DIARIO OFICIAL
DE LA REPÚBLICA DE CHILE
Ministerio del Interior

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 44.337 | Miércoles 31 de Diciembre de 2025 | Página 1 de 9

Normas Generales

CVE 2748664

MINISTERIO DE DEFENSA NACIONAL

Subsecretaría de Defensa

APRUEBA REGLAMENTO DE CIBERSEGURIDAD DE LA DEFENSA NACIONAL

Santiago, 23 de mayo de 2025.- Con esta fecha se ha resuelto lo siguiente:
Núm. 2.

Visto:

Lo dispuesto en los artículos 32 N° 6 y 35 de la Constitución Política de la República, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto supremo 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 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, establece bases de los procedimientos administrativos que rigen los órganos de la Administración del Estado; en la ley N° 18.948, ley orgánica constitucional de las Fuerzas Armadas; en la ley N° 20.424, estatuto orgánico del Ministerio de Defensa Nacional; en la ley N° 21.174, establece nuevo mecanismo de financiamiento de las capacidades estratégicas de la Defensa Nacional; en la ley N° 21.663, ley marco de ciberseguridad; en la ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia; en la ley N° 21.180, sobre transformación digital del Estado; en el decreto N° 2.226, de 1944, Código de Justicia Militar; en el decreto supremo N° 248, de 2010, del Ministerio de Defensa Nacional, que aprueba el reglamento orgánico y de funcionamiento del Ministerio de Defensa Nacional; en el decreto supremo N° 3, de 2017, del Ministerio de Defensa Nacional, que aprueba Política de Ciberdefensa; en el decreto supremo N° 164, de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba Política Nacional de Ciberseguridad 2023-2028; en la Orden Ministerial N° 002 de 2018, del Ministerio de Defensa Nacional, que actualiza directiva de ciberseguridad para el Ministerio de Defensa Nacional y deja sin efecto lo que indica; en la Orden Ministerial N° 2393/2020, de 2020, del Ministerio de Defensa Nacional, que dispone organización y funcionamiento del Estado Mayor Conjunto; en el decreto supremo N° 295, de 2024, del Ministerio del Interior y Seguridad Pública; en el decreto supremo N° 285, de 2024, del Ministerio del Interior y Seguridad Pública; en el 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 a la ley N° 21.180.

Considerando:

1. Que, la ley N° 21.663 Marco de Ciberseguridad establece la creación de un equipo de respuesta a incidentes de Seguridad Informática de la Defensa Nacional, en adelante, CSIRT de la Defensa Nacional, como el organismo responsable de la coordinación, protección y seguridad de las redes y sistemas del mencionado Ministerio y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la defensa y la seguridad nacional. Este equipo dependerá del Estado Mayor Conjunto, del Ministerio de Defensa Nacional.

2. Que, a su vez, la ley establece la existencia de equipos de respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional, en adelante CSIRT Institucionales, los que tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la Defensa Nacional.

3. Que, la ley establece que un reglamento regulará al CSIRT de la Defensa Nacional y a los CSIRT Institucionales de la Defensa Nacional.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

4. Que, el CSIRT de la Defensa Nacional tendrá como función conducir y asegurar la protección y defensa de los riesgos y amenazas presentes en el ciberespacio. Para ello, estará a cargo de la coordinación y será enlace entre los diferentes CSIRT Institucionales de la Defensa Nacional.

5. Que, el CSIRT de la Defensa Nacional entregará los lineamientos para que puedan constituirse Equipos de Respuesta de Incidentes de Seguridad Informática Institucionales de la Defensa Nacional.

6. Que, la Agencia requerirá informe fundado al Ministerio de Defensa Nacional para que se pronuncie sobre aquellas instituciones públicas y privadas que deban calificarse como operadores de importancia vital, de acuerdo a lo establecido en el artículo 6 de la ley N° 21.663.

