APRUEBA NUEVA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA DE CALIDAD DE LA EDUCACIÓN, Y DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 1440, DE 2014 QUE INDICA.

AGENCIA DE CALIDAD DE LA EDUCACION
16 MAY 2019
DOCUMENTO TOTALMENTE TRAMITADO

RESOLUCIÓN EXENTA Nº 0589

SANTIAGO, 16 MAY 2019

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, que crea el Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización; en el DFL N° 29, de 2004, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; 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 la Resolución N° 136, de 2013, de la Agencia; en la Resolución TRA 120441/1064/2016, de 2016, de la Agencia; en el Decreto Exento N° 48, de 2019, del Ministerio de Educación; y en la Resolución Nº 1.600, de 2008, de la Contraloría General de la República; y

CONSIDERANDO:

1° 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.

2° 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.

3° Que, la Agencia de Calidad de la Educación ha revisado su Politíca General de Seguridad de la Información vigente a la fecha respecto de la cual se ha estimado necesaria su revisión y actualización para el cumplimiento centralizado de uno de los indicadores del Programa de Mejoramiento de la Gestión (PMG), esto es, el relativo al cumplimiento de los controles de seguridad de la información implementados respecto del total definido en la norma NCH ISO 27001, y de aumentar de manera progresiva en el tiempo, los niveles de madurez de la institución, tanto, en materia de seguridad de la información, como de la ciberseguridad.

4° Que, en atención a lo ya expresado, el Comité de Seguridad de la Información de este Servicio, acordó, en sesión de 30 de abril de 2019, aprobar una nueva Política General de Seguridad de la Información de la Agencia de Calidad de la Educación.

RESUELVO:

PRIMERO: APRUÉBASE la nueva Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

"POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA DE CALIDAD DE LA EDUCACIÓN"

1.- DECLARACIÓN INSTITUCIONAL.

La Agencia de Calidad de la Educación, en adelante la Agencia, define su misión, siendo fiel a los objetivos establecidos en el Artículo 10 de la Ley 20.529, como: Evaluar tanto los logros de aprendizaje de los alumnos, como el desempeño de los establecimientos educacionales, con el objetivo de, tanto establecer un orden de éstos en función de los indicadores obtenidos, como de proporcionar información a la comunidad 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, como a nivel general, en cumplimiento con su rol de informador a la comunidad en las materias de su competencia.

Es así, como la Agencia reconoce la información como su activo de mayor relevancia, catalogándola como un elemento crítico de apoyo al cumplimiento de la Misión

Institucional, que por tanto, requiere ser protegida convenientemente (junto a los procesos y sistemas que la utilizan) frente a amenazas 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 establecerá un proceso, el cual, velará 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 fortalecerá 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, autenticidad y privacidad de los activos de información institucionales relevantes o claves para la operación de la organización. Esto, operará a través de la implementación de un Sistema de Gestión de la Seguridad de la Información y la Ciberseguridad a nivel institucional, en adelante SGSIC, que permita aumentar de manera progresiva en el tiempo, los niveles de madurez de la organización en 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.

3.- MARCO GENERAL: SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN.

Dadas las facultades que apalancan el cumplimiento de la Misión Institucional, detalladas en el Artículo 11 de la ley 20.529, la Agencia comprende que su actividad central es la manipulación de datos e información propia confidencial, y/o datos e información 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 desiciones 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 SGSIC.

Para dar cumplimiento a la aplicación de esta política, la Agencia deberá identificar y mantener actualizados permanentemente:

1. 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.
2. 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.
3. 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.

4. 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 cúales son los activos de información más críticos para la Agencia, y por que procesos fluyen durante la ejecución de la operación de la institución.
5. 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.
6. 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.
7. 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:
    a) Seguridad de la información y ciberseguridad de los recursos humanos.
    b) Gestión de activos de información.
    c) Gestión del riesgo de los activos de información.
    d) Establecimientos de mecanismos y medidas de protección sobre los activos de información.
    e) Establecimientos de mecanismos y buenas prácticas de seguridad de la información, relacionadas con el proceso de desarrollo y/o adquisición de software y tecnología.
    f) Gestión de vulnerabilidades y remediación de brechas.
    g) Establecimientos de mecanismos y medidas de monitoreo sobre los activos de información e identificación de posibles incidentes.
    h) Establecimiento de mecanismos y medidas de contención y respuesta frente a incidentes.

i) Establecimiento de mecanismos y medidas de recuperación y vuelta a la normalidad de los procesos y sistemas frente a posibles incidentes.

j) 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.

8. En base al punto anterior, la Agencia deberá implementar un gobierno, 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. Este gobierno, se deberá establecer en base a la determinación y asignación de roles definidos para tales efectos. Por lo tanto, la Agencia incorporará 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.

Junto con lo anterior, la Agencia contará con una estructura funcional del SGSIC, la cual considerará:

a) Comité de Seguridad de la Información.

b) Encargado(a) de Seguridad de la Información.

Las responsabilidades y funciones de esta estructura se encontrarán descritas en una resolución de creación y nombramiento exenta.

4.- OBJETIVOS ESPECÍFICOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

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) **Autenticidad**, la Agencia deberá verificar por la aplicación de los controles necesarios para resguardar los activos de información que no pierdan sus

características de validez y uso asegurando el no repudio de ésta. Resguardando la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser.

e) ***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.

5.- 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 aprobadas por el Secretario Ejecutivo de la Agencia.

6.- REVISIÓN DEL CUMPLIMIENTO DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

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.

7.- COMUNICACIÓN DE LA PRESENTE POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN A LA INSTITUCIÓN Y A TERCEROS.

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.

8.- 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 a las entidades sujetas a su evaluación otros servicios que los señalados en la ley, ya sea en forma directa o indirecta.

Las infracciones a esta norma serán consideradas falta grave para efectos de exigir responsabilidad administrativa, la que se exigirá con independencia de la responsabilidad civil o penal que pudiera configurarse.

SEGUNDO: DÉJASE SIN EFECTO la Resolución Exenta N° 1440, de 2014, de este servicio, que dejó sin efecto la Resolución Exenta N° 666, de 26 de julio de 2013, así como cualquier otro acto administrativo de este servicio en donde figure alguna referencia a la Resolución Exenta N° 1440, de 2014,de la Agencia de la Calidad de la Educación.

TERCERO: DIFÚNDASE el presente acto administrativo al personal de la Agencia de Calidad de la Educación y a todo aquel quien tenga acceso a sus activos de información.

ANÓTESE Y PUBLíQUESE EN EL PORTAL DE TRANSPARENCIA

AGENCIA DE CALIDAD DE LA EDUCACIÓN Secretario Ejecutivo (S)

JUAN BRAVO MIRANDA
SECRETARIO EJECUTIVO (S)
AGENCIA DE CALIDAD DE LA EDUCACIÓN

ASA/SHS/MSG/CAB/GCB/BGP/MLG/CCL/DBL

Distribución:
- Divisiones (5)
- Secretaría Ejecutiva
- Unidad de Planificación
- Departamento de Auditoria
- Oficina de Partes