Boletín N° 16.143-02

Proyecto de ley, iniciado en Mensaje de S.E. el Presidente de la República para la protección de la infraestructura crítica del país.

Santiago, 01 de agosto de 2023

M E N S A J E N°122-371/

Honorable Senado:

A S.E. EL PRESIDENTE DEL H. SENADO

En uso de mis facultades constitucionales, tengo el honor de someter a vuestra consideración el proyecto de ley del rubro, a fin de que sea considerado en el seno de esa H. Corporación:

I. ANTECEDENTES

El 3 de febrero de 2023, se publicó la ley N° 21.542, que Modifica la Carta Fundamental con el objeto de permitir la Protección de Infraestructura Crítica por parte de las Fuerzas Armadas, en caso de peligro grave o inminente. Esta reforma constitucional tuvo su origen en una moción de los H. Senadores y Senadoras Aravena, Elizalde, Pugh, Quintana y Rincón (boletín Nº 15.219-07, refundida con el boletín Nº 13.085-07 del H. Senador Chahuán).

La referida reforma constitucional contenía dos artículos. El primero de ellos, consagró una nueva atribución presidencial mediante la incorporación, en el artículo 32 de la Constitución Política de la República, de un numeral 21º, nuevo. Con esta modificación se facultó al Presidente de la República para disponer de las Fuerzas Armadas (FF.AA.) mediante decreto supremo fundado, con la finalidad de

proteger la infraestructura crítica del país en caso de peligro grave o inminente.

El artículo segundo de la referida reforma constitucional, a su vez, incorporó una disposición quincuagésima tercera transitoria a la Constitución que establece que, dentro de un plazo de seis meses contado desde la publicación de la reforma constitucional, el Presidente de la República debe enviar al Congreso Nacional un Mensaje para regular las distintas materias que menciona el numeral 21°, nuevo, de la Constitución. Estas son, fundamentalmente, los criterios para definir qué se entenderá por infraestructura crítica del país para efectos de su protección, las obligaciones para organismos públicos y entidades privadas a cargo de esta, y las atribuciones y deberes de las FF.AA. en caso de un despliegue dispuesto en conformidad con el artículo 32, numeral 21º, de la Constitución Política de la República. Hoy, mediante el envío del presente Mensaje a esta H. Corporación, el Ejecutivo cumple con dicho compromiso.

A mayor abundamiento, cabe señalar que la antedicha reforma constitucional, en su artículo primero, tiene criterios generales sobre el concepto de infraestructura crítica, entregando a una ley la necesidad de regular los criterios específicos para poder identificar cuándo una determinada infraestructura debe ser considerada como tal para estos efectos.

Cabe considerar además que, actualmente, nuestro ordenamiento jurídico contempla una regulación sectorial de infraestructura crítica en el caso de las telecomunicaciones. La ley N° 20.478, sobre Recuperación y Continuidad en Condiciones Críticas y de Emergencia del Sistema Público de Telecomunicaciones, incorporó a la ley N° 18.168, General de Telecomunicaciones, un título VIII, nuevo, denominado “De las Infraestructuras Críticas de Telecomunicaciones”. El referido título contiene diferentes instrumentos para la protección de cierta infraestructura de telecomunicaciones entendida como crítica para efectos de esa regulación. Es el Ministerio de Transportes y Telecomunicaciones quien debe declarar como infraestructura crítica las redes y sistemas

de telecomunicaciones cuyo daño generaría serio impacto en la seguridad de la población afectada.

Por su parte, el Decreto 60 del año 2012 del Ministerio de Transportes y Telecomunicaciones, establece el Reglamento para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los Sistemas de Telecomunicaciones. Dicho Reglamento contempla una definición de Infraestructura Crítica (IC) del siguiente tenor: "*Corresponde a aquellas redes y sistemas de telecomunicaciones cuya interrupción, destrucción, corte o fallo generaría un serio impacto en la seguridad de la población afectada. Para estos efectos, la I.C. será aquella que sea declarada como tal conforme al artículo 24º del presente Reglamento*" (artículo 2°,letra j).