7. Que, esta regulación debe adecuarse a la política de Ciberdefensa y a los lineamientos generales que entregue la Agencia Nacional de Ciberseguridad (en adelante la "Agencia").

8. Que, a su vez, la ley dispone que el CSIRT de la Defensa reportará a la Agencia Nacional de Ciberseguridad todos los incidentes identificados cuando no se ponga en riesgo la seguridad y la defensa nacional.

9. Que, por su parte, la Política Nacional de Ciberseguridad 2023-2028 establece como objetivo 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.

10. Que, el Estado Mayor Conjunto, de acuerdo al artículo 25 de la ley N° 20.424 Estatuto Orgánico del Ministerio de Defensa Nacional, es el organismo de trabajo y asesoría permanente del Ministro(a) de Defensa Nacional en materias que tengan relación con la preparación y empleo conjunto de las Fuerzas Armadas.

11. Que, entre las funciones del Estado Mayor Conjunto conforme al artículo 25 citado anteriormente, se encuentran aquellas establecidas en el literal j), consistente en proveer de inteligencia a la Subsecretaría de Defensa para efectos de la planificación primaria; así como la dispuesta en el literal k), relativa a conducir al Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional en coordinación con la Subsecretaría de Defensa.

12. Que, la Subsecretaría de Defensa es el órgano de colaboración inmediata del Ministerio de Defensa en asuntos de política de defensa.

13. Que, de acuerdo al decreto supremo N° 248, de 2010, del Ministerio de Defensa Nacional, que "Aprueba el Reglamento Orgánico y de Funcionamiento del Ministerio de Defensa Nacional", se establece que la División de Desarrollo Tecnológico e Industria de la Subsecretaría de Defensa contará con un departamento de Ciberdefensa y Ciberseguridad, el cual tendrá entre sus funciones establecer y verificar el cumplimiento de los controles de ciberseguridad y de su constante actualización, conforme a los lineamientos estratégicos que, al interior de la Subsecretaría, se den respecto a la seguridad de la información.

14. Que, por todo lo expuesto anteriormente, corresponde la dictación del presente reglamento.

Decreto:

Apruébese el siguiente Reglamento de Ciberseguridad de la Defensa Nacional:

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1°.- Objeto.

Este reglamento tiene por objeto establecer los principios y las normas para estructurar, regular y coordinar las acciones de ciberseguridad en el ámbito de la defensa nacional. En ese sentido, regula el Equipo de Respuesta de Incidentes de Seguridad Informática de la Defensa Nacional, en adelante CSIRT de la Defensa o CSIRT-DN, que depende del Ministerio de Defensa Nacional, el cual será responsable de coordinar, proteger y asegurar las redes y sistemas del Ministerio, así como los servicios esenciales y operadores vitales para la defensa nacional, y de cumplir con las tareas que se le encomienden, conforme a lo establecido en la ley N° 21.663, Marco de Ciberseguridad. Asimismo, regula los equipos de respuesta de incidentes de Seguridad Informática Institucionales de la Defensa Nacional, en adelante CSIRT-IDN, y el procedimiento de reporte de ciberataques e incidentes de ciberseguridad que estos equipos deben informar al CSIRT-DN.

Artículo 2°.- Definiciones. Para los efectos de este Reglamento se entenderá por:

1. Activo informático: toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
2. Agencia o ANCI: la Agencia Nacional de Ciberseguridad.
3. Almacenamiento de datos: la conservación o custodia de datos en un registro o banco de datos.
4. Auditorías de seguridad: procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

