseguridad en la Agencia.
Tiempo de Recuperación Objetivo (RPO)	El Tiempo de Recuperación Objetivo, o RPO por sus siglas en inglés para Recovery Time Objetive, es la expresión en unidades de tiempo, del máximo de información que se puede perder en caso de incidencia.
Usuario	Corresponde al personal de la Agencia, de planta o contrata, que por cumplimiento de su ámbito de responsabilidades, se le debe otorgar acceso a los sistemas de la Agencia.
Vulnerabilidad	Debilidad de diseño o implementación en sistemas y softwares, que de ser explotadas pueden comprometer la confidencialidad, integridad y disponibilidad de los activos de información.

12.2. Listado de legislación vigente para el SSI

1: Política de Seguridad de la Información.

D.S. N°83, 2005	Art. 11; Art. 37
D.S. N°93, 2006	Art.2
Ley N°19.799	Art. 7
Ley N°20.285	Art. 11; Art. 33; Art. Décimo
Ley N°20.529	Art. 35; Art. 41

2: Organización de la Seguridad de la Información.

D.S. N°83, de 2005	Art. 10; Art.12; Art. 37
D.S. N°93, 2006	Art.2
Ley N°19.223	Art. 4
Ley N°19.628	Art.7; Art.11
Ley N°19.799	Art. 9; Art.10; Art.11; Art.12; Art. 17; Art. 18; Art.21; Art. 23
Ley N°20.285	Art.3: Art.11; Art.16; Art. 20; Art.26; Art. 31; Art. 32; Art.33; Art.34; Art.35; Art.1 transitorio; Art. Décimo
Ley N°20.529	Art.41

3: Gestión de Activos.

D.S. N°83, 2005	Art.13; Art.14; Art.15; Art. 16; Art. 37
Ley N°19.880	Art.7; Art.18
Ley N°20.285	Art. 22; Art.23
Ley N°20.529	Art. 41

4: Control de acceso.

D.S. N°83, de 2005	Art.9: Art.18; Art.27; Art.28;Art.29; Art.30; Art.31; Art.32; Art.33; Art.37
Ley N°19.233	Art.1; Art.2; Art.3
Ley N°19.799	Art.1; Art.14; Art.15; Art.16
Ley N°20.529	Art.41

5: Seguridad de las comunicaciones.

D.S. N°83, 2005	Art.7; Art.10; Art.15; Art.22; Art.23; Art.24; Art.25; Art.26; Art.37
D.S. N°93, 2006	Art. 1; Art.2; Art.5; Art.6; Art.7; Art.9
Ley N°19.628	Art.4; Art.5; Art.12; Art.17; Art.18; Art.19; Art.20; Art.22
Ley N°19.799	Art.8; Art.12; Art.18; Art.19; Art.20; Art.23; Art.24
Ley N°19.880	Art.5; Art.14; Art.19; Art.30; Art.39; Art.46; Art.48; Art.58; Art.59; Art.64; Art.65
Ley N°20.285	Art.4; Art.5; Art.6; Art.7; Art.10; Art.12; Art.15; Art.35
Ley N°20.529	Art.11

6: Seguridad física y del medio ambiente.

D.S. N°83, 2005	Art.17; Art.18; Art.19; Art.26; Art.37
D.S. N°93, 2006	Art.4: Art.5
Ley N°19.799	Atr.17

7: Seguridad de las operaciones.

D.S. N°83, 2005	Art.7; Art.10; Art.15; Art.22; Art.23; Art.24; Art.25; Art.26; Art.37
D.S. N°93, 2006	Art.1; Art.2; Art.5; Art.6; Art.7; Art.9
Ley N°19.628	Art.4; Art.5; Art.12; Art.17; Art.18; Art.19; Art.20; Art.22
Ley N°19.799	Art.8; Art.12; Art.18; Art.19; Art.20; Art.23; Art.24
Ley N°19.880	Art.5; Art.14; Art.19; Art.30; Art.39; Art.46; Art.48; Art.58; Art.59; Art.64; Art.65
Ley N°20.285	Art.4; Art.5: Art. 6; Art.7; Art.10; Art.12; Art.15; Art.35
Ley N°20.529	Art.11

8: Criptografía.

D.S. N°83, 2005	Art.11; Art.25; Art.26
D.S. N°93, 2006	Art.2
Ley N°20.285	Art.11; Art.33
Ley N°20.529	Art.35; Art.41

9: Relaciones con proveedores.

D.S. N°83, 2005	Art.11
D.S. N°93, 2006	Art.2
Ley N°19.913	Art.3
Ley N°20.285	Art.11; Art.33
Ley N°20.529	Art.35; Art.41

10: Desarrollo, mantenimiento y adquisición de sistemas.

D.S. N°83, 2005	Art.26; Art.37
D.S. N°93, 2006	Art.2; Art.8
Ley N°19.223	Art.1; Art.2; Art.3; Art.4
Ley N°19.799	Art.17; Art.18; Art.19; Art.20
Ley N°20.285	Art.17
Ley N°20.529	Art.41

11: Continuidad del negocio.

D.S. N°83, 2005	Art.7; Art.35 Art.37
Ley N°19.799	Art.12; Art.16; Art.18
Ley N°19.880	Art.5; Art.19
Ley N°20.529	Art.41

12: Gestión de incidentes de seguridad de la información.

