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

**APRUEBA ACTUALIZACIÓN DE PROCEDIMIENTO DE RESPUESTA ANTE INCIDENTES**

**RESOLUCIÓN EXENTA N°** 585

**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 la Resolución N°1338, de 2019, de la Agencia de Calidad de la Educación; en el Memorándum N°83, de 2019, del Secretario Ejecutivo de la Agencia de Calidad de la Educación; 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°218, de 2021 que aprueba medidas y procedimientos de datos personales; en la Resolución N°7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del Trámite de Toma de Razón, y

**CONSIDERANDO:**

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

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

Que, por Resolución Exenta N°1338, de 16 de octubre de 2019, del Servicio, se aprobó la Política de Gestión de Incidentes de la Agencia de Calidad de la Educación.

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 la regulación vigente se consagra el principio de gestión de incidente, conforme al cual, ante la inminente probabilidad de ocurrencia de un incidente de seguridad de la información, se debe contar con los lineamientos y directrices necesarias para agendar

una adecuada y eficaz respuesta institucional que permita contener, mitigar, responder y recuperarse, minimizando los impactos que este tipo de sucesos puedan generar. Asimismo, para el cumplimiento de tales acciones se contempla la operación de un procedimiento sobre la materia.

Que, teniendo en cuenta lo expuesto, corresponde aprobar la actualización del procedimiento de respuesta ante incidentes de la Agencia de Calidad de la Educación, dejando sin efecto la regulación vigente sobre la misma materia.

**RESUELVO:**

**PRIMERO**: **APRUEBASE,** la actualización de procedimiento de respuesta ante incidentes de la Agencia de Calidad de la Educación, cuyo texto es el siguiente:

## 1. OBEJTIVO

Establecer los lineamientos, criterios y flujo procedimental para una coherente y eficaz gestión de incidentes de seguridad de información y ciberseguridad.

## 2. ALCANCE

Este procedimiento debe ser aplicado ante cualquier evento adverso, sea de tipo evento o incidente, que ponga en riesgo la confidencialidad, disponibilidad, integridad y privacidad de los activos de información de la Agencia, así como los datos personales de terceros de los cuales la institución es responsable.

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.06.01.03 – Contacto con autoridades.

b) ISO/IEC 27.001:2013, Control A.16.01.01 – Responsabilidades y procedimientos.

c) ISO/IEC 27.001:2013, Control A.16.01.02 – Informe de eventos de seguridad de información.

d) ISO/IEC 27.001:2013, Control A.16.01.04 – Evaluación y decisión sobre eventos de seguridad.

e) ISO/IEC 27.001:2013, Control A.16.01.05 - Respuesta ante incidentes de seguridad.

f) ISO/IEC 27.001:2013, Control A.16.01.06 – Aprendizaje de los incidentes de seguridad.

## 3. NORMAS Y REFRENCIAS

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 6.2.5 relativo al principio de gestión de 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) Memorándum N°83, de 26 de diciembre de 2019, del Secretario Ejecutivo de la Agencia de Calidad de la Educación.

## 4. TÉRMINOS Y DEFINICIONES

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

## 5. ROLES Y RESPONSABILIDADES

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

## 6. LINEAMIENTOS DEL PROCEDIMIENTO

Los lineamientos entregados en esta sección del procedimiento abarcan los siguientes aspectos generales y transversales para la gestión y respuesta ante incidentes de seguridad:

a) Detección y notificación de incidentes y eventos.

b) Evaluación y decisión sobre incidentes y eventos de seguridad.

c) Comunicación y respuesta ante incidentes y eventos de seguridad.

d) Recuperación ante incidentes de seguridad.

### 6.1. Lineamientos para Detección y Notificación de Incidentes o Eventos

Todos los usuarios de la Agencia, sin importar el rol que posean al interior de esta o dentro del SSI, así como si son internos o externos, serán responsables de notificar de forma inmediata las debilidades y brechas que puedan poner en riesgo la disponibilidad, integridad, confidencialidad y/o privacidad de los activos de información críticos de la institución.

La notificación de una brecha o debilidad debe hacerse de la forma más rápida y eficiente posible para disminuir el tiempo en que la organización puede gestionarlas y responder si así corresponde, así como incluir al propietario de los activos de información, encargada de seguridad de información, encargada de ciberseguridad, y Jefatura de Unidad de TIC - DAG si así corresponde, usando los siguientes medios de comunicación:

a) Correo electrónico institucional.

b) Notificación telefónica.

c) Notificación verbal.