5. Autenticación: propiedad de la información que da cuenta de su origen legítimo.
6. Ciberataque: acción o intento de acceder, destruir, exponer, alterar, deshabilitar, exfiltrar o hacer uso no autorizado de un activo informático.
7. Ciberdefensa: es una actividad del ámbito de la Defensa Nacional, que apoya a las operaciones militares para enfrentar las acciones hostiles en el Ciberespacio, ejecutadas con fines militares o de inteligencia por parte de otros Estados u otros.
8. 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 en el ámbito de la Defensa.
9. Confidencialidad: propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.
10. CSIRT-DN: Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional.
11. CSIRT-IDN: Equipo de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional.
12. Dato estadístico: dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.
13. Datos de carácter personal o datos personales: cualquier información concerniente a personas naturales, identificadas o identificables.
14. Datos sensibles: aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
15. Disponibilidad: propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.
16. 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.
17. Incidente de ciberseguridad: cualquier 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.
18. Integridad: propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.
19. Información sensible: cualquier dato o información que, si se difunde, se pierde o se utiliza de forma distinta a la prevista, el resultado puede ser un daño grave para las personas o la organización a la que pertenece esa información.
20. Ley Marco: ley N° 21.663, Marco de Ciberseguridad.
21. OIV-DN: Operadores de Importancia Vital para la Defensa Nacional.
22. Organismos e instituciones del sector Defensa: son los organismos de la Administración del Estado que prestan servicios esenciales y son parte del sector Defensa.
23. Plan de Ciberseguridad: documento que identifica los activos informáticos, los riesgos de ciberseguridad, y las medidas para gestionar riesgos, incidentes, ciberamenazas y vulnerabilidades.
24. Red y sistema informático: conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.
25. 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.
26. Riesgo: posibilidad de que ocurra un incidente de ciberseguridad, cuya magnitud se mide en función de la probabilidad de su ocurrencia y el impacto de sus consecuencias.
27. Sector Defensa: conjunto de órganos, servicios públicos y empresas del Estado y sus filiales, que dependen del Ministerio de Defensa Nacional o se relacionan con el Gobierno a través de éste.
28. Titular de los datos: persona natural a la que se refieren los datos de carácter personal.
29. Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

Artículo 3°.- Principios rectores. Para alcanzar los objetivos de este reglamento se deberán observar los siguientes principios:

1. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad siempre se deberá actuar coordinada y diligentemente, y adoptar las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

2. Principio de cooperación con la autoridad: para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.
3. Principio de coordinación: de conformidad a lo dispuesto por el inciso segundo del artículo 5° de la ley N° 18.575, orgánica constitucional de bases generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 1-19.653 de 2000, del Ministerio Secretaría General de la Presidencia, la Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente, propender a la unidad de acción y evitar la duplicación o interferencia de funciones.
4. Principio de seguridad en el ciberespacio: es deber del Estado garantizar la seguridad en el ciberespacio. El Estado velará para que todas las personas puedan participar de un ciberespacio seguro y otorgará especial protección a las redes y sistemas informáticos que contengan información de grupos de personas particularmente vulnerables a ciberataques.
5. Principio de respuesta responsable: el Estado, en el marco de la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques en el ámbito de la Defensa, de acuerdo con el artículo 51 de la Carta de las Naciones Unidas, podrá hacer uso de los medios que estime apropiados, tanto físicos como digitales, en el ejercicio de su derecho a la legítima defensa.
6. Principio de seguridad informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el uso de cifrado.
7. Principio de racionalidad: las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades deberán ser necesarios y proporcionales al grado de exposición a los riesgos, y al eventual impacto social y económico.
8. Principio de seguridad y privacidad por defecto y desde el diseño: los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.

Artículo 4°.- De los servicios esenciales para la Defensa Nacional. Son servicios esenciales para la Defensa Nacional aquellos provistos por los organismos e instituciones del sector Defensa, conforme lo establecido en el inciso segundo del artículo 1° y en el artículo 4° de la ley N° 21.663.

Artículo 5°.- De las políticas de seguridad de la información y ciberseguridad. Los prestadores de servicios esenciales de la Defensa Nacional deberán elaborar Políticas de Seguridad de la Información y Ciberseguridad.