D.S. N°83, 2005	Art.12; Art.37
Ley N°19.628	Art.5; Art.23
Ley N°19.799	Art.5; Art.9; Art.13; Art.19
Ley N°19.880	Art.35
Ley N°20.285	Art.24; Art.25: Art.27; Art.28; Art.45; Art.46; Art.47; Art.49
Ley N°20.529	Art.35; Art.41

13: Seguridad de Recursos Humanos.

D.S. N°83, 2005	Art.20; Art.21; Art.37
D.S. N°93, 2006	Art.1; Art.2; Art.9
Ley N°19.223	Art.4
Ley N°19.628	Art.7
Ley N°19.799	Art.11; Art.12; Art.16; Art.17; Art.18; Art.20; Art.21; Art.23
Ley N°20.285	Art.35; Art. Décimo
Ley N°20.529	Art.41; Art.42; Art.44

14: Cumplimiento.

D.S. N°83, 2005	Art.7; Art.22
D.S. N°93, 2006	Art.2; Art.3; Art.8
Ley N°17.336	Art.3; Art.8; Art.18; Art.19; Art.24; Art.37 bis; Art.71 B; Art.71 Q; Art.71 M
Ley N°19.223	Art.1: Art.3; Art.4
Ley N°19.628	Art.1; Art.3; Art.4; Art.5; Art.6; Art.7; Art.9; Art.10; Art.11; Art.13; Art.15; Art.16; Art.18; Art. 20; Art.21; Art.23; Art. 1 trans; Art.2 trans.
Ley N°19.799	Art.1; Art.3; Art.6; Art.9; Art.12; Art.19; Art.23
Ley N°20.285	Art.7; Art.8; Art.11; Art.16; Art.20; Art.21; Art.33; Art. Quinto; Art. Sexto
Ley N°20.529	Art.9; Art.10; Art.11; Art.32; Art.35; Art.41; Art.42; Art.44; Art. Séptimo; Art. Octavo; Art. Noveno; Art. Décimo

II. Referencias Legales.

- D.S. N°83, de 2005, del Ministerio Secretaría General de la Presidencia, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

- Decreto Supremo N°93, de 2006, del Ministerio Secretaría General de la Presidencia, Aprueba Norma Técnica para la Adopción de Medidas Destinadas a Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos Masivos No Solicitados en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios.
- Ley N°17.336, sobre Propiedad Intelectual.
- Ley N°19.223, sobre Delitos Informáticos.
- Ley N°19.628, sobre Protección de la Vida Privada.
- Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha Firma.
- Ley N° 19.880, Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado.
- ley n°19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos.
- Ley N°20.285, sobre Acceso a la Información Pública.
- Ley N°20.529, Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización.

12.3. Anexo III: Contacto con grupos de interés especiales

De forma de aportar a la mejora continua del SSI, y al desarrollo de los roles en el ámbito de las responsabilidades mencionados en este documento, se listan a continuación Grupos de Interés Especiales con los cuales deben mantener contacto los roles del SSI como parte del cumplimiento de sus responsabilidades según muestra la siguiente tabla:

Grupo de Interés	Descripción	Rol SSI Receptor	Roles SSI Destinatarios
Fundación SOCHISI	Ejecución de charlas gratuitas y remotas de ciberseguridad y privacidad de datos.	- Encargada de Seguridad de Información. - Encargada de Ciberseguridad.	- Jefaturas de División. - Jefatura de Unidad de TIC.
CSIRT - GOB	Entrega de lineamientos asociados a la seguridad de información y ciberseguridad en el Estado de Chile.	- Encargada de Seguridad de Información. - Encargada de Ciberseguridad.	- Jefatura de Unidad TIC.
INCIBE	Entrega de boletines relativos a la seguridad de información y concientización de usuarios.	– Líder(es) Interno(s) del SSI de todas las Divisiones.	– Jefaturas de División - Jefaturas de Unidad y Departamento
Center of Internet Security (CIS) Newsletter	Información relacionada a la seguridad de las TIC y herramientas tecnológicas de seguridad.	Jefatura de Unidad TIC - DAG	- Equipos Internos Unidad de TIC
OWASP	Información relacionada con la inclusión de la seguridad de información y ciberseguridad en el desarrollo, actualización y adquisición de software.	Jefatura de Unidad TIC - DAG	– Equipo de Desarrollo de Software – Unidad de TIC

SEGUNDO: DÉJASE SIN EFECTO las Resoluciones Exentas N°s 589; 1024; 614 y 1620 de 2019 de la Agencia de Calidad de la Educación.

TERCERO: COMUNIQUESE por el Departamento de Gestión de Personas la presente resolución mediante correo electrónico a todo el personal y colaboradores de la Agencia de Calidad de la Educación.

CUARTO: COMUNIQUESE por parte de sus respectivas contrapartes técnicas, a todos los proveedores de la Agencia de Calidad de la Educación con contratos actualmente vigentes la presente resolución mediante correo electrónico.

PUBLÍQUESE la presente resolución en el Portal Transparencia.

REPUBLICA DE CHILE
Agencia de Calidad de la Educación
SECRETARIO EJECUTIVO

DANIEL RODRÍGUEZ MORALES
SECRETARIO EJECUTIVO
AGENCIA DE CALIDAD DE LA EDUCACIÓN

ASA/GCL/NJO

Distribución:

- División de Información a la Comunidad
- División de Evaluación y Logros del Aprendizaje
- División de Estudios
- División de Evaluación y Orientación de Desempeño
- Macrozonas Agencia de Calidad de la Educación
- Archivo