DIARIO OFICIAL
DE LA REPUBLICA DE CHILE
Ministerio del Interior y Seguridad Pública

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 44.088 | Sábado 1 de Marzo de 2025 | Página 1 de 6

Normas Generales

CVE 2617387

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA

Subsecretaría del Interior

APRUEBA REGLAMENTO DE REPORTE DE INCIDENTES DE CIBERSEGURIDAD DE LA LEY N° 21.663

Núm. 295.- Santiago, 25 de septiembre de 2024.

Vistos:

Lo dispuesto en el artículo 32, N° 6, y 35 de la Constitución Política de la República de Chile, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto N° 100, de 2005, del Ministerio Secretaría General de la Presidencia; en el decreto con fuerza de ley 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 Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado; en la Ley N° 20.502, que crea el Ministerio del Interior y Seguridad Pública y el Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol, y modifica diversos cuerpos legales; en la Ley N° 21.663, marco de Ciberseguridad; en el decreto con fuerza de ley N° 1, de 2020, del Ministerio Secretaría General de la Presidencia, que establece normas de aplicación del artículo 1° de la Ley N° 21.180, de transformación digital del Estado; en el decreto supremo N° 164, de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba la Política Nacional de Ciberseguridad 2023-2028; y 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.

Considerando:

1. Que, la Ley N° 21.663, marco de Ciberseguridad, se publicó en el Diario Oficial el 8 de abril de 2024.

2. Que, conforme a su artículo 1°, la ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones determinadas en el artículo 4°, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

3. Que, dentro de los objetivos centrales que contempla la Política Nacional de Ciberseguridad 2023-2028, contenida en el decreto supremo N° 164, de 2023, del Ministerio del Interior y Seguridad Pública, se establece el de "Infraestructura resiliente", el cual implica contar con una "infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos"; señalándose, además que, para avanzar en este objetivo, es necesario "fortalecer la resiliencia de nuestros servicios esenciales frente a incidentes de ciberseguridad";

4. Que, el artículo 9° de la ley establece el deber de reportar, conforme el cual todas las instituciones públicas y privadas señaladas en su artículo 4° tendrán la obligación de reportar al Equipo de Respuesta a Incidentes de Seguridad Informática Nacional (en adelante, "CSIRT Nacional") tan pronto les sea posible los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos indicados en su artículo 27, lo cual, deberá realizarse conforme al esquema señalado en el citado artículo 9°.

5. Que, en relación con lo anterior, cabe hacer presente que, el referido artículo 9° en su inciso final, mandata que, el contenido de las diversas clases de reportes señalados en dicho artículo deberá

ser regulado, a través de la dictación de un reglamento expedido por el Ministerio encargado de la seguridad pública.

6. Que, de acuerdo con lo dispuesto en el inciso final del artículo 27 de la ley, el procedimiento específico para notificar un incidente de ciberseguridad de efecto significativo, la forma, así como las condiciones de anonimato, la taxonomía del informe y la periodicidad, serán establecidos en el reglamento de la presente ley.

7. Que, durante los días 29, 30 y 31 de julio de 2024 se realizó un proceso de diálogo público privado que contó con la participación de representantes gremiales, instituciones académicas y representantes de la sociedad civil (ONGs) con el objeto de fortalecer la elaboración del presente reglamento.

8. Que, durante los días 7 y 12 de agosto de 2024 se publicó el borrador del presente reglamento en el sitio web de la Coordinación Nacional de Ciberseguridad con el objeto de que los interesados en su elaboración pudieren formular observaciones;

9. Que, para efectos de lo anterior y en virtud de lo dispuesto en el artículo 2° de la ley N° 20.502, que crea el Ministerio del Interior y Seguridad Pública y el Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol, y modifica diversos cuerpos legales, el Ministerio del Interior y Seguridad Pública es el Ministerio encargado de la seguridad pública; y en uso de mis facultades.

Decreto:

Artículo único.- Apruébese el reglamento de reporte de incidentes de ciberseguridad de la ley N° 21.663.