Estas políticas tendrán por objeto establecer las directrices generales en la materia, debiendo alinearse con las políticas nacionales y sectoriales vigentes. Su aprobación corresponderá a la jefatura o jefe superior del órgano o servicio y/o directores, según corresponda, mediante acto administrativo.

Artículo 6°.- De los deberes generales de ciberseguridad. Los prestadores de servicios esenciales de la Defensa Nacional deberán aplicar medidas continuas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso. Además, deberán realizar anualmente un análisis de riesgos, y según los resultados obtenidos en éste, aplicar las medidas de mitigación necesarias.

El cumplimiento de estas obligaciones exige la debida implementación de los protocolos y estándares generales establecidos por la Agencia, así como los protocolos y estándares mínimos que dicte el CSIRT-DN, y los estándares particulares de ciberseguridad definidos por cada institución u organismo según sus normas internas. Asimismo, se deberán seguir las normas generales, técnicas e instrucciones emitidas por la autoridad ministerial para fortalecer la ciberseguridad.

Los protocolos, estándares, normas e instrucciones tendrán como objetivo la prevención y gestión de los riesgos asociados a la ciberseguridad, así como la contención y mitigación del impacto de los incidentes en la continuidad operacional del servicio prestado, y en la confidencialidad e integridad de la información, las redes o los sistemas informáticos, conforme a lo establecido en la Ley Marco.

Artículo 7°.- Protocolos y estándares mínimos de ciberseguridad. El CSIRT-DN establecerá, en coordinación con la Agencia y conforme al principio de coordinación regulatoria, los protocolos y estándares mínimos de ciberseguridad para el sector Defensa. Dichos protocolos deberán considerar las características, capacidades y tamaños de las instituciones y organizaciones del sector, así como sus presupuestos.

Los protocolos y estándares mínimos dictados por el CSIRT-DN deberán referirse a la prevención, detección, contención, protección, recuperación de los sistemas y respuesta, considerando los lineamientos establecidos por la Agencia y la Política de Ciberdefensa.

Los organismos e instituciones del sector deberán implementar los protocolos y estándares mínimos establecidos por el CSIRT-DN, pero podrán, a través de sus respectivos CSIRT-IDN, establecer protocolos y estándares superiores, según lo requiera la misión y tipo de organización.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

Artículo 8°.- Deber de reportar. Todos los organismos e instituciones del sector Defensa están obligados a reportar al CSIRT-DN, cualquier ciberataque o incidentes de ciberseguridad que pueda tener efectos significativos, de acuerdo a lo señalado en el artículo 27 de la ley N° 21.663. El reporte deberá ser realizado tan pronto como sea posible y conforme al procedimiento establecido en el título IV del presente reglamento.

El CSIRT-DN reportará a la Agencia sobre la ocurrencia de cualquier incidente de ciberseguridad o ciberataque que pueda comprometer su información, redes o sistemas informáticos.

Artículo 9°.- Informe para el procedimiento de calificación de los operadores de importancia vital. Para los efectos de lo previsto en el artículo 6°, inciso primero de la ley N° 21.663, la Agencia requerirá informe fundado al Ministerio de Defensa Nacional para que se pronuncie sobre aquellas instituciones públicas y privadas que deban calificarse como operadores de importancia vital. Dicho informe deberá ser evacuado en la forma prescrita en el reglamento del procedimiento de calificación de importancia vital de la ley N° 21.663, dictado por el Ministerio del Interior y Seguridad Pública.

Para la elaboración del informe, el Ministro(a) de Defensa Nacional, a través del Subsecretario(a) de Defensa, podrá requerir a los organismos e instituciones del sector los antecedentes necesarios para ello.

La información contenida en estos informes tendrá el carácter de secreto, conforme a lo establecido en los numerales 3 y 5 del artículo 21 (del artículo primero) de la ley N° 20.285, en relación con el artículo 436 del Código de Justicia Militar.