En relación con lo anterior, es importante destacar que actualmente se encuentra en su segundo trámite constitucional el proyecto de ley que Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (boletín N° 14.847-06). Este proyecto busca establecer la institucionalidad y normativa para estructurar, regular y coordinar las acciones de ciberseguridad.

En consideración de lo anterior, el presente proyecto de ley se aboca a la protección de la infraestructura crítica existente en el territorio nacional. Cabe señalar que durante la tramitación de la ley N° 21.542, se abordó expresamente cuál sería la manera más adecuada de regular esta materia de forma coherente con el boletín N° 14.847-06 antes mencionado. En vista de ello, la redacción del numeral 21° consagró que la infraestructura crítica comprende "el conjunto de instalaciones, sistemas *físicos* o servicios esenciales y de utilidad pública", precisamente con el objeto de excluir los sistemas informáticos y redes que son materia propia de la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

En cuanto al ordenamiento vigente, cabe tener presente el decreto con fuerza de ley N° 1, de 2003, del Ministerio del Trabajo y Previsión Social, que fija el texto refundido, coordinado y sistematizado del Código del Trabajo, el cual, en su artículo 362, determina las empresas en las que no se puede ejercer el derecho a huelga. Estas corresponden a aquellas "corporaciones o empresas, cualquiera sea su naturaleza, finalidad o función, que atiendan servicios de utilidad pública o cuya paralización cause grave daño a la salud, a la economía del país, al abastecimiento de la población o a la seguridad nacional". Estas empresas se determinan mediante resolución conjunta de los Ministros del Trabajo y Previsión Social, Defensa Nacional y Economía, Fomento y Turismo, previa solicitud fundada de parte.

Por su parte, el decreto ley N° 3.607, del año 1981, del Ministerio del Interior, que deroga DL. N° 194, de 1973, y Establece nuevas Normas sobre Funcionamiento de Vigilantes Privados, en su artículo 3° se refiere a "las empresas estratégicas". Estas, junto con los servicios de utilidad pública que se determine, deben contar con su propio servicio de vigilantes privados y mantener un organismo de seguridad interno, del que depende una oficina de seguridad.

Las empresas estratégicas se determinan como tales por decreto supremo con carácter de secreto, firmado por los Ministros o las Ministras del Interior y de Defensa Nacional. Estas entidades, como las demás señaladas en el artículo 3° del mencionado decreto ley deben contar con un plan de seguridad, tramitado y aprobado, de acuerdo a lo dispuesto en el decreto N° 1.773, del año 1981, del Ministerio del Interior, que Aprueba el Reglamento del Decreto Ley N° 3.607, de 1981, sobre Funcionamiento de Vigilantes Privados, y Deroga Decreto N° 315 de 1981.

Por último, en esta misma línea cabe señalar la ley N°19.303 que establece obligaciones a entidades que indica, en materia de seguridad de las personas. Esta ley obliga a determinadas entidades definidas mediante decreto supremo de los Ministerios del Interior y

Seguridad Pública, y de Economía, Fomento y Turismo, previo informe de Carabineros de Chile, a contar con medidas de seguridad.

II. FUNDAMENTOS

En consideración de los antecedentes expuestos este proyecto de ley tiene los siguientes objetivos:

1) Establecer criterios para determinar qué se entenderá por infraestructura crítica del país para los efectos del artículo 32, numeral 21º de la Constitución Política de la República.

2) Crear instrumentos de planificación y gestión para la protección de la infraestructura crítica.

3) Establecer obligaciones para los operadores públicos y privados de la infraestructura catalogada como crítica.

4) Determinar las atribuciones y deberes de las Fuerzas Armadas y de Seguridad y Orden Pública en caso de despliegue dispuesto en conformidad con el artículo 32, numeral 21º, de la Constitución Política de la República.