Así mismo, la notificación debe ser lo más completa y específica posible en cuanto a información se refiere, de forma de facilitar la evaluación y posterior decisión que deben tomar los roles respectivos.

En caso de que la brecha o debilidad notificada sea declarada como incidente de seguridad crítico, la Encargada de Seguridad de Información o la Encargada de Ciberseguridad deberán notificar al CSIRT de Gobierno como autoridad para soportar a la Agencia en estos casos, siguiendo los lineamientos que éste ha dispuesto. Para lo anterior se deben utilizar los siguientes medios de comunicación:

d) Correo electrónico: soc@interior.gob.cl

e) Notificación telefónica: +56 2 2486 3850

f) Notificación mediante sistema del CSIRT: https://www.csirt.gob.cl/

## 6.2. Evaluación y Decisión sobre Eventos e Incidentes de Seguridad

Para tomar una decisión efectiva sobre las acciones a seguir frente a una notificación de evento o incidente, se debe realizar un análisis del alcance que ésta puede tener, donde se debe evaluar al menos lo siguiente:

a) Taxonomía, según la tabla del Anexo 1 de este documento.

b) Cantidad de equipos y/o usuarios afectados.

c) Sistemas e infraestructura tecnológica afectada.

d) Analizar un evento de seguridad como una posible acción que responde a un conjunto de otros eventos o brechas, no necesariamente de ocurrencia simultánea, de forma de identificar si éste es un suceso aislado o puede ser parte de una cadena de actividades maliciosos que conformen un ciberataque en contra de la Agencia, caso en el cual el evento debe ser declarado incidente de seguridad críticos de forma inmediata para proceder a su respuesta.

Se debe definir el alcance del impacto que pueda tener el posible evento o incidente de seguridad, para lo cual se establecen los siguientes criterios:

| NIVELES DE IMPACTO | DESCRIPCIÓN | MODO DE ACTUACIÓN |
|---|---|---|
| **CRÍTICO** | La notificación corresponde a un evento que es parte de un conjunto de eventos de seguridad que ponen en riesgo la operación de la Agencia y/o los activos de información críticos de la Primera Línea de Defensa. | Debe ser tratado como incidente de seguridad crítico. |
| **MUY ALTO** | La notificación corresponde a un evento que es parte de un conjunto de eventos de seguridad que ponen en riesgo la operación de la Agencia y/o los activos de información críticos de la Segunda Línea de Defensa. | Debe ser tratado como incidente de seguridad crítico. |
| **ALTO** | La notificación corresponde a un suceso aislado que pone en riesgo la operación de la Agencia y/o sus activos de información críticos, sean estos de la Primera o la Segunda línea de Defensa. | Debe ser tratado como incidente de seguridad. |
| **BAJO** | La notificación corresponde a un suceso aislado que supone una brecha de seguridad o falla en un control de seguridad que afecta activos de información y/o procesos críticos de la Agencia. | Debe ser tratado como evento de seguridad. |
| **INSIGNIFICANTE** | La notificación corresponde a un suceso aislado que supone una brecha de seguridad o falla en un control de seguridad que no afecta ni activos de información ni procesos críticos de la Agencia. | Debe ser tratado como evento de seguridad. |

### 6.3. Comunicación y Respuesta ante Eventos e Incidentes de Seguridad

Una vez determinado el modo de actuación en base al impacto y alcance del evento o incidente, se deben tener las siguientes consideraciones para su comunicación y posterior respuesta:

a) Comunicación y respuesta ante eventos de seguridad:

   i. Como se muestra en la tabla anterior, los eventos de seguridad serán aquellas brechas o debilidades cuyo impacto de carácter INSIGNIFICANTE O BAJO.
   ii. La respuesta a los eventos de seguridad no considera la notificación al CSIRT de Gobierno.
   iii. Los eventos de seguridad deben ser comunicados a los Custodios de los Activos de Información afectados y al Líder Interno del SSI respectivo, así como a los Administradores de los Sistemas afectados. Esto de forma de coordinar las medidas necesarias para su respuesta y solución.
   iv. La respuesta a los eventos de seguridad debe considerar un tiempo no mayor a 2 meses posterior a la notificación del mismo.

b) Comunicación y respuesta ante incidentes de seguridad:

   i. Como se muestra en la tabla anterior, los incidentes de seguridad serán aquellas brechas o debilidades cuyo impacto de carácter ALTO o superior.
   ii. La respuesta a los incidentes de seguridad debe contemplar al CSIRT de Gobierno sólo si éstos son declarados incidentes de seguridad de alta criticidad.
   iii. Los incidentes de seguridad deben ser comunicados de forma inmediata a los Propietarios de los Activos de Información afectados y los Líderes Internos del SSI respectivos, así como a los Dueños Funcionales de los Sistemas afectados. Esto de forma de coordinar las medidas necesarias para su contención, respuesta y recuperación en el menor tiempo posible.
   iv. En caso de incidentes de seguridad de alta criticidad, se debe convocar una sesión extraordinaria del Comité de Seguridad de Información.
   v. La respuesta a los incidentes de seguridad debe ser inmediatas de forma que su contención y posterior recuperación sea en el menor tiempo posible.

### 6.4. Recuperación ante Incidentes de Seguridad

Se considerará como fase de recuperación, el momento en el cual el incidente ya fue contenido y las acciones de respuesta ya fueron aplicadas, es decir, cuando los activos de información y operación de la Agencia se encuentren fuera de riesgo.

La recuperación de un incidente de seguridad debe considerar:

a) La validación de que los sistemas afectados se encuentran nuevamente en operación normal. Esto considera que se debe haber ingresado la información eventualmente recolectada o generada de forma manual, de forma de minimizar la pérdida de información que pudo haber significado el incidente.
b) La validación de que los controles de seguridad se encuentren nuevamente operativos.

Así mismo, para dar cierre formal a un incidente o evento, se debe actualizar la información de éstos en la planilla de registro de incidentes que se muestra en el Anexo 2 de este documento, de forma de generar información de valor que permita a la

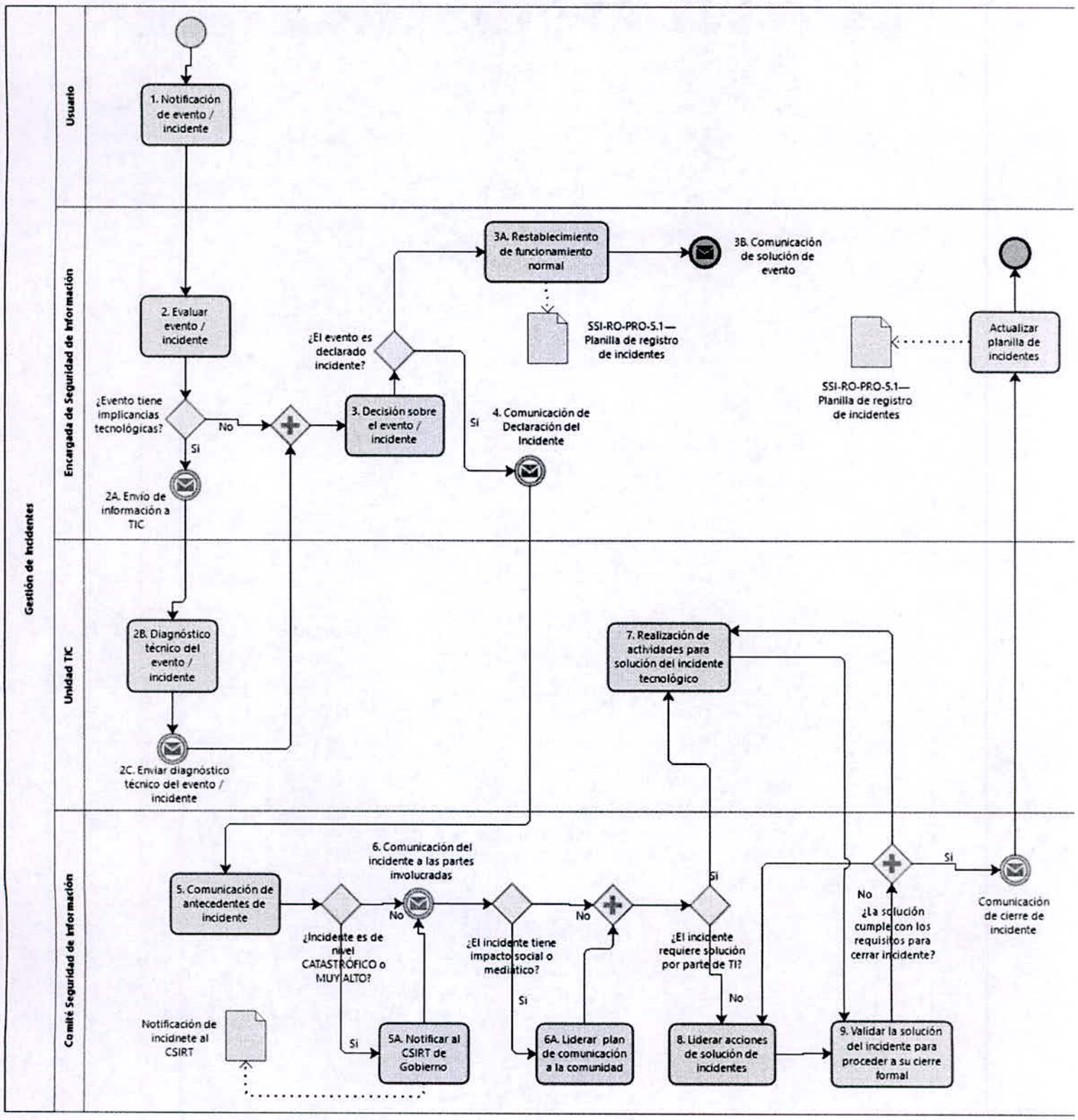
organización aprender de lo ocurrido, así como definir las mejoras o iniciativas para que éstos no se vuelvan a generar.

## 7. MODO DE OPERACIÓN

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

a) Procedimiento de Respuesta ante Incidentes.

## 7.1. Flujo de Procedimiento para Respuesta ante Incidentes



## 7.2. Matriz de Procedimiento para Respuesta ante Incidentes

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

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

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

### 7.3. Matriz de Responsabilidades

A continuación, se presenta la matriz RECIE del procedimiento bajo la siguiente nomenclatura:

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

| ID | ACTIVIDAD | COMITÉ SI | UNIDAD TIC | ENC. SI | DUEÑO ACTIVO | USUARIO |
|---|---|---|---|---|---|---|
| 1 | Notificación de evento / incidente | - | I | I | I | R/E |
| 2 | Evaluar evento / incidente | - | I | R/E | C | C |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2A | Envío de información a TIC | - | I | R/E | C | C |
| 2B | Diagnóstico técnico del evento / incidente | - | R/E | C | C | C |
| 2C | Enviar diagnóstico técnico del evento / incidente | - | R/E | I | I | I |
| 3 | Decisión sobre el evento / incidente | I | I | R/E | I | I |
| 3A | Restablecimiento de funcionamiento normal | - | R/E | I | - | - |
| 3B | Comunicación de solución de evento | - | R/E | I | I | I |
| 4 | Comunicación de Declaración del Incidente | I | I | R/E | I | I |
| 5 | Comunicación de antecedentes de incidente | R | C | E | C | - |
| 5A | Notificar al CSIRT de Gobierno | R | I | E | I | - |
| 6 | Comunicación del incidente a las partes involucradas | R/E | I | I | I | I |
| 6A | Liderar plan de comunicación a la comunidad | R/E | C | C | C | - |
| 7 | Realización de actividades para solución del incidente tecnológico | R | E | C | I | - |
| 8 | Liderar acciones de solución de incidentes | R/E | C | C | C | - |
| 9 | Validar la solución del incidente para proceder a su cierre formal | R/E | C | C | C | - |
| 10 | Comunicación de cierre de incidente | R/E | I | I | I | I |
| 11 | Actualizar planilla de incidentes | I | I | R/E | I | - |

## 8. REGISTROS DE OPERACIÓN

| INFORMACIÓN DEL REGISTRO | DESCRIPCIÓN |
|---|---|
| **NOMBRE** | SSI-RO-PRO-5.1—Planilla de registro de incidentes. |
| **MANUAL / PROCEDIMIENTO** | Respuesta ante incidentes |
| **CONTROLES ISO 27.001** | • A.06.01.03 – Contacto con autoridades.<br>• A.16.01.01 – Responsabilidades y procedimientos.<br>• A.16.01.02 – Informe de eventos de seguridad de información.<br>• A.16.01.04 – Evaluación y decisión sobre eventos de seguridad.<br>• A.16.01.05 - Respuesta ante incidentes de seguridad.<br>• A.16.01.06 – Aprendizaje de los incidentes de seguridad |
| **RESPONSABLE** | Encargada de Seguridad de Información |
| **DESCRIPCIÓN** | Corresponde a la información del incidente que debe ser llenada en la planilla del RO. |
| **FRECUENCIA** | En función de la ocurrencia de eventos / incidentes. |
| **ALMACENAMIENTO** | Digital – Google Drive del responsable |

## 9. ANEXOS

### 9.1. Anexo 1: Tabla para Clasificación de Eventos e Incidentes según su Taxonomía

| Tabla de Clasificación de Incidentes según Taxonomía | | |
|---|---|---|
| **N°** | **Clase de Incidente** | **Tipo de Incidente** |
| **1** | Contenido Abusivo | Pornografía Infantil - Sexual - Violencia |
| | | Spam |
| **2** | Código Malicioso | Malware y Virus |
| **3** | Recopilación de Información | Scanning |
| | | Sniffing |
| | | Ingeniería Social |
| **4** | Intentos de Intrusión | Intentos de acceso |
| | | Explotación de vulnerabilidades conocidas |
| | | Nueva Firma de Ataque |
| **5** | Intrusión | Compromiso de Cuenta Privilegiada |
| | | Compromiso de Cuenta sin privilegios |
| | | Compromiso de Aplicación |

| | | |
|---|---|---|
| **6** | Disponibilidad | Ataque de denegación de servicio (DoS / DDoS) |
| | | Sabotaje |
| | | Intercepción de información |
| **7** | Información de seguridad de contenidos | Acceso no autorizado a la información |
| | | Modificación no autorizada de la información |
| **8** | Fraude | Phishing |
| | | Derechos de Autor |
| | | Uso no autorizado de recursos |
| | | Falsificación de registros |
| | | Generación y/o utilización de certificados maliciosos |
| **9** | Vulnerable | Sistemas y/o softwares desactualizados |
| **10** | Reportes de Seguridad | Uso no autorizado de administración de sistemas |
| | | Explotación de fallas de software |
| | | Ataque fuerza bruta |
| | | Hombre del medio /Secuestro de sesión |
| | | Inyección de red |
| | | Errores de configuración |
| **11** | Solicitud | Solicitud de Información |
| **12** | Otros | Fuga de información |
| | | Manipulación de Información |
| | | Cross-site scripting (XSS) |

### 9.2. Anexo 2: Campos mínimos que debe contener la planilla para registro de incidentes/eventos de seguridad

La planilla de registro de incidentes debe considerar los siguientes campos:

a) Notificación: Indica el origen de la notificación.

b) Fecha y hora de notificación.

c) Taxonomía: Debe ser llenado en base a los criterios del Anexo 1.

d) Impacto: Indica el impacto asignado al momento de evaluar el suceso. Se deben usar los criterios definidos en este documento.

e) Clasificación: Define si el suceso se abordó como evento o incidente.

f) Descripción: Se debe entregar la mayor información posible del incidente / evento y cómo la Agencia respondió e éste.

g) Controles comprometidos: se debe identificar qué controles de la Agencia fallaron o dieron pie para el evento / incidente. En este punto se debe indicar el documento asociado (Políticas, manuales y procedimientos).

h) Procesos / activos involucrados.

i) Fecha / hora de cierre: corresponde a la fecha y hora en la cual se dio por cerrado el evento / incidente según lo indicado en este documento.

j) Solución: Descripción de las medidas ejecutadas para la solución del evento / incidente.

k) Compromiso de solución definitiva: Describe las actividades o iniciativas a seguir para solucionar la causa raíz del evento o incidente.

l) Compromiso de mejora: Describe los compromisos adoptados por la organización para abordar la solución definitiva del evento / incidente.

**SEGUNDO: DÉJASE SIN EFECTO** la Resolución Exenta N°1338, 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 las jefaturas de las Divisiones y Macrozonas de la Agencia de Calidad de la Educación.

**CUARTO**: **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**

ASA/GCL/NSO/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