Gobierno de Chile

LPC/NOC/JSR/JJG/RVL/BRE

MINISTERIO DE EDUCACION
22 NOV 2021
DOCUMENTO TOTALMENTE TRAMITADO

**APRUEBA POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE EDUCACIÓN.**

Solicitud N° 5799

**SANTIAGO,**

**RESOLUCIÓN EXENTA N°** 5904

**VISTO:** 22.NOV2021

Lo dispuesto en la Ley N° 18.956, que Reestructura el Ministerio de Educación; en la Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; en la Ley N° 17.336, de Propiedad Intelectual; en la Ley N° 19.223 que Tipifica Figuras Penales Relativas a la Informática; en la Ley N° 19.628, sobre Protección de la Vida Privada; en el D.F.L N° 29 de 2004, del Ministerio de Hacienda, que fija el texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en el D.F.L N° 1-19.653, de 2000 del Ministerio Secretaría General de la Presidencia que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración; en el Decreto 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 Resolución Exenta N° 296 de 19 de enero de 2021 que Aprueba la Nueva Política de Seguridad de la Información del Ministerio de Educación y Define las Labores del Órgano Encargado de Velar por su Cumplimiento; en el Decreto Exento N° 1.122 de 2018, que Aprueba la Política de Gestión de Incidentes de Seguridad de la Información para el Ministerio de Educación; en el Memorándum N° 21 del 2021 del Encargado de Seguridad de la Información y, en la Resolución N° 7, de 2019, de Contraloría General de la República.

**CONSIDERANDO:**

Que, en conformidad a lo dispuesto en la Ley N° 18.956 de 1990, que Reestructura el Ministerio de Educación, esta Cartera es la encargada, entre otras funciones, de fomentar el desarrollo de la educación en todos sus niveles.

Para apoyar su cumplimiento, el Ministerio de Educación, ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y produce el almacenaje de datos, mediante diferentes dispositivos, que permiten interactuar tanto con los funcionarios en todo el país, como con la comunidad escolar y la ciudadanía en general.

Que, mediante la Resolución Exenta N° 296 de 19 de enero de 2021, de Educación, se aprobó la "Política de Seguridad de la Información para la Subsecretaría de Educación, y Define las Labores del Órgano Encargado de Velar por su Cumplimiento". Por su parte, mediante la Resolución Exenta N° 4.503, de 11 de julio de 2014, de esta Subsecretaría de Educación, se estableció la función del Encargado de Seguridad de la Información.

Que, esta Subsecretaría reconoce que la información que posee es un bien estratégico para sus funciones, por lo que se requiere que sea protegida tanto en su obtención, como en su proceso, transmisión y almacenamiento.

Que, para cumplir tanto con esta política, como con la obligación que tiene esta Subsecretaría, en orden a proporcionar un marco estándar enfocado en la protección de la seguridad de dicha información, es que se hace necesario Renovar la Política de Gestión de Incidentes de Seguridad de la Información, debido a que la anterior ha cesado su vigencia, según Memorándum N° 21, del año 2021, del Encargado de Seguridad de la Información.

Que, mediante Decreto N° 1.122 de 2018 del Ministerio de Educación, se aprobó la Política de Gestión de Incidentes de Seguridad de la Información, la cual tendría una vigencia de 3 años, según lo establecido en la misma.

Que, en mérito de lo anterior y acorde al lineamiento que deriva de la Política de Seguridad de la Información mencionada, se establece mediante este acto una nueva Política de Gestión de Incidentes de Seguridad de la Información, elaborada por el Encargado de Seguridad de la Información.

**RESUELVO:**

**1.Apruébase** la "Política de Gestión de Incidentes de Seguridad de la Información" del Ministerio de Educación, cuyo texto y sus anexos, se adjuntan al presente acto y se entienden forman parte integrante del mismo.

**2.Déjase constancia**, que la "Política de Gestión de Incidentes de Seguridad de la Información para el Ministerio de Educación" aprobada mediante Decreto Exento N° 1122 de 2018 del Ministerio de Educación, será reemplazada por la que se adjunta, en atención a que ha cesado la vigencia de la anterior.

**ANÓTESE, COMUNÍQUESE Y ARCHÍVESE**


**JORGE POBLETE AEDO**
**SUBSECRETARIO DE EDUCACIÓN**

Distribución:
- Of. Partes
- Gabinete Sr. Ministro
- Gabinete Sr. Subsecretario
- División de Educación Superior
- División de Educación Parvularia
- Coordinación Nacional de Tecnología
- División Jurídica
- División de Administración General
- Archivo
- Exp. N° 27.463

Gobierno de Chile

# POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

## Ministerio de Educación

| Elaborado por: | Revisado Por: | Aprobado por: |
|---|---|---|
| NOMBRE: **Juan Antonio Serrano** | NOMBRE: **Wanda Viera Andrade** | NOMBRE: **León Paul** |
| CARGO: **Encargado de Seguridad de la Información** | CARGO: **Coordinador Nacional de Tecnología** | CARGO: **Presidente Comité de Seguridad de la Información** |

## 1. DECLARACIÓN INSTITUCIONAL

El Ministerio de Educación, MINEDUC en adelante, en conformidad a lo dispuesto en la Ley N°18.956 de 1990, que reestructura este Ministerio, es la Secretaría de Estado encargada, entre otras funciones, de fomentar el desarrollo de la educación en todos sus niveles.

Para apoyar el cumplimiento de sus funciones, el MINEDUC ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes activos de Información, los que permiten el trabajo conjunto de los funcionarios en todo el país, y su interacción con la comunidad escolar y con la ciudadanía en general, en aras del cumplimiento de las funciones que le han sido encomendadas y le competen.

Así, la información que se encuentra en poder de esta Subsecretaría de Educación es un bien estratégico para sus funciones, por lo que se requiere que sea protegida tanto en su obtención, procesamiento, transmisión y almacenamiento. Por lo tanto, el personal que integra la organización será responsable de velar por su confidencialidad, integridad y disponibilidad según lo que su cargo y función le corresponda administrar y gestionar, de conformidad al marco legal actualmente vigente.

En este orden de ideas y, con el fin de apoyar la organización de la seguridad de la información, esta Cartera de Estado aprobó mediante Rex 296 del 19 de enero del 2021 la "Nueva Política de Seguridad de la Información y define las labores del órgano encargado de velar por su cumplimiento". Por su parte, por la Resolución Exenta N° 4.503, de 11 de julio de 2014, de esta Subsecretaría de Educación, estableció la función de Encargado de Seguridad de la Información.

En este orden de ideas, y acorde al lineamiento que deriva de la Política de Seguridad de la Información antes referida, se establece por este acto la Política de Gestión de Incidentes de Seguridad de la Información.

## 2. OBJETIVO

El objetivo de la presente política es proporcionar un marco estándar enfocado en la protección de la seguridad la información orientada a la gestión de incidentes de seguridad de la información, proceso constituido por los siguientes subprocesos o etapas:

- Preparación para enfrentar incidentes de seguridad.
- Detección, reporte y clasificación del incidente.
- Respuesta y resolución del incidente.
- Mejora continua de la gestión de incidentes de seguridad.

## 3. ALCANCE

La Política de Gestión de Incidentes de Seguridad de la Información, aplica a todos los funcionarios del Ministerio de Educación, ya sean funcionarios de planta, contrata, honorarios y externos que presten servicios a esta Cartera de Estado.

Esta política aplica a todo tipo de incidente de seguridad que afecte el normal funcionamiento o uso de activos de información del Ministerio de Educación, afectando la confidencialidad, integridad o disponibilidad de la información.

Asimismo, es aplicable a todo activo de información que la organización posea actualmente o en el futuro, cubriendo prioritariamente aquellos que están asociados a procesos de provisión de los productos estratégicos de la institución (Formulario A1 de definiciones estratégicas, que efectúa trienalmente la Dirección de Presupuestos y que se encuentra disponible en la Intranet Ministerial).