La regulación propuesta tiene en consideración la experiencia internacional en la materia. Particularmente, el caso español, que cuenta desde el 2011 con la Ley N° 8, por la que se establecen medidas para la protección de la infraestructura crítica ubicada en el territorio español. Esta ley 8/2011 española establece un Sistema de Protección de Infraestructuras Críticas (SPIC) y un Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). A su vez, contempla instrumentos como el Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC), el Catálogo Nacional de Infraestructuras Estratégicas, el Acuerdo sobre Protección de Infraestructuras Críticas, y Planes Estratégicos Sectoriales, de Seguridad del Operador, de Protección Específicos y Planes de Apoyo Operativo.

El órgano rector o principal responsable en este sistema, es la Secretaría de Estado de Seguridad, bajo cuya tutela está la Comisión Nacional para la Protección de las Infraestructuras Críticas, encargada de aprobar los diferentes Planes Estratégicos Sectoriales, y de definir los operadores críticos, a propuesta de un Grupo de Trabajo Interdepartamental.

En cuanto a experiencia comparada se consideró asimismo que el Consejo Europeo, desde el año 2004, empujó una estrategia global para mejorar la protección de infraestructuras crítica. La materia fue adquiriendo mayor relevancia luego de los ataques del 11 de septiembre a las Torres Gemelas en Estados Unidos, a la red de trenes de Madrid el año 2004 y al transporte público en Londres el año 2005. Ello, particularmente ante la necesidad enfrentar el terrorismo y de proteger infraestructura cuya perturbación tendría consecuencias transfronterizas en la comunidad europea, dada su interdependencia.

El año 2008 el Consejo Europeo dictó la Directiva 2008/114/CE, la que define la infraestructura crítica como: "*el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones*".

En el caso de Estados Unidos, luego de los ataques del 11 de septiembre del 2001 se desarrolló un Plan Nacional de Protección de Infraestructuras de Estados Unidos (NIPP). Este aborda la preparación para amenazas y peligros, reducción de vulnerabilidades, mitigación, programas de protección, etc. A su vez, desde el 2018 existe el *National Infrastructure Coordinating Center* (NICC), entidad que forma parte de la División de Seguridad e Infraestructura de la CISA (por sus siglas en inglés, *Cybersecurity and Infrastructure Security*

Agency), vigente desde la *Cybersecurity and Infrastructure Security Agency Act* (2018).

III. CONTENIDOS

El presente proyecto de ley consta de 31 artículos agrupados en seis títulos. Los ejes del proyecto son los siguientes:

1. Instrumentos de gestión y planificación

Uno de los ejes centrales del proyecto es la creación de los siguientes instrumentos de planificación y gestión para la protección de la infraestructura crítica:

a) Listado de sectores y subsectores estratégicos: áreas diferenciadas dentro de la actividad laboral, económica y productiva del país que proporcionan un servicio esencial o necesario para el mantenimiento de las funciones sociales básicas y el normal funcionamiento de la población.

b) Criterios de criticidad e impacto: permiten la valorización de cada infraestructura perteneciente a algún sector estratégico.

c) Catálogo nacional de infraestructura crítica: establece aquellas entidades que, para los efectos del artículo 32 N° 21 de la Constitución Política de la República y de la presente ley, serán consideradas como infraestructura crítica. Es elaborado a partir del listado de sectores y subsectores estratégicos y los criterios de criticidad e impacto.

d) Plan nacional de protección de infraestructura crítica: plan estratégico que define y orienta las acciones y coordinaciones generales a nivel nacional para la protección de la infraestructura crítica. Considera riesgos, amenazas y

vulnerabilidades; coordinación de acciones de prevención y respuesta; alertas tempranas y monitoreo de incidentes.

e) Planes regionales de protección de la infraestructura crítica: define y orienta acciones y coordinaciones a nivel regional para la protección de la infraestructura crítica de cada región.

f) Plan del operador para la protección de infraestructura crítica: presentado al ministerio encargado de la seguridad por cada operador de IC incluido en el Catálogo. Deberá incluir al menos: a) identificación de riesgos, amenazas, vulnerabilidades y elementos importantes de la infraestructura; b) medidas de prevención orientadas a disminuir el riesgo y las vulnerabilidades, y disuadir potenciales ataques; c) medidas para detectar potenciales ataques; d) medidas de respuesta oportuna frente a ataques para reducir impactos, interrumpir ataques y mitigar sus consecuencias; e) sistema de gestión de seguridad para la implementación de estas medidas, alertas, registro de ataques y acciones realizadas y su monitoreo, y la coordinación y comunicación; f) medidas de continuidad operacional; y, g) ejercicios de simulacros y análisis.

2. Obligaciones

Un segundo eje del proyecto consiste en establecer nuevas obligaciones para los operadores públicos y privados de infraestructura crítica en el país. Estas son:

a) Deber de cumplimiento: se requiere cumplir con la presentación de un plan de seguridad y con las medidas del plan ya aprobado.

b) Encargado o encargada de seguridad: se debe designar a una persona encargada de la seguridad, la que deberá ser informada a la autoridad y actuará como contraparte de ésta.

c) Deberes de reporte: se deben reportar al ministerio encargado de la seguridad: (i) todas las alertas de ataques, incidentes o amenazas de ataques, en un plazo de 24 horas; (ii) los detalles de los ataques o incidentes una vez que hayan transcurrido, en un plazo de 7 días; (iii) la identificación de nuevos riesgos, amenazas y vulnerabilidades.

d) Deberes de capacitación: para trabajadores relacionados directamente con la seguridad de la infraestructura respecto del plan del operador de infraestructura crítica, además de fomentar el conocimiento de las medidas entre los trabajadores, cuando ello sea pertinentes para su adecuada protección.

3. Infracciones y sanciones

Se establecen facultades de fiscalización para monitorear el cumplimiento de las obligaciones de operadores de infraestructura crítica, así como infracciones a la ley, clasificadas en gravísimas, graves y leves, con las correspondientes sanciones.

4. Atribuciones y deberes de las fuerzas armadas

Un tercer eje del proyecto es la regulación de las atribuciones y deberes de las Fuerzas Armadas en caso de despliegue para la protección de la infraestructura crítica en conformidad con el artículo 32, numeral 21º, de la Constitución Política de la República. Se establecen a ese respecto atribuciones del Oficial General al mando de las fuerzas, además de las siguientes atribuciones y deberes especiales para las Fuerzas Armadas y Fuerzas de Orden y Seguridad Pública:

a) Control de entrada y salida del perímetro definido.

b) b) Control de identidad y registro de vestimentas, equipaje y vehículos.

c) c) Detención. En los términos de los artículos 120, 130, 131 y 134, todos del Código Procesal Penal, además de ante las faltas previstas en los artículos 495 N° 1 y 496 N° 1, ambos del Código Penal, ante transgresión de orden de autoridad respecto de restricciones de entrada, salida o tránsito, o desobedecimiento de una orden de detenerse.

d) d) Deber de publicidad de las medidas que se adopten para la protección de infraestructura crítica.

5. Principios, deberes y reglas del uso de la fuerza

Se regulan principios y deberes en el uso de la fuerza. Adicionalmente, se establecen reglas precisas y claras para el uso de la fuerza, que ya son conocidas por las Fuerzas Armadas y Fuerzas de Orden y Seguridad, y que regirán hasta la aprobación de una regulación general sobre el uso de la fuerza.

6. Normas adecuatorias

Con el objeto de asegurar la eficacia operacional de la misión de protección de la infraestructura crítica y de resguardo de las áreas de las zonas fronterizas del país, encomendada a un Oficial General al mando de las fuerzas, se ha estimado necesario considerar la participación del Estado Mayor Conjunto, incorporando una letra k) en el artículo 25 de la ley 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional. Esta nueva facultad consistirá en prestar asesoría militar en el trabajo y conducción estratégica conjunta, que demande el despliegue de las Fuerzas Armadas, en el ejercicio de la atribución especial dispuesta en el artículo 32 N°21 de la Constitución Política de la República, en idénticos términos a la actual letra a), que regula la participación del Estado Mayor Conjunto en situaciones que puedan demandar los estados de excepción constitucional.

7. Disposición transitoria

Por último, se establece una disposición transitoria sobre la vigencia de la ley, en caso que el presente proyecto se aprobare, para que los principios y reglas en materia de uso de la fuerza rijan hasta la aprobación de una regulación general del uso de la fuerza, considerando que actualmente se encuentra en tramitación un proyecto de ley que Establece Normas Generales sobre el Uso de la Fuerza para el Personal de las Fuerzas de Orden y Seguridad Pública y de las Fuerzas Armadas en las circunstancias que se señala (boletín N° 15805-07), que tiene por pretensión establecer a nivel legal una regulación armónica de las normas de uso de la fuerza.

En mérito de lo anterior, someto a vuestra consideración, el siguiente

P R O Y E C T O D E L E Y :

“TÍTULO I
DISPOSICIONES GENERALES

Artículo 1°.- Objeto. La presente ley tiene por objeto establecer los criterios para la determinación de la infraestructura crítica del país; definir instrumentos de planificación y gestión para su protección; establecer las atribuciones de los organismos del Estado a cargo de su protección; orientar la coordinación entre los distintos actores; y establecer las obligaciones de las instituciones públicas y privadas operadoras de infraestructura crítica incluidas en el catálogo nacional que define la presente ley. Asimismo, la presente ley regula las atribuciones y deberes de las Fuerzas Armadas en caso de despliegue para la protección de la infraestructura crítica en conformidad con el artículo 32 N° 21 de la Constitución Política de la República.

Artículo 2°.- Definiciones. Para los efectos de esta ley se entenderá por:

1) Sector estratégico: áreas diferenciadas dentro de la actividad laboral, económica y productiva que involucren un servicio esencial o necesario para el mantenimiento de las funciones sociales básicas y el normal funcionamiento de la población.

2) Subsector estratégico: los distintos ámbitos que en conjunto forman un sector estratégico.

3) Operador de infraestructura crítica: institución pública o privada que para la prestación de servicios esenciales utiliza infraestructura que está incluida en el Catálogo nacional de infraestructura crítica.

4) Servicio Esencial: servicio necesario para el mantenimiento de las funciones sociales básicas del país, tales como la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

5) Infraestructura crítica: es aquella determinada en conformidad a los criterios establecidos en la presente ley y que comprende el conjunto de instalaciones, sistemas físicos o servicios esenciales y de utilidad pública, así como aquellos cuya afectación cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país. Se entiende por este concepto la infraestructura indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de los servicios e insumos básicos para la población, tales como energía, gas, agua o telecomunicaciones; la relativa a la conexión vial, aérea, terrestre, marítima, portuaria o ferroviaria, y la correspondiente a servicios de utilidad pública, como los sistemas de asistencia sanitaria o de salud.

Artículo 3°.- Ámbito de aplicación. La presente ley aplicará a la infraestructura crítica ubicada en el territorio nacional y definida como tal en conformidad con el artículo 7° de la presente ley; a los organismos del Estado a cargo de su protección; a las instituciones públicas y privadas operadoras de dicha Infraestructura crítica; y a las Fuerzas Armadas y de Orden y Seguridad Pública dispuestas para su protección.

No se aplicarán las disposiciones de esta ley a la infraestructura del Ministerio de Defensa Nacional, de las Fuerzas Armadas y sus organismos dependientes, que se regirán por su propia normativa y procedimientos.

TÍTULO II
INSTRUMENTOS DE PLANIFICACIÓN Y GESTIÓN PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA

Artículo 4°.- Instrumentos de planificación y gestión. Los instrumentos de planificación y gestión para la protección de la Infraestructura crítica son los siguientes:

1) Listado de Sectores y Subsectores estratégicos.