TÍTULO I
Aspectos Generales

Artículo 1°. Definiciones. Para efectos del presente Reglamento se entenderá por:

a) Administración del Estado: Para efectos de este reglamento, y conforme el artículo 1° de la ley, la Administración del Estado estará constituida por los Ministerios, las Delegaciones Presidenciales Regionales y Provinciales, los Gobiernos Regionales, las Municipalidades, las Fuerzas Armadas, las Fuerzas de Orden y Seguridad Pública, las empresas públicas creadas por ley, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa. Las disposiciones de este reglamento serán aplicables a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio.

b) Agencia: Agencia Nacional de Ciberseguridad.

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

d) Director o Directora: Director o Directora Nacional de la Agencia Nacional de Ciberseguridad

e) Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT: 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.

f) 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.

g) Incidente gestionado: Se entenderá que un incidente se encuentra gestionado en el momento en que los antecedentes proporcionados por las instituciones afectadas permitan a la Agencia declararlo como cerrado.

h) Información: Información generada, almacenada o transmitida por sistemas informáticos.

i) Informe: Reporte electrónico que contiene los antecedentes fácticos y tecnológicos respecto de un incidente o ciberataque elaborado por una institución que hubiere o pudiere ser afectada.

j) Ley: Ley N° 21.663, marco de Ciberseguridad.

k) Operadores de importancia vital: Aquellos proveedores de servicios esenciales y aquellas instituciones privadas que, sin tener la calidad de proveedores de servicios esenciales, han sido calificados como tales, de conformidad a lo dispuesto en el artículo 5° de la Ley y su Reglamento.

l) Plataforma: Sistema tecnológico dispuesto por la Agencia Nacional de Ciberseguridad para realizar el reporte de incidentes dispuesto en el artículo 2° de este Reglamento.

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

Artículo 2°. Del deber de reportar. Las instituciones públicas y privadas que presten servicios calificados como esenciales y aquellas que hubieren sido calificadas como operadores de importancia vital de conformidad a la ley y su reglamento, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos.

TÍTULO II
De los incidentes

Artículo 3°. Incidente de ciberseguridad con efecto significativo. Se considerará que un incidente de ciberseguridad tiene efecto significativo si es capaz de producir alguno de los siguientes efectos:

a) Interrumpir la continuidad de un servicio esencial. En dicho caso deberá considerarse, tanto los servicios entregados por proveedores, como la cadena de suministro, de una institución que preste servicios esenciales o de un operador de importancia vital.
b) Afectar la integridad física o la salud de las personas.
c) Afectar la integridad o confidencialidad de activos informáticos, o la disponibilidad de alguna red o sistema informático, aun cuando esto no produzca o hubiere producido afectación inmediata en la provisión del servicio.
d) Utilizar o ingresar sin autorización a redes o sistemas informáticos, aun cuando esto no produzca o hubiere producido afectación inmediata en la provisión del servicio.
e) Afectar sistemas informáticos que contengan datos personales.

Para determinar la importancia de los efectos de un incidente de ciberseguridad se deberán tener especialmente en consideración el número de personas afectadas; la duración del incidente; y/o la extensión geográfica con respecto a la zona afectada por el incidente.
El Director o Directora, podrá determinar las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación, así como los prestadores de servicios esenciales que estarán exentos de la obligación de notificar.
Para tal efecto, el CSIRT deberá elaborar un informe con los criterios técnicos para la determinación de las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación, atendiendo a las características y relevancia del servicio proveído por el prestador.

Artículo 4°. Mantenciones regulares. Las mantenciones planificadas que produzcan o pudieren producir indisponibilidad de los sistemas informáticos de una institución regida por el presente reglamento no se considerarán incidentes. Para dichos efectos, la institución deberá incluirlas en sus planes de continuidad operacional y ciberseguridad.

TÍTULO III
De la taxonomía del informe

Artículo 5°. Taxonomía del Informe. Los informes enviados al CSIRT Nacional para dar cumplimiento a lo establecido en el artículo 2° deberán contener, como mínimo, la siguiente información:

a) Datos para la debida identificación de la institución afectada; nombre, RUT, dirección y correo electrónico el cual será utilizado, además, para efectos de la notificación dispuesta en la letra k) artículo 11 de la ley.
b) Individualización y datos de contacto del delegado de ciberseguridad o quien ostente el cargo relacionado a ciberseguridad de mayor responsabilidad en la organización de la institución afectada.
c) Fecha y hora en la cual se tomó conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad y fecha estimada de inicio del incidente de ciberseguridad, si fuese conocida;
d) Evidencia, si la hubiera, que el ciberataque o incidente de ciberseguridad responde a una acción tipificada como delito en la legislación nacional;
e) Potenciales repercusiones del ciberataque o incidente de ciberseguridad en otras instituciones;
f) Indicios de la ocurrencia del incidente, por ejemplo, denegación, indisponibilidad o degradación de servicio; acceso no autorizado a la red o al dispositivo; exposición, robo o fuga de datos; código malicioso o malware; phishing o fraude; u otro que corresponda;
g) Activos y recursos potencialmente afectados, detectados al momento de elaboración del informe. Para estos efectos, se entenderá por activo la infraestructura física y digital de la organización, tales como servidores, data centers, aplicaciones, repositorios de datos y activos informáticos.
h) Indicadores de compromiso detectados, tipo, fuente o ubicación, si los hubiere; y
i) Cualquier otro dato que fuere útil para la gestión oportuna del ciberataque o incidente de ciberseguridad.

Mediante resolución del Director o Directora, se actualizará el contenido mínimo de los reportes de incidentes. Dicha resolución deberá contar con un informe técnico del CSIRT Nacional, quien deberá considerar las prácticas y recomendaciones de los organismos internacionales con competencia en la materia.

Artículo 6°. Datos personales. El reporte de incidente deberá omitir todo dato o información personal, conforme a lo dispuesto en el artículo 2°, letra f), de la Ley N° 19.628, sobre Protección de

la Vida Privada. Para efectos de lo dispuesto en este inciso, no se considerará que la dirección IP sea un dato o información personal.

Artículo 7°. Si la Agencia tomare conocimiento que una institución ha sido afectada por un incidente de ciberseguridad de efecto significativo y no ha realizado el reporte dispuesto en el artículo 9 de la ley deberá requerirla para que lo realice conforme el artículo siguiente.

La notificación será practicada al correo electrónico que la institución hubiere informado para tales efectos. Si dicho correo electrónico no hubiere sido informado deberá realizar la notificación de acuerdo al decreto supremo N° 4, de 2020, del Ministerio Secretaría General de la Presidencia, que aprueba el reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la Ley N° 21.180 sobre Transformación Digital del Estado.

Las instituciones y órganos señalados en el artículo 53 de la ley no estarán sujetos en modo alguno a la regulación, fiscalización o supervigilancia de la Agencia, sin perjuicio de que deberán convenir mecanismos de reportes de incidentes de ciberseguridad y de coordinación y cooperación para la respuesta de incidentes.

TÍTULO IV
De las alertas, reportes e informes

Artículo 8°. Plataforma de reporte de incidentes. Los informes de ciberataques e incidentes de ciberseguridad deberán realizarse a través de la plataforma de notificación dispuesta por la Agencia, la que deberá estar operativa las veinticuatro horas, todos los días del año.

La plataforma, además, permitirá que los reportes de incidentes realizados por los sujetos obligados sean comunicados simultáneamente a otros órganos sectoriales cuando existiere la obligación de notificar a más de una autoridad.

Artículo 9°. Alerta Temprana. Una vez que la institución obligada a reportar hubiere tomado conocimiento de la ocurrencia de un incidente de ciberseguridad, deberá enviar una alerta sobre la ocurrencia del evento en el plazo máximo de tres horas, contado desde que hubiere tomado conocimiento de la ocurrencia del incidente.

El reporte deberá contener, al menos, la información requerida en las letras a), b), c), f) y g) del artículo 5° de este Reglamento.

Si la institución tomare conocimiento de información adicional deberá actualizar el reporte de alerta temprana, conforme el flujo dispuesto en la plataforma.

Artículo 10. Segundo reporte. Transcurrido el plazo de máximo de setenta y dos horas desde que la institución hubiere tomado conocimiento de la ocurrencia de un incidente de ciberseguridad, deberá enviar un segundo reporte al CSIRT Nacional. Si la institución afectada fuera un operador de importancia vital y éste viera afectada la prestación de sus servicios esenciales a causa del incidente, la actualización de la información, a través del segundo reporte, deberá entregarse en el plazo máximo de veinticuatro horas.

Dicho reporte deberá actualizar la información entregada en el artículo anterior, incluyendo la totalidad de los campos dispuestos en el artículo 5° si corresponden, además de una evaluación inicial de la gravedad e impacto del incidente y los indicadores de compromiso obtenidos en el caso que existieran.

Artículo 11. Plan de acción de los operadores de importancia vital. Los operadores de importancia vital deberán implementar e informar el plan de acción frente al incidente en un plazo que, en ningún caso, podrá ser superior siete días corridos, contados desde que se tiene conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad.

Dicho plan de acción deberá incluir al menos, un programa de recuperación de información; inclusión de responsabilidades técnicas y administrativas y estimación de tiempo de recuperación de los servicios si es que su continuidad fue interrumpida.

Mediante instrucción general aprobada por resolución del Director o Directora se establecerán los contenidos y parámetros que deberá contener dicho plan de acción.

Artículo 12. Informe Final. Dentro del plazo máximo de quince días corridos contados desde el envío de la alerta temprana y siempre que el incidente hubiese sido gestionado, la institución deberá elaborar un informe final que deberá incluir, como mínimo, una confirmación o actualización de todos los datos informados en los reportes anteriores, además de la siguiente información:

a) Una descripción detallada del incidente, incluyendo su gravedad e impacto.
b) El tipo de amenaza o causa principal que, probablemente, haya causado el incidente.
c) Las medidas de mitigación aplicadas y en curso.
d) Si procede, las repercusiones transfronterizas del incidente.

Si la institución afectada fuera un operador de importancia vital y éste viera afectada la prestación de sus servicios esenciales a causa de un ciberataque o incidente de ciberseguridad, se deberá incluir de forma adicional:

a) La identificación de la o las vulnerabilidades explotadas y las aplicaciones abusivas (exploits) utilizadas para vulnerar los activos afectados, si es que esta información estuviera disponible. Si la información fuera desconocida al momento del informe, deberá indicarse esto explícitamente.

b) La identificación de los controles técnicos que deberían haber prevenido o mitigado el incidente de ciberseguridad o ciberataque junto con las causas por las cuales los controles fallaron; o la causa de la ausencia de controles implementados.

c) Si a la fecha de ocurrencia del incidente, el CSIRT Nacional hubiere difundido alertas tempranas, avisos e información sobre riesgos e incidentes para las comunidades relacionadas con el mismo, la institución deberá indicar si ellas fueron adoptadas oportuna y expeditamente. En caso de no haber sido adoptadas, la institución deberá indicar las razones para no implementarlas.

Artículo 13. Informe parcial de incidente de ocurrencia prolongada. Si el incidente no se hubiera gestionado en el plazo dispuesto en el artículo anterior, la institución deberá postergar el envío del informe final y remitir un informe parcial sobre el estado de la situación. Dichos informes deberán actualizarse cada quince días contados desde el último envío. Si no existieran nuevos antecedentes, se deberá indicar dicha circunstancia.

Artículo 14. Actualización de los informes. Sin perjuicio de lo dispuesto en los artículos anteriores, el CSIRT Nacional podrá solicitar información adicional a la institución obligada a reportar con el objetivo de realizar la gestión del incidente.

Los informes que reciba la Agencia en cumplimiento del deber de reporte se considerarán como información secreta, cuando dichos informes contengan información reservada en virtud de una norma legal, en particular aquella mencionada en los incisos cuarto y quinto del artículo 33 o cuando le haya sido entregada bajo tal calidad en virtud de lo dispuesto en el artículo 35 de la Ley.

Artículo 15. Proveedores de servicios de tecnologías de la información de los organismos del Estado. Para dar cumplimiento al deber establecido en el artículo 2, las y los jefes de servicio de los organismos del Estado deberán exigir a los proveedores de servicios de tecnologías de la información que compartan la información sobre vulnerabilidades e incidentes que puedan afectar a las redes y sistemas informáticos de dichos organismos, con el objeto de prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o reforzar el nivel de ciberseguridad, y garantizar, a su vez, que se respete la posible naturaleza delicada de la información compartida.

Los contratos de prestación de servicios no podrán incluir cláusulas que restrinjan o dificulten lo dispuesto en el inciso anterior ni la comunicación de información sobre amenazas por parte del prestador de servicios. Dichos contratos deberán resguardar la seguridad y protección de datos, incluida la confidencialidad y protección de la propiedad intelectual.

Artículo 16. Instrucciones Generales. La Agencia, mediante resolución del Director o Directora, dictará las demás instrucciones generales que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente reglamento.

En los casos en que estas instrucciones generales tengan efecto en áreas de competencia de otra entidad sectorial, deberá previamente remitir la información relevante a dicha entidad y solicitar un informe con el propósito de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración efectiva entre ambas autoridades, de conformidad a lo dispuesto en el artículo 25 de la ley.

Las reglas establecidas en los incisos precedentes no obstarán a lo dispuesto en el inciso final del artículo 25 de la ley, cuando corresponda.

TÍTULO V
Disposiciones finales

Artículo 17. CSIRT Sectoriales. Los CSIRT que pertenezcan a los organismos de la Administración del Estado tendrán la obligación de tomar las providencias necesarias para apoyar el restablecimiento del servicio afectado, bajo la coordinación del CSIRT Nacional.

Artículo 18. Notificaciones Voluntarias. La Agencia propiciará las notificaciones voluntarias de instituciones no obligadas conforme el artículo 9° de la ley, dicha notificación en ningún caso impondrá a la entidad de origen obligaciones contempladas para los sujetos obligados conforme la presente ley.

La Agencia establecerá canales anónimos para quienes deseen resguardar su identidad al realizar un reporte. Dicha facultad en ningún caso podrá ser utilizada por quienes tengan el deber de reporte, de conformidad en el artículo 2° de este Reglamento.

DISPOSICIONES TRANSITORIAS

Artículo primero transitorio. El presente Reglamento comenzará a regir desde la fecha de iniciación de las actividades de la Agencia, de conformidad a lo dispuesto en el artículo 1° transitorio de la ley N° 21.663.

Artículo segundo transitorio. Las notificaciones electrónicas dispuestas en el presente reglamento comenzarán a practicarse de conformidad a las reglas de gradualidad dispuestas en el decreto con fuerza de ley N° 1, de 2020, del Ministerio Secretaría General de la Presidencia, que establece normas de aplicación del artículo 1° de la Ley N° 21.180, de Transformación Digital del Estado, respecto de los procedimientos administrativos regulados en leyes especiales que se expresan a través de medios electrónicos y determina la gradualidad para la aplicación de la misma ley, a los órganos de la administración del Estado que indica y las materias que les resultan aplicables. En tanto no entrare en vigencia dicho régimen, las notificaciones serán practicadas por carta certificada al domicilio de la respectiva institución conforme lo dispuesto en la legislación vigente.

Artículo tercero transitorio. Los contratos que fueran celebrados por los órganos de la Administración del Estado y aquellos procedimientos de contratación cuyas bases o términos de referencia hayan sido aprobadas antes de la entrada en vigencia del presente Reglamento, se regularán por la normativa vigente a la fecha de dicha aprobación.

Anótese, tómese razón y publíquese.- CAROLINA TOHÁ MORALES, Vicepresidenta de la República.- Manuel Monsalve Benavides, Ministro del Interior y Seguridad Pública (S).

Lo que transcribo a Ud. para su conocimiento.- Atentamente, Vanessa Marimón Fuentes, Subsecretaria del Interior (S).

CVE 2617387 | Director: Felipe Andrés Peroti Díaz
Sitio Web: www.diariooficial.cl | Mesa Central: 600 712 0001 E-mail: consultas@diariooficial.cl
Dirección: Dr. Torres Boonen N°511, Providencia, Santiago, Chile.