## 4. POLÍTICA

### 4.1. Responsabilidades

4.1.1. Encargado de Seguridad de la Información:

a) Establecer los procedimientos necesarios para asegurar una respuesta oportuna, sistemática y eficaz frente a los incidentes de seguridad de la información.

b) Mantener actualizada la presente política, controlar su implementación y velar por su correcta aplicación.

c) Entregar las orientaciones para el debido reporte de los incidentes de seguridad por el personal de la Institución.

Luego del cierre del incidente, el Encargado de Seguridad debe organizar las siguientes acciones:

- Solicitar a las partes aplicar lecciones aprendidas y ajuste de procedimientos y mecanismos de comunicación.
- Preparar un informe ejecutivo al Comité de Seguridad de la Información según corresponda a su magnitud indicando causales e impacto del incidente.

4.1.2. Jefe de la Coordinación Nacional de Tecnologías

Disponer lo necesario para que la CNT de solución a los incidentes de seguridad informática que afecten a algún activo de información y restablecer la entrega de los servicios.

4.1.3. Encargado de Soporte y Mesa de Ayuda

a) Registrar, clasificar y derivar los eventos o incidentes de seguridad detectados y reportados por personal del Ministerio.

4.1.4. Jefaturas de Área de la CNT

Velar por el correcto cumplimiento de esta Política.

4.1.5. Funcionarios(as)

Reportar cualquier incidente de seguridad de la información o evento que pueda desencadenar un incidente.

## 4.2. Lineamientos

### 4.2.1. Preparación para enfrentar incidentes de seguridad

Este subproceso incluye todas las actividades de tipo proactivo que puedan llevarse a cabo para evitar incidentes y responderlos si es que ocurren. El área responsable de su gestión es Seguridad de la Información. Algunas actividades para realizar son:

a) Gestión de riesgos de Seguridad de la Información.

b) Auditorías técnicas sobre servicios e infraestructura tecnológica.

c) Revisiones de Seguridad de la Información sobre procesos y activos de información. Las Revisiones de seguridad pueden ser referidas a un control o grupos específicos de controles, por ejemplo, cumplimiento de normativa (políticas y procedimientos), cumplimiento de contratos relacionados con mantención o gestión de activos de información

d) Actividades de sensibilización y entrenamiento

### 4.2.2. Reporte de eventos e incidentes de seguridad

En caso de que alguna persona que está dentro del alcance de esta política observe un incidente de seguridad de la información o una situación que pueda desencadenar un incidente, tiene la responsabilidad de informar inmediatamente a Mesa de Ayuda, correo electrónico mesa.ayuda@mineduc.cl, o los canales establecidos para estos efectos.

Se debe concientizar a los usuarios acerca de la importancia de reportar cualquier evento o incidente del que tenga conocimiento.

Además, se impartirán instrucciones y orientaciones a todos los funcionarios acerca de los mecanismos formales para reportar los eventos e incidentes de seguridad.

En la medida de lo posible, se debe evitar que se realicen acciones sin apoyo técnico.

En el caso de que se detecten incidentes de seguridad por efecto de monitoreo, revisiones de seguridad o por inspección técnica, es responsabilidad del área técnica que lo detecte, informar de inmediato según el procedimiento establecido.

### 4.2.3. Registro, clasificación y derivación

El incidente deberá registrarse según el procedimiento definido y clasificarse según el tipo y nivel de criticidad.

En esta fase se debe asignar a algún(as) área(s) la responsabilidad de realizar el diagnóstico, análisis, contención, investigación, para una adecuada gestión y pronta resolución del incidente.

Dependiendo de la magnitud e impacto, se debe informar del incidente al Comité de Seguridad de la Información, Directivos y/o Autoridad, según corresponda,

### 4.2.4 Análisis y diagnóstico

Según el tipo de incidente y nivel de criticidad se deben adoptar las acciones inmediatas correspondientes para contener el daño y mitigar riesgos.

Se debe recopilar la mayor cantidad posible de información acerca del incidente, con el fin de que efectuar un diagnóstico adecuado.

Si se estima necesario, se debe realizar una reunión de relevamiento, análisis y evaluación con todos los referentes e involucrados en el incidente.

Se debe, además, proteger la evidencia, tal como registro de logs, capturas de pantalla, archivos u otros.

Cuando sea necesario se debe iniciar gestiones para notificar a División Jurídica, a fin de que realice la denuncia correspondiente a PDI u otros organismos externos.

### 4.2.5. Comunicación con CSIRT de Gobierno

En el caso de incidentes de ciberseguridad, dependiendo de la magnitud e impacto, estos se deben reportar al Equipo de Respuesta a Incidentes de Seguridad Informática

(CSIRT) vía correo electrónico a csirt@interior.gob.cl o según los mecanismos que disponga dicha entidad.

### 4.2.6. Investigación y Resolución

La investigación y resolución del incidente la realizará un área técnica que puede ser Gestión de Proyectos, Desarrollo, Mantención Evolutiva y Operaciones según corresponda. En la situación de que la falla sea a nivel de alguna plataforma administrada por Operaciones, esta área deberá investigar y resolver.

En cualquier caso, el registro de estado de avance y resolución del incidente es responsabilidad del área que realiza la investigación y resolución. El registro debe contener los siguientes aspectos:

- Acciones inmediatas
- Causas del incidente
- Forma de solución
- Horas de inicio y término cada actividad
- Medios de evidencia

Se deben documentar las acciones realizadas.

La resolución se realizará de acuerdo a los procedimientos específicos definidos para cada caso.

### 4.2.6 Comunicación a usuarios

Durante el desarrollo del incidente debe realizarse una adecuada comunicación a las áreas usuarias, la cual debe estar a cargo del Jefe de Proyecto responsable del servicio ante el usuario, el Jefe de la Coordinación Nacional de Tecnologías o instancia superior según el procedimiento establecido para estos efectos.

### 4.2.7. Análisis de causa e informe de cierre

En esta etapa se debe realizar un análisis de causa del incidente y elaborar un informe de cierre que contenga, al menos:

- los activos afectados,
- impacto,
- causas del incidente,
- acciones realizadas,
- solución y
- lecciones aprendidas.

Se debe preparar un Informe ejecutivo al Comité de Seguridad de la Información, Directivos y/o Autoridad, según corresponda, dependiendo de la magnitud e impacto del incidente.

### 4.2.8. Mejora continua de la gestión de incidentes.

El proceso de mejora continua agrupa todas las actividades que serán organizadas por parte de Seguridad de la Información, con el fin de mejorar la postura de seguridad ante futuras situaciones de incidencia. Actividades de este subproceso son:

- Revisión del cierre del incidente.
- Determinación de patrones de ocurrencia por periodo de tiempo, tipo de servicio, área responsable del servicio y áreas que se ven afectadas por el incidente.
- Implementación de controles que eviten la ocurrencia de incidentes similares en el futuro. Por ejemplo, ajustar o desarrollar procedimientos y/o políticas.

## 5. VIGENCIA

Las revisiones de la presente Política se realizarán cada tres años, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad del Servicio. Todo el personal del Ministerio de Educación deberá tomar conocimiento por

escrito de la presente política, la cual se encontrará en formato electrónico en la Intranet para futuras consultas.

## 6. LEGISLACIÓN VIGENTE

- Ley N° 17.336, de Propiedad Intelectual, y sus actualizaciones
- Ley N° 19.223, que Tipifica Figuras penales relativas a la Informática.
- D.F.L. N° 29 de 2004, que fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo.
- Ley N° 19.628, sobre Protección de la Vida Privada.
- Ley N° 19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.
- Ley N° 20.285, sobre Acceso a la Información Pública.
- Decreto Supremo N° 14 del 2014 Ministerio de Economía, Fomento y Reconstrucción que Modifica Decreto N° 181, de 2002, que aprueba reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica,
- Decreto Supremo N° 83 del 2005 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.
- Norma Chilena NCh-ISO27001:2013 sobre "Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos".

## 7. ACCIONES DISCIPLINARIAS.

La infracción a las obligaciones establecidas en este documento eventualmente podría constituir una violación al principio de probidad administrativa, en cuyo caso será sancionada en conformidad a lo dispuesto en el D.F.L. N° 29, de 2004, del Ministerio de Hacienda, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834,

sobre Estatuto Administrativo. Lo anterior, sin perjuicio de la responsabilidad civil o penal que pudiera concurrir.

Por su parte y, respecto del personal a honorarios o de carácter externo a MINEDUC, la infracción a las obligaciones materia del presente instructivo podría, eventualmente, constituir una infracción a su respectivo contrato, acarreando las consecuencias jurídicas del caso.

## 8. GLOSARIO DE TERMINOS

Para los propósitos de esta Política, las siguientes palabras se entenderán en el sentido que a continuación se indica:

**Activo**: Cualquier elemento que tenga valor para la organización. Para el ámbito de seguridad de la información, se puede clasificar en:

a) **Activos de Información**: Se entenderá por Activo de Información todo elemento en que se registre, en que se almacene y/o procese datos e información, sea a través de medios tecnológicos o no, tales como: bases de datos y archivos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, plan de continuidad de negocio, información de auditorías, información archivada, activos de software, activos físicos y servicios.

b) **Activos de Software**: Constituidos por las aplicaciones de software, Software de sistemas y Herramientas de desarrollo y utilidades.

c) **Activos Físicos**: Constituidos por el equipamiento computacional, Equipamiento de comunicaciones, Medios móviles y otros equipamientos.

d) **Servicios**: Servicios de computación y comunicaciones. Utilidades generales (ej. electricidad, luz, aire acondicionado, etc.)

e) **Personas**: Constituidos por los usuarios, que utilizan la estructura tecnológica, el área de comunicaciones y que gestionan la información.

f) **Intangibles**: Constituidos por los activos referidos a la reputación e imagen de la institución.

g) **Computador**: Equipo PC de escritorio, Computador portátil Tipo Notebook o Netbook, Servidores.

h) **Puesto de Trabajo:** Escritorio, oficina, mesón de atención etc.

i) **Malware:** Virus, troyano, gusano, programa malicioso.

j) **Antivirus:** Son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominados malware).

k) **Virus:** Son programas informáticos que se ejecutan normalmente sin el consentimiento del legítimo propietario y que tienen la característica de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la información

l) **Troyano:** Se denomina troyano (o caballo de Troya, *traducción más fiel* del inglés Trojan horse aunque no tan utilizada) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona, pero sin afectar al funcionamiento de ésta.

m) **Spyware:** Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

n) **Spam:** Correo electrónico basura o no deseado.

o) **Hackers:** es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones que utiliza sus técnicas para atacar otro PC

p) **Denegación de Servicio:** Caída de servicio de cualquier índole debido a algún incidente de Seguridad.

**Confidencialidad**: Garantía de que accedan a la información sólo aquellas personas autorizadas a hacerlo.

**Integridad**: Mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.

**Disponibilidad:** Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

**Evento de seguridad de la información:** una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de medidas de seguridad o una situación desconocida que pueda ser relevante para la seguridad. Un evento de seguridad de la información no es necesariamente una ocurrencia maliciosa o adversa, pero un evento de seguridad sí se puede transformar en un incidente de seguridad.

**Incidente de seguridad de la información:** un evento o situación que compromete la seguridad de un activo de información en sus aspectos de confidencialidad, integridad y disponibilidad. También se puede considerar como incidente la violación o amenaza *inminente* implícita o explícita a una política de seguridad de la información.

Entiéndase por Incidente de Seguridad:

- Robo o pérdida de información sensible
- Robo y pérdida de notebook, netbook o similar con información sensible
- Denegación de servicio sobre equipos de networking, afectando la operación diaria del Ministerio de Educación.
- Denegación de servicio por el ingreso y propagación de virus y amenazas que explotan vulnerabilidades
- Sabotaje Corporativo a través de modificaciones de programas por parte del personal interno que generó problemas de disponibilidad en servicios críticos (programa troyano)
- Amenazas y denuncias falsas a través de mensajes de correo electrónico anónimo
- En resumen cualquier tipo de incidente que afecte el correcto funcionamiento de las tecnologías de información de Mineduc.