2) Criterios de criticidad e impacto.

3) Catálogo nacional de infraestructura crítica.

4) Plan nacional de protección de infraestructura crítica.

5) Planes regionales de protección de infraestructura crítica.

6) Plan del operador para la protección de la infraestructura crítica.

Artículo 5°.- Listado de sectores y subsectores estratégicos. El ministerio encargado del gobierno interior deberá definir, mediante resolución dictada por el ministro, previa consulta a la Agencia Nacional de Inteligencia, a través del ministerio encargado de la seguridad, el listado de los sectores y subsectores estratégicos. Esta resolución deberá revisarse y actualizarse cada cuatro años.

Artículo 6°.- Criterios de criticidad e impacto Los criterios de criticidad e impacto son aquellos que permiten la valorización de cada infraestructura perteneciente a algún sub sector estratégico, para determinar el orden y la priorización de aquella que se catalogará como infraestructura critica.

Los criterios de criticidad permiten determinar la relevancia de la infraestructura en un determinado contexto, considerando su función para garantizar la prestación de servicios esenciales y la seguridad de los ciudadanos. Los criterios de criticidad son:

a) **Seguridad:** mide la disponibilidad de sistemas, equipos y elementos destinados al resguardo de las instalaciones de una infraestructura crítica. Por ejemplo, barreras físicas sólidas para personas y vehículos, control de acceso humano y digital, sistemas de identificación físico y biométrico, sensores de movimiento, entre otros.

b) Resiliencia: evalúa la capacidad de recuperación y continuidad del servicio mediante la disponibilidad de sistemas de respaldo.

c) Vulnerabilidad: considera las debilidades existentes en instalaciones o sistemas que, ante una potencial afectación de carácter antrópica, generarían daño tanto a las instalaciones como a la prestación del servicio.

d) Interdependencia: mide el grado de incidencia de un sector o subsector estratégico sobre otros sectores o subsectores.

Los criterios de impacto se utilizan para evaluar las consecuencias que puede tener un determinado evento en una infraestructura. Los criterios de impacto son:

a) Cantidad de personas afectadas: se refiere al número potencial de víctimas mortales o heridas con lesiones graves, ante una interrupción del servicio o afectación a una infraestructura.

b) Impacto económico: evalúa la magnitud de las pérdidas en la actividad económica, el deterioro de productos y servicios, y su efecto en las personas.

c) Impacto operativo: mide el grado de afectación en la operatividad de una infraestructura respecto a la continuidad del servicio en relación con su alcance territorial y usuarios afectados.

d) Impacto en la reputación del Estado: evalúa la percepción respecto a la capacidad de respuesta estatal ante la pérdida o grave deterioro de la prestación de servicios esenciales.

e) Tiempo de recuperación: mide el tiempo requerido para que la infraestructura crítica afectada esté operativa nuevamente.

Artículo 7°.- Catálogo Nacional de Infraestructura Crítica. El Catálogo nacional de infraestructura crítica será elaborado considerando tanto el Listado de sectores y subsectores estratégicos como los Criterios de criticidad e impacto establecidos en la presente ley.

Este catálogo será elaborado por el ministerio encargado del gobierno interior, mediante una o más resoluciones fundadas de la Subsecretaría del Interior sujetas a secreto, y establecerá la que será considerada infraestructura crítica y sus operadores, para los efectos del artículo 32 N° 21, párrafo segundo, de la Constitución Política de la República y de la presente ley.

Este Catálogo deberá revisarse y actualizarse, a lo menos, cada 4 años. Para estos efectos, la Agencia Nacional de Inteligencia, a través del Ministerio encargado de la seguridad, presentará un informe a la Subsecretaría del Interior, que incluya una matriz de identificación de infraestructura crítica.

Para la elaboración de dicha matriz, la Agencia, a través del ministerio encargado de la seguridad, podrá solicitar información a las distintas subsecretarías de todos los ministerios de los sectores estratégicos definidos en conformidad con el articulo 5° de esta ley. Las mencionadas subsecretarías estarán obligadas a proporcionar los antecedentes en los mismos términos en que les sean solicitados, respecto de los cuales deberá guardar estricta reserva.

Asimismo, la Subsecretaría del Interior requerirá a los operadores ya incluidos en el Catálogo o a aquellos que formen parte de un subsector estratégico, toda la información que resulte necesaria a fin de determinar las características de su infraestructura y los criterios de criticidad e impacto de la misma.

La Subsecretaría del Interior, a más tardar cuatro meses antes del término del plazo comunicará por cualquier medio idóneo a los operadores la definición preliminar de la infraestructura que se mantendrá en el Catálogo o que se incorporará o eliminará de tal definición. Los operadores tendrán un plazo máximo de dos meses a contar de la comunicación antes señalada para enviar a la Subsecretaría observaciones fundamentadas acerca de su potencial inclusión o exclusión del Catálogo. Vencido este plazo, con o sin las observaciones fundamentadas, la Subsecretaría dictará la o las resoluciones referidas en el inciso primero.

La inclusión de los operadores dentro de este Catálogo será notificada personalmente, por un funcionario de la Subsecretaría, al representante legal de la entidad respectiva. Si la persona no fuere habida en más de una oportunidad en el respectivo recinto o local, la notificación se efectuará mediante carta certificada. Entendiéndose, en este último caso, notificada la entidad desde el tercer día de enviada la carta.

Los operadores de infraestructura crítica incluidos en el Catálogo serán considerados entidades obligadas a contar con seguridad privada y les serán aplicables todas las disposiciones correspondientes a ese tipo de entidades.

Artículo 8°.- Recursos contra la resolución que establece el Catálogo Nacional de Infraestructura crítica. Los operadores podrán reclamar contra la o las resoluciones en conformidad con lo establecido en la ley N° 19.880. Transcurrido el plazo para que el ministerio encargado del gobierno interior resuelva la reposición sin que lo haya hecho, operará el silencio negativo en la forma establecida en el artículo 65 de la ley N° 19.880.

Procederá asimismo contra la resolución del artículo 7° el reclamo de ilegalidad ante la Corte de Apelaciones de Santiago, el que podrá interponerse en un plazo de 10 días hábiles desde su notificación. La reclamación no podrá ser interpuesta mientras no hayan sido resueltos los recursos que haya interpuesto el operador de infraestructura crítica ante la Administración, suspendiéndose el plazo para la interposición del reclamo de ilegalidad desde la presentación del recurso ante la Administración hasta la notificación de la resolución que lo resuelva o desde que haya operado el silencio negativo.

Ante la interposición de un reclamo de ilegalidad, la Corte de Apelaciones revisará la admisibilidad del mismo, declarando admisible el recurso si el reclamante señala en su escrito, con precisión, el acto u omisión objeto del reclamo, la norma legal que se supone infringida, la forma en que se ha producido la infracción y la razones por las cuales el acto le perjudica.

Admitido a tramitación el reclamo, la Corte de Apelaciones dará traslado al ministro o ministra del ministerio encargado del gobierno interior, que dispondrá de diez días hábiles para presentar sus descargos u observaciones.

Evacuado el traslado o teniéndose por evacuado en rebeldía, la Corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil. Vencido el término de prueba la Corte ordenará traer los autos en relación y la vista de la causa gozará de preferencia. La Corte de Apelaciones, a solicitud de las partes, oirá los alegatos de éstas, y dictará sentencia dentro del término de diez días hábiles desde la vista de la causa.

Si se da lugar al reclamo, la Corte decidirá u ordenará, según sea procedente, la anulación total o parcial del acto impugnado y la dictación de la resolución que corresponda para subsanar la omisión o reemplazar la parte de la resolución anulada.

Los procesos a que den lugar las reclamaciones a que se refieren los incisos anteriores serán secretos y deberán mantenerse en custodia, pudiendo ser conocidos sólo por las partes o sus representantes.

Artículo 9°.- Plan nacional de protección de infraestructura crítica. El Plan nacional de protección de infraestructura crítica es un plan estratégico que define y orienta las acciones y coordinaciones generales a nivel nacional, necesarias para la protección de la Infraestructura crítica. El plan deberá incluir al menos:

1) Un panorama de riesgos, amenazas y vulnerabilidades.

2) Directrices generales para la coordinación de acciones de prevención y respuesta orientadas a disminuir el riesgo, superar las vulnerabilidades y enfrentar las amenazas y ataques.

3) Definición de un sistema de alertas tempranas y monitoreo de incidentes.

El Plan nacional de protección de infraestructura crítica será definido por el ministerio encargado de la seguridad pública mediante decreto supremo sujeto a secreto. Para la elaboración del Plan, el ministerio deberá considerar un informe con recomendaciones del Ministerio de Defensa Nacional, la Agencia Nacional de Inteligencia y las Fuerzas de Orden y Seguridad Pública. Este Plan deberá actualizarse al menos cada 4 años.

Artículo 10°.- Planes regionales de protección de infraestructura crítica. Los planes regionales de protección de infraestructura crítica definen y orientan las acciones y coordinaciones a nivel regional necesarias para la protección de la Infraestructura crítica de cada región del país. Estos planes se basarán en los lineamientos estratégicos del Plan definido en el artículo anterior, y deberán incluir al menos:

1) Un panorama de riesgos, amenazas y vulnerabilidades a nivel regional.

2) Directrices para la coordinación de acciones de prevención y respuesta orientadas a disminuir el riesgo, superar las vulnerabilidades y enfrentar las amenazas y ataques.

Para la elaboración del plan regional, el ministerio encargado de la seguridad pública requerirá un informe con recomendaciones al Ministerio de Defensa Nacional, la Agencia Nacional de Inteligencia y las Fuerzas de Orden y Seguridad Pública. Recibidos los informes, los remitirá a cada representante regional del ministerio encargado de la seguridad pública, los que elaborarán una propuesta de plan regional que será enviada al ministerio encargado de la seguridad pública. Recibida la propuesta, el ministerio encargado de la seguridad pública, mediante uno o más decretos supremos sujetos a secreto, dictado por el o la ministra, aprobarán los respectivos planes regionales. Este Plan deberá actualizarse en concordancia con la actualización del Plan Nacional. El responsable de su implementación y seguimiento será el representante regional del ministerio encargado de la seguridad pública.

Artículo 11.- Plan del operador para la protección de infraestructura crítica. Cada operador de infraestructura crítica deberá elaborar un plan que defina y oriente las acciones y coordinaciones específicas que sean necesarias para la protección de la infraestructura crítica que opere. El plan deberá incluir al menos:

1) Identificación de riesgos, amenazas, vulnerabilidades y elementos importantes de la infraestructura.

2) Medidas de prevención orientadas a disminuir el riesgo y las vulnerabilidades, y disuadir potenciales ataques.

3) Medidas para detectar potenciales ataques.

4) Medidas de respuesta oportuna frente a ataques para reducir impactos, interrumpir ataques y mitigar sus consecuencias.

5) Sistema de gestión de seguridad que incluya la implementación de las medidas indicadas en los numerales anteriores, las alertas, el registro de ataques y acciones realizadas y su monitoreo, y la coordinación y comunicación.

6) Medidas de continuidad operacional.

7) Ejercicios de simulacros y análisis.

El plan del operador para la protección de infraestructura crítica deberá ser presentado al ministerio encargado de la seguridad pública en un plazo de tres meses contados desde que hayan transcurrido los plazos concedidos para la interposición de los recursos de reposición y jerárquico referidos en el artículo 8 o desde que se haya notificado su resolución.

Recibido el estudio de seguridad de la entidad obligada, el ministerio requerirá a la Agencia Nacional de Inteligencia un informe técnico sobre la misma. El informe deberá ser remitido al ