Ministerio de Educación

Gobierno de Chile

APRUEBA POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Solicitud N° 9501

SANTIAGO, 31 JUL 2025

RESOLUCIÓN EXENTA N° 9589

VISTO:

Lo dispuesto 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 del Estado; en el D.F.L 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°18.956, que Reestructura el Ministerio de Educación; en la Ley N°21.459, que establece Normas sobre Delitos Informáticos, deroga la Ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest; en la Ley N°19.628, sobre Protección de la Vida Privada; 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°20.285, sobre Acceso a la Información Pública; en la Ley N°21.663, Marco de Ciberseguridad; en el Decreto N°83, de 2004, 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 el Decreto N°7, de 2023, del Ministerio Secretaría General de la Presidencia, que Establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme la Ley N°21.180; en la Resolución Exenta N°2.693, de 2023, del Ministerio de Educación, que Aprueba Política de Seguridad de la Información del Ministerio de Educación y Define las Labores del Órgano Encargado de Velar por su Cumplimiento; en la Resolución Exenta N°4.877, de 2024, del Ministerio de Educación, que Designa a Responsable Institucional de Seguridad de la Información y Ciberseguridad y a Responsable Institucional de Activos de la Información; y, en la Resolución N°36, de 2024, de la Contraloría General de la República.

MINISTERIO DE EDUCACIÓN
09 MAR 2026
DOCUMENTO TOTALMENTE TRAMITADO

CONSIDERANDO:

Que, esta Secretaría de Estado, en conformidad a lo dispuesto en el artículo 1°, de la Ley N°18.956, que Reestructura el Ministerio de Educación (Mineduc), tiene a su cargo entre otras funciones, el fomentar el desarrollo de la educación en todos sus niveles. .

Que, el referido cuerpo legal en su artículo 5 establece que la Subsecretaría de Educación es el órgano de colaboración directa del (de la) Ministro(a), y le corresponderá, en general, la administración interna del Ministerio y la coordinación de los órganos y servicios públicos del sector, y el cumplimiento de las demás funciones que en materias de su competencia le encomiende la ley y el Ministro. Por su parte, el inciso primero del artículo 6 indica que el (la) Subsecretario(a) es el (la) colaborador(a) inmediato(a) del (de la) Ministro(a) y el (la) Jefe(a) Administrativo del Ministerio, teniendo a su cargo la coordinación de las Subsecretarías que componen el Ministerio.

Que, con la finalidad de cumplir esas funciones, la Subsecretaría de Educación ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes activos, que permiten interactuar con la comunidad escolar, la ciudadanía en general y los integrantes de esta repartición en todo el país, para dar cumplimiento a las funciones que el mandato legal exige, considerando que la información resguardada puede ser propia de los sistemas de esta Cartera de Estado, de los servicios o sus procesos, así como también de los usuarios internos o externos.

Que, por su parte, estos datos son un bien estratégico para sus funciones, por lo que se requiere que sean protegidos tanto en su obtención, procesamiento, transmisión y almacenamiento; deber que incluye al personal que integra la organización, toda vez que será responsable de velar por su confidencialidad, integridad y disponibilidad según lo que su cargo y función le corresponda.

Que, en este contexto, es pertinente definir los requerimientos a establecer, implementar, mantener y mejorar de manera continua, regulando un sistema de gestión de la seguridad de la información dentro de esta Cartera de Estado.

Que, mediante la Resolución Exenta N°2.693, de 2023, de la Subsecretaría de Educación se aprobó la Política de Seguridad de la Información del Ministerio de Educación y definió las labores del órgano encargado de velar por su cumplimiento.

Que, en la Resolución señalada se establecen los principios y marco general de trabajo de esta Cartera de Estado, para administrar, mantener, sensibilizar, monitorear y revisar el Sistema de Seguridad de la Información (SGSI) acorde a las definiciones estratégicas, la misión y objetivos estratégicos institucionales, asegurando la confidencialidad, integridad y disponibilidad de los activos de la información, a través de su adecuada implementación, asignación de roles, funciones y responsabilidad.

Que, el mismo acto administrativo, señala en el punto 5. "Gestión de la Seguridad de la Información y ciberseguridad", que esta Subsecretaría de Educación mantendrá una organización para la gestión de la seguridad de la información, lo cual implica, dentro de otras materias, establecer directrices de carácter general, las que están destinadas a servir de guía para la definición de normas específicas que se contendrán en las disposiciones complementarias de carácter administrativo y técnico, que se dicten para su cumplimiento.

Que, a su vez, se define como Incidente de ciberseguridad todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.

Que, son ejemplos de un incidente de ciberseguridad: robo o pérdida de un equipo que almacena información; robo o pérdida de documentación sensible; filtraciones de datos; denegación de servicio sobre equipos de red y comunicaciones; fallas graves en sistemas informáticos institucionales; ingresos no autorizados a los sistemas de información; y cualquier evento que impida el acceso o dañe los sistemas de almacenamiento de información relevante del Ministerio.

Que, conforme a lo anterior, atendida la normativa vigente y sus disposiciones en esta materia, resulta necesario establecer la política de gestión de incidentes de seguridad de la información mediante el presente acto administrativo:

RESUELVO:

ARTÍCULO ÚNICO: APRUÉBASE la Política de Gestión de Incidentes de Seguridad de la Información:

"POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN"

1. DECLARACIÓN INSTITUCIONAL

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

Por su parte, la Subsecretaría de Educación es el órgano de colaboración directa del (de la) Ministro(a), y le corresponderá, en general, la administración interna del Ministerio, correspondiéndole así al (a la) Subsecretario(a) ser el (la) Jefe(a) Administrativo de la Cartera de Estado en comento.

Para apoyar el cumplimiento de sus deberes, ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes activos, los que permiten el trabajo conjunto de los funcionarios en todo el país, 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, los datos que se encuentran en poder de esta repartición pública son un bien estratégico para sus funciones, por lo que se requiere que sean protegidos tanto en su obtención, como en su procesamiento, transmisión y almacenamiento. Por lo tanto, el personal que integra la organización será responsable de velar por su confidencialidad, integridad y disponibilidad de acuerdo con lo que según su cargo y función le corresponda administrar y gestionar, de conformidad al marco legal actualmente vigente.

Luego, con el fin de apoyar su organización, mediante la Resolución Exenta N°2.693, de 2023, de este origen, se aprobó una Nueva Política de Seguridad de la Información, junto con las definiciones de las labores del órgano encargado de velar por su cumplimiento.

En este orden de ideas y acorde al lineamiento que deriva de la política antes referida, es necesario establecer 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 de la información, orientada a la gestión de los incidentes asociados a la misma. Proceso constituido por las siguientes etapas:

- Preparación para enfrentar incidentes de seguridad.
- Detección y comunicación.
- Contención.
- Resolución del incidente.
- Actividad post incidente de seguridad.

3. ALCANCE

La Política de Gestión de Incidentes de Seguridad de la Información, es aplicable a la totalidad de las personas que se relacionan con el Ministerio de Educación y que tengan acceso a estos activos, sean estos funcionarios(as) de planta, contrata o personal a honorarios, incluyendo a su vez a los(as) asesores(as), consultores(as), practicantes y, en general, toda aquella persona natural o jurídica que preste servicios y se vincule al Ministerio de Educación. Por tal razón, las políticas establecidas en este documento deberán ser de conocimiento y cumplimiento obligatorio para todos(as) a quienes se les otorgue acceso a estos activos, por el motivo que sea.

A su vez, es aplicable 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) y a aquellos priorizados por el Comité de Seguridad de la Información de la Subsecretaría de Educación.

4. DOCUMENTOS RELACIONADOS:

a. Política de Seguridad de la Información.

b. Política de Continuidad del Servicio.

c. Política de Seguridad de la Información en la relación con proveedores.

d. Procedimiento de respuesta a incidentes de seguridad de la información.

5. POLÍTICA

5.1. Roles y responsabilidades

5.1.1. Encargado(a) de Seguridad de la Información:

a. Establecer los lineamientos necesarios para asegurar una gestión oportuna, sistemática y eficaz frente a los incidentes de seguridad de la información, definiendo marco, estrategia, política y proponiendo planes de respuesta.

b. Mantener actualizada la presente política, controlar su implementación y velar por su correcta aplicación, y definir y actualizar metodologías para los planes de respuesta a incidentes.

c. Notificar al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), dependiente de la Agencia Nacional de Ciberseguridad (ANCI) de acuerdo a la normativa vigente.

d. Apoyar y monitorear la respuesta a incidentes y su recuperación.

e. Informar acerca de los incidentes de seguridad al Comité de Seguridad, y según la criticidad de los mismos, solicitar a la División Jurídica la evaluación de acciones judiciales.

f. Solicitar a las partes involucradas en un incidente aplicar las lecciones aprendidas, que se ajuste el procedimiento y los mecanismos de comunicación, así como revisar el informe relacionado al incidente.

g. Actuar como contraparte de la ANCI.

5.1.2. Coordinador(a) Nacional de Tecnología:

a. Disponer en forma oportuna lo necesario para que la Coordinación Nacional de Tecnología (CNT) prepare, detecte, comunique, contenga, resuelva y realice actividades post incidentes de seguridad informática que afecten a algún activo de información. Por lo dicho, debe:

   i. Preparar y gestionar la respuesta y recuperación frente a incidentes de ciberseguridad, de acuerdo con la política y los planes de respuesta establecidos, coordinando con personal interno, áreas usuarias y servicios de terceros.

   ii. Analizar, monitorear y gestionar la información de amenazas, eventos e incidentes de ciberseguridad.

   iii. Asegurar el resguardo de evidencia de incidentes de ciberseguridad y gestionar las actividades de peritaje informático cuando sea requerido.

   iv. Gestionar información de eventos e incidentes en base de conocimiento.

   v. Gestionar que los inventarios de activos técnicos dentro del alcance de esta política se encuentren actualizados.

5.1.3. Encargados(as) de área de la CNT:

a. Recibir, registrar y derivar los eventos o incidentes de seguridad detectados y reportados por personal del Ministerio.

b. Colaborar en la respuesta de incidentes según su ámbito de competencia.

5.1.4. Encargado(a) Técnico(a) de CNT:

a. Definir las áreas técnicas necesarias en el CSIRT de la Subsecretaría de Educación.

b. Apoyar en el proceso de respuesta y recuperación de incidentes de seguridad de la información y ciberseguridad.

5.1.5. Encargado(a) de Operaciones de la CNT:

a. Facilitar antecedentes técnicos del incidente al Equipo de Seguridad Operacional de CNT.

b. Ejercer como contraparte técnica de CNT.

c. Solucionar incidentes de seguridad, normalizar la entrega de servicios, registrar, analizar y evaluar el escalar a otras instancias como especialistas de otros organismos de gobierno o de proveedores.

5.1.6. Equipo de Seguridad Operacional de CNT:

a. Reunir e informar los detalles del incidente al Encargado de Seguridad para reportar a CSIRT Nacional dentro del periodo indicado en la normativa.

5.1.7. Equipo de Soporte y Mesa de Ayuda de la CNT:

a. Recibir, registrar y derivar los eventos o incidentes de seguridad detectados y reportados por personal del Ministerio, en el Nivel Central.

b. Apoyar en acciones relativas a la gestión de incidentes, tales como acciones técnicas requeridas en los equipos de usuario final, en el Nivel Central.

5.1.8. Coordinador(a) Regional de Informática (CRI):

a. Recibir, registrar y derivar los eventos o incidentes de seguridad detectados y reportados por personal del Ministerio, en la Seremi de Educación respectiva.

b. Apoyar en acciones relativas a la gestión de incidentes, tales como acciones técnicas requeridas en los equipos de usuario final, en la Seremi de Educación respectiva.

5.1.9. Jefe(a) de la División Jurídica (o a quién el(ella) designe):

a. Evaluar las acciones jurídicas y legales a ejecutar en caso de que ocurra un incidente de seguridad de la información.

5.1.10. Encargado(a) de Comunicaciones de la Subsecretaría de Educación:

a. Definir y gestionar la comunicación institucional en caso de un incidente de alto impacto.

5.1.11. Equipo de Respuesta a Incidentes de Seguridad de la Información y Ciberseguridad (CSIRT de la Subsecretaría de Educación):

a. Equipo de funcionarios/as de la CNT establecido para el manejo de incidentes, constituido por el(la) Encargado(a) Técnico, el Encargado(a) de Operaciones y el Equipo de Seguridad Operacional.

5.1.12. Proveedor(a):

a. En caso de detectar vulnerabilidades e incidentes que pueden afectar a las redes y sistemas informáticos del Ministerio de Educación, debe notificarlo con el fin de prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; la modalidad de reporte se realizará según los niveles de servicio y mecanismos señalados en el contrato, y cuando esto no estuviere definido, lo notificará a la contraparte técnica designada en el plazo máximo del día siguiente hábil, respetando en todo momento la posible naturaleza delicada de la información compartida.

5.1.13. Funcionarios(as):

a. Reportar cualquier incidente de seguridad de la información, evento o anomalía que pueda desencadenar un incidente, y colaborar en la entrega de la información requerida por parte del Encargado de Seguridad o de la Coordinación Nacional de Tecnología a fin de responder al incidente.

5.2. Lineamientos generales

5.2.1. Preparación para enfrentar incidentes de seguridad

Este subproceso incluye todas las actividades de tipo proactivo que puedan llevarse a cabo para evitar incidentes y responder si es que ocurren. Algunas actividades a 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 cuales pueden referirse a un control o grupos específicos de controles, como por ejemplo el cumplimiento de la normativa (políticas y procedimientos) y el cumplimiento de contratos relacionados con mantención o gestión de activos de información.

d. Actividades de sensibilización y entrenamiento.

e. Establecer roles, responsabilidades y procedimientos para una respuesta efectiva en caso de incidente.

f. Realizar actividades de prueba.

5.2.2. Detección y Comunicación

5.2.2.1. Detección y comunicación del Incidente:

En caso de que alguna persona que se encuentre 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 de la CNT, a través del correo electrónico mesa.ayuda@mineduc.cl o de los canales establecidos para estos efectos. Mesa de Ayuda notificará con prontitud al CSIRT de la Subsecretaría de Educación.

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

En cualquier caso, se debe evitar el realizar acciones sin apoyo técnico.

5.2.2.2. Reporte de incidente a CSIRT Nacional del Ministerio de Seguridad Pública:

Si el nivel de afectación del incidente puede tener efectos significativos en los servicios tecnológicos, se debe reportar al CSIRT Nacional de acuerdo con los mecanismos que haya dispuesto dicha entidad, tan pronto sea posible y en un plazo máximo de tres horas desde que se tiene conocimiento del ciberataque o incidente de ciberseguridad según lo señala la normativa. Se procederá con similar criterio en el caso de que el incidente suponga una infracción a la Ley de Delitos Informáticos.

5.2.2.3. Comunicación a usuarios:

Durante el desarrollo del incidente el(a) Encargado(a) de Comunicaciones informará a los equipos internos del Ministerio y a la Comunidad Escolar según corresponda.

5.2.3. Contención y resolución

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

En esta fase se debe asignar al área(s) técnica(s) que corresponda la responsabilidad de realizar la investigación, diagnóstico y análisis para adoptar las acciones inmediatas orientadas a contener el daño, mitigar riesgos y posteriormente resolver el incidente.

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

Dependiendo de la magnitud e impacto, el Encargado de Operaciones de la CNT deberá mantener informado de su desarrollo al equipo de Seguridad Operacional, quien reunirá antecedentes para comunicarlos al Encargado de Seguridad de la Información.

5.2.4. Actividad post incidente

Se realizará una evaluación con el fin de revisar la aplicación de medidas correctivas de fondo y se generará un informe para revisar y compartir lecciones aprendidas. Además, se deben iniciar las gestiones para notificar a la División Jurídica, a fin de que evalúe si realizar la denuncia correspondiente a la Policía de Investigaciones (PDI) u otros organismos externos.

El proceso de mejora continua agrupa todas las actividades que serán organizadas por parte de Seguridad de la Información, con el fin de optimizar la postura de seguridad ante futuras situaciones de incidencia. En ese sentido, se incluyen como parte de este subproceso las siguientes actividades:

a. Revisión del cierre del incidente.

b. Determinación de patrones de ocurrencia por periodo de tiempo y tipo de servicio.

c. Implementación de controles que eviten la ocurrencia de incidentes similares en el futuro, como por ejemplo, ajustar o desarrollar procedimientos y/o políticas.

6. VIGENCIA

La revisión de la presente Política se realizará cada tres años, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad del Servicio.

Todo el personal del Ministerio deberá tomar conocimiento por escrito de la presente política, la cual se encontrará en formato electrónico en la Intranet para las consultas respectivas.

7. MARCO NORMATIVO

a. Ley N°17.336, de Propiedad Intelectual.

b. Ley N°19.628, sobre Protección de la Vida Privada.

c. Ley N°19.799, sobre Documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

d. Ley N°20.285, sobre Acceso a la Información Pública.

e. Ley N°21.459 que Establece Normas sobre Delitos Informáticos, deroga la Ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

f. Ley N°21.663, Marco de Ciberseguridad.

g. D.F.L. N°29 de 2004, que Fija el Texto Refundido, Coordinado y Sistematizado de la Ley N°18.834, sobre Estatuto Administrativo.

h. Decreto Supremo N°83, de 2004, 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.

i. Decreto Supremo N°273, de 2022, del Ministerio del Interior y Seguridad Pública, que Establece Obligación de Reportar Incidentes de Ciberseguridad.

j. Decreto Supremo N°7, de 2023, del Ministerio Secretaría General de la Presidencia, que Establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme la Ley N°21.180.

k. Política Nacional de Ciberseguridad.

l. Norma Chilena NCh-ISO27001:2023 y NCh-ISO27002:2023 sobre "Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos".

8. RESPONSABILIDAD ANTE INFRACCIONES

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, respecto de los dependientes que detentan la calidad de funcionarios públicos, ya sea Titulares o a Contrata, 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 podrá constituir causal suficiente para producir el término inmediato y anticipado del respectivo contrato que los vincule con el Ministerio, de acuerdo a lo que dicho contrato establezca, sin perjuicio de otras responsabilidades civiles o penales, que la infracción pudiere irrogarles.

En esta materia, la Coordinación Nacional de Tecnología aplicará las medidas necesarias para monitorear el cumplimiento de esta política, mantendrá a los usuarios informados sobre nuevas amenazas y cuidados con respecto al resguardo de los activos de información, de manera de evitar incidentes producidos por el no cumplimiento de esta Política.

Sin perjuicio de lo anterior, las acciones disciplinarias estarán supeditadas a las disposiciones, deberes e infracciones establecidos en la Ley N°21.663 Marco de Ciberseguridad, así como a sus distintas normas, reglamentos y actos administrativos concordantes al respecto.

9. GLOSARIO DE TÉRMINOS

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

a. Activo: Cualquier elemento que tenga valor para la organización. Para el ámbito de la gestión de incidentes es de interés el siguiente:

   - Activos informáticos: Toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.

b. Ciberataque: Intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.

c. Ciberseguridad: Preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas

informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.

d. Confidencialidad: Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.

e. Disponibilidad: Propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

f. CSIRT: Sigla del inglés (Computer Security Incident Response Team), definida como aquellos centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

g. Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), de la Agencia Nacional de Ciberseguridad: es el ente encargado de responder y coordinar la gestión de ciberataques de impacto significativo a nivel nacional, así como también de asesorar técnicamente a los CSIRT de los organismos de la Administración del Estado, entre otras funciones establecidas en la Ley N°21.663.

h. Equipo de Respuesta a Incidentes de Seguridad Informática De la Subsecretaría de Educación (CSIRT de la Subsecretaría de Educación): Centro multidisciplinario que tiene por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúa conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos. Se encuentra conformado por el(la) Encargado(a) Técnico, el(la) Encargado(a) de Operaciones y el Equipo de Seguridad Operacional, todos(as) de la CNT.

i. Evento de seguridad de la información: 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. No es necesariamente una ocurrencia maliciosa o adversa, pero si se puede transformar en un incidente de seguridad.

j. Incidente de ciberseguridad: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o

resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.

k. Incidente de efecto significativo: Se considerará que un incidente de ciberseguridad tiene efecto significativo si es capaz de interrumpir la continuidad de un servicio esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales. Para determinar la importancia de los efectos de un incidente, se tendrán especialmente en cuenta los siguientes criterios:

   - El número de personas afectadas.
   - La duración del incidente.
   - La extensión geográfica con respecto a la zona afectada por el incidente.

l. Integridad: Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.

m. Red y sistema informático: conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.

n. Resiliencia: capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.

o. Riesgo: posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.

p. Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

q. Usuario: Todo aquel que utiliza la estructura tecnológica para el cumplimiento de las funciones laborales.

r. Mesa de Ayuda de la CNT: Conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar las solicitudes de usuarios internos de manera integral, junto con la atención

de requerimientos que tengan relación con las Tecnologías de la Información y la Comunicación.

s. Playbook: Documento que contiene el flujo de tareas cuyo objetivo es dar instrucción, guía y recomendaciones, para el tratamiento y la respuesta, abordando de manera dirigida el incidente de seguridad de la información o ciberseguridad, dependiendo su característica.

t. GLPI: Acrónimo en Francés (Gestionnaire Libre de Parc Informatique) Software de código abierto utilizado para la gestión y seguimiento de servicios, incidentes y solicitudes de usuarios que tengan relación con plataformas, sistemas y tecnologías de la información.

u. Coordinación Nacional de Tecnología (CNT): es la unidad ministerial que desarrolla proyectos e implementa soluciones que tengan relación con la tecnología, así como también da soporte tecnológico a las iniciativas ministeriales.

v. SOC: Sigla del inglés (Security Operations Centers) o centro de operaciones de seguridad, el cual es el equipo responsable de supervisar y analizar la actividad en redes, servidores, terminales, bases de datos, aplicaciones, sitios web y otros sistemas en búsqueda de comportamientos anormales que puedan indicar un incidente de seguridad utilizando soluciones tecnológicas, teniendo un enfoque preventivo.

ANÓTESE, PUBLÍQUESE INTERNAMENTE Y ARCHÍVESE

REPUBLICA DE CHILE
MINISTERIO DE EDUCACIÓN

ALEJANDRA ARRATIA MARTÍNEZ
SUBSECRETARIA DE EDUCACIÓN

Distribución:
- Gabinete Sr. Ministro
- Gabinete Sra. Subsecretaria de Educación
- Gabinete Sra. Subsecretaria de Educación Parvularia
- Gabinete Sr. Subsecretario de Educación Superior
- División Jurídica
- Oficina de Partes y Archivos.
- Archivo.
  Expediente N° 37.731-2024