Artículo 10.- La obligación de proveedores de servicios de tecnologías de la información. Los servicios esenciales de la Defensa Nacional exigirán a sus proveedores de servicios de tecnologías de la información el reporte de información sobre vulnerabilidades e incidentes que afecten o puedan afectar a las redes y sistemas informáticos de sus organismos. Esta obligación tendrá por objeto la prevención y detección de incidentes, la respuesta oportuna ante estos, la recuperación de los sistemas afectados y la reducción de su impacto.

Los organismos obligados deberán incorporar estas exigencias en sus procesos de compra. Los contratos de prestación de servicios no podrán incluir cláusulas que restrinjan o dificulten la comunicación de información sobre amenazas por parte del proveedor de servicios. Para este efecto, los organismos obligados deberán adaptar sus procesos de contratación.

La aplicación de estas disposiciones deberá considerar la protección de la confidencialidad de la información sensible, la seguridad de los datos y la propiedad intelectual involucrada.

TÍTULO II

DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA DEFENSA NACIONAL

Artículo 11.- Del Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional. El Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional dependerá del Estado Mayor Conjunto del Ministerio de Defensa Nacional. Este equipo será responsable de la coordinación, protección y seguridad de las redes y sistemas del Ministerio, así como de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas con el propósito de resguardar la defensa y la seguridad nacional. La conducción del equipo, que comprende la planificación, operación y ejecución de sus funciones, será ejercida por el Estado Mayor Conjunto en coordinación con la Subsecretaría de Defensa, en su calidad de encargada ministerial de ciberseguridad. Esta coordinación incluirá el intercambio de información y la articulación de programas, planes y políticas sectoriales para el resguardo de la defensa y seguridad nacional.

Artículo 12.- Dependencia. El CSIRT-DN depende del Ministerio de Defensa Nacional, a través del Estado Mayor Conjunto.

Para los efectos presupuestarios, este CSIRT-DN dependerá del Ministerio de Defensa Nacional, y se regirá por el presente reglamento y, en lo que le sea aplicable, por la Ley Marco.

Artículo 13.- De las funciones del CSIRT de la Defensa Nacional. El CSIRT-DN tiene las siguientes funciones:

a) Conducir y asegurar la protección y defensa de los riesgos y amenazas presentes en el ciberespacio, que permitan preservar la confidencialidad, integridad y disponibilidad de las redes de información, los servicios esenciales y operadores vitales para la Defensa Nacional. Para ello, estará a cargo de la coordinación y será enlace entre los diferentes CSIRT-IDN del sector.
b) Asumir el rol de coordinador y enlace entre la Agencia y el CSIRT Nacional con los CSIRT-IDN, asegurando la cooperación, colaboración e intercambio de información pertinente que fortalezca la ciberseguridad.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

c) Establecer los protocolos y estándares mínimos de ciberseguridad para prevenir, detectar, contener, proteger, recuperar los sistemas de respuesta dependientes de las Fuerzas Armadas y del Estado Mayor Conjunto, considerando los lineamientos establecidos por la Agencia.
d) Prestar colaboración o asesoría técnica en la implementación de las políticas de ciberseguridad nacionales a los CSIRT-IDN.
e) Proponer a la autoridad ministerial, a través del Subsecretario(a) de Defensa, la dictación de normas, directrices e instrucciones de ciberseguridad dirigidas a las instituciones y organismos del sector.
f) Emitir alertas tempranas, avisos e información sobre riesgos e incidentes de ciberseguridad para los organismos del sector.
g) Solicitar información anonimizada sobre incidentes de ciberseguridad y vulnerabilidades encontradas a los organismos y/o las instituciones del sector afectadas, así como los planes de acción para mitigarlos dando cumplimiento a los plazos señalados en el presente reglamento, y elaborar informes cuando corresponda.
h) Supervisar el cumplimiento de los estándares y protocolos mínimos de ciberseguridad, así como normas generales, técnicas, instrucciones, alertas y recomendaciones por parte de los organismos del sector.
i) Coordinar la ejecución de ejercicios de simulacro y entrenamiento sectorial para mejorar la preparación y capacidad de respuesta ante incidentes de seguridad informática.
j) Informar al Ministro(a) de Defensa Nacional, a través del Subsecretario(a) de Defensa, las infracciones o incumplimientos en que incurran las instituciones y organismos del sector en relación con las obligaciones y deberes que se establecen en la ley, el presente reglamento y demás que establezcan instrumentos normativos sectoriales sobre ciberseguridad.
k) Entregar los lineamientos para la constitución de los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional.
l) Coordinar con la Agencia lo relativo a estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades, especialmente aquellas de efecto significativo, y respecto a las materias que serán objeto de intercambio de información.
m) Recopilar, gestionar, analizar y compartir con los CSIRT-IDN información sobre las ciberamenazas, vulnerabilidades y/o incidentes relacionados con infraestructuras de Tecnologías de la Información y la Comunicación.
n) Coordinar las respuestas a los incidentes a nivel del sector Defensa, prestando asistencia operativa especializada.
o) Organizar ejercicios de ciberseguridad con el fin de someter a prueba el nivel de ciberseguridad de los organismos e instituciones del sector.
p) Realizar, a solicitud previa del organismo o institución del sector, una exploración proactiva de los sistemas de redes y de información de acceso público de aquella, con el objeto de detectar vulnerabilidades.
q) Coordinar gestión de incidentes y ciberataques de efectos significativos en el sector.
r) Elaborar reportes para el Comité de Ciberdefensa del Ministerio e informes al Ministro(a) de Defensa Nacional sobre vulnerabilidades, incidentes y ciberataques en el sector.

Artículo 14.- Alertas y recomendaciones. El CSIRT-DN emitirá alertas y recomendaciones dirigidas a los CSIRT-IDN.

Las alertas tendrán por objeto comunicar medidas urgentes de seguridad que se deben aplicar en un plazo determinado. Para tal efecto, los CSIRT-IDN, tras haber recibido la alerta, deberán informar al CSIRT-DN, la forma en como se aplicaron.

Las recomendaciones tendrán carácter voluntario para los CSIRT-IDN. Sin embargo, deberán informar al CSIRT-DN los motivos de la decisión de no adoptar o implementar su contenido.

TÍTULO III

LOS EQUIPOS DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA INSTITUCIONALES DE LA DEFENSA NACIONAL

Artículo 15.- De los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional. Los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional, tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, servicios y equipos físicos y de tecnología de la información de los respectivos organismos e instituciones.

Se podrán constituir CSIRT-IDN conforme a los lineamientos entregados por el CSIRT-DN, considerando la disponibilidad presupuestaria de cada organización.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

Artículo 16.- De las funciones de los CSIRT Institucionales de la Defensa Nacional. Los CSIRT-IDN tendrán las siguientes funciones:

a) Asegurar la protección y defensa contra los riesgos y amenazas en el ciberespacio, salvaguardando la confidencialidad, integridad y disponibilidad de las redes de información, de los prestadores de servicios esenciales y operadores de importancia vital, asegurando la protección de la infraestructura crítica de la información (ICI) institucional.
b) Establecer los protocolos y estándares de ciberseguridad institucionales, ajustándose a los protocolos y estándares del CSIRT-DN, así como a los establecidos por la Agencia, para garantizar la prevención, detección, contención, protección y recuperación de los sistemas dentro de su institución.
c) Informar al CSIRT-DN sobre cualquier incidente o vulnerabilidad que afecte sus sistemas, proporcionando los detalles sobre la implementación de los planes de acción requeridos para la recuperación ante dichos incidentes, cumpliendo con los plazos estipulados en el presente reglamento.
d) Compartir alertas tempranas e inteligencia de amenazas con el CSIRT-DN sobre riesgos e incidentes de ciberseguridad que afecten a los organismos del sector Defensa.
e) Realizar ejercicios de simulacro y entrenamiento para mejorar la preparación y capacidad de respuesta ante incidentes de seguridad de la información.
f) Supervisar el cumplimiento de los estándares de ciberseguridad a los prestadores de servicios esenciales y operadores de importancia vital de su institución.
g) Velar por el cumplimiento de las medidas de seguridad establecidas en el organismo o institución, así como de la protección efectiva de la información y los sistemas informáticos involucrados en la prestación de los servicios esenciales.
h) Adoptar o implementar las directrices que emita la autoridad ministerial e informar al CSIRT-DN la no adopción o implementación de las recomendaciones emitidas en el ámbito de sus competencias.

TÍTULO IV

EL PROCEDIMIENTO DE REPORTE DE INCIDENTES DE CIBERSEGURIDAD

Artículo 17.- Obligación de reporte de ciberataques e incidentes. Todos los organismos e instituciones del sector Defensa deberán reportar los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos al CSIRT-DN.

El incumplimiento de la obligación de reporte de ciberataques e incidentes de ciberseguridad, cuando no ponga en riesgo la seguridad y la defensa nacional, será puesto en conocimiento de la Agencia por parte del CSIRT-DN, a fin de que aquella aplique, si corresponde, las sanciones previstas en el Título VII de la ley.

Artículo 18.- Incidentes con efecto significativo.

Conforme al artículo 27 de la Ley Marco, 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:

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

Los CSIRT-IDN, tendrán la obligación de tomar las providencias necesarias para apoyar el restablecimiento del servicio afectado, bajo la coordinación del CSIRT-DN.

El CSIRT-DN reportará a la Agencia los incidentes identificados.

Artículo 19.- Excepción del deber de reporte de incidentes. Sin perjuicio de lo dispuesto en el artículo anterior, si con ello se pusiere en riesgo la seguridad y la defensa nacional, el CSIRT-DN no tendrá el deber de notificar a la Agencia, debiendo informar al Ministerio de Defensa Nacional, a través de la Subsecretaría de Defensa.

Se entenderá que un ciberataque o incidente de ciberseguridad pone en riesgo la seguridad y la defensa nacional cuando se comprometa gravemente la integridad de la información, las redes y los sistemas informáticos de los organismos del sector.

Artículo 20.- Procedimiento de reporte de incidentes de ciberseguridad. La notificación de incidentes de ciberseguridad entre el CSIRT-DN y la Agencia deberá ser realizada conforme a lo

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

establecido en el reglamento de reporte de incidentes de ciberseguridad aprobado por decreto supremo N° 295 de 2024 del Ministerio del Interior y Seguridad Pública, en cuanto a:

- Forma.
- Taxonomía del informe.
- Periodicidad.

Artículo 21.- Plazos de reporte. Para garantizar el cumplimiento del deber de reporte, tratándose de los ciberataques e incidentes de ciberseguridad con efecto significativo, los organismos e instituciones del sector deberán informar al CSIRT-DN conforme a los siguientes plazos:

a) Dentro del plazo máximo de tres horas contadas desde que se tiene conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad que tiene impactos significativos, se deberá enviar una alerta temprana sobre la ocurrencia del evento.
b) Dentro del plazo máximo de setenta y dos horas, se deberá enviar una actualización de la información contemplada en el literal a), que incluya una evaluación inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles. Sin embargo, en caso de que la institución afectada fuera un operador de importancia vital de la defensa y este viera afectada la prestación de los servicios esenciales a causa del incidente, la actualización de la información deberá entregarse al CSIRT-DN en un plazo máximo de 24 horas contadas desde que haya tenido conocimiento del incidente.
c) Dentro del plazo máximo de quince días corridos contados desde el envío de la alerta temprana contemplada en el literal a), se deberá enviar un informe final en el que se recojan al menos los siguientes elementos:

i. Una descripción detallada del incidente, incluyendo su gravedad e impacto.
ii. El tipo de amenaza o causa principal que probablemente haya provocado el incidente.
iii. Las medidas de mitigación aplicadas y en curso.
iv. Si procede, las repercusiones transfronterizas del incidente.

Sin perjuicio de lo anterior, tanto la Agencia, el Ministerio de Defensa Nacional y/o el CSIRT-DN, podrán requerir las actualizaciones pertinentes sobre la situación objeto del reporte.

El CSIRT-DN reportará a la Agencia los ciberataques e incidentes de ciberseguridad de efecto significativo, que le hayan reportado los organismos e instituciones del sector, salvo en los casos previstos en el artículo 19 del reglamento.

Artículo 22.- Protección de datos personales y de carácter secreto al reportar. En los reportes de incidentes de ciberseguridad deberá omitirse 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.

Asimismo, deberá omitirse toda información que tenga el carácter de secreta por afectación a la seguridad y defensa nacional, conforme al ordenamiento jurídico vigente.

TÍTULO V

DE LA RESERVA DE INFORMACIÓN EN MATERIA DE CIBERSEGURIDAD

Artículo 23.- De la reserva de información en materia de ciberseguridad. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder del CSIRT-DN o CSIRT-IDN o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos tome conocimiento en el desempeño de sus funciones o con ocasión de éstas, conforme lo dispone el artículo 33 de la Ley Marco.

Los funcionarios y funcionarias de los CSIRT-DN e institucionales del sector que hubieren tomado conocimiento de los antecedentes a que se refiere el inciso primero, estarán obligados a mantener el carácter secreto de su existencia y contenido aun después del término de sus funciones en los respectivos servicios.

De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de seguridad de la información y los registros previstos en el artículo 8° de la Ley Marco, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad nacional o el interés nacional.

Adicionalmente, será considerada como información secreta o reservada, la siguiente:

i. Las matrices de riesgos de ciberseguridad.
ii. Los planes de continuidad operacional y planes ante desastres.
iii. Los planes de acción y mitigación de riesgos de ciberseguridad.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

Además, se entenderán por documentos secretos aquellos cuyo contenido se relacione directamente con la seguridad del Estado, la Defensa Nacional, el orden público interior o la seguridad de las personas en los términos que establece el artículo 436 del Código de Justicia Militar.

Asimismo, serán considerados reservados o secretos aquellos actos, resoluciones, sus fundamentos y procedimientos concurriendo los requisitos establecidos en el inciso segundo del artículo 8° de la Constitución Política de la República.

NORMAS TRANSITORIAS

Artículo primero.- Todas las instituciones y organismos del sector, dentro del plazo de seis meses contados desde la entrada en vigor del presente reglamento, deben realizar un diagnóstico inicial y evaluar la madurez de ciberseguridad que comprenderá todos los elementos de sus redes y sistemas, debiendo remitir sus resultados al CSIRT-DN, directamente o a través de los CSIRT-IDN. Posteriormente, y dentro del plazo de 12 meses desde la vigencia de este reglamento, todas las instituciones y organizaciones del sector deberán haber implementado completa y efectivamente los protocolos y estándares mínimos de ciberseguridad determinados por el CSIRT-DN, lo que será supervisado por este último a través de los CSIRT-IDN con el fin de garantizar su correcta ejecución y eficacia.

Artículo segundo.- El CSIRT-DN dentro del plazo de 12 meses desde la publicación del presente reglamento, deberá establecer los protocolos y estándares mínimos de ciberseguridad, tanto para la prevención, detección, contención, protección, recuperación de los sistemas y respuesta dependientes de las Fuerzas Armadas y del Estado Mayor Conjunto, considerando los lineamientos establecidos por la Agencia.

Anótese, tómese razón y publíquese.- GABRIEL BORIC FONT, Presidente de la República.- Adriana Delpiano Puelma, Ministra de Defensa Nacional.

Lo que transcribo para su conocimiento.- Ricardo Montero Allende, Subsecretario de Defensa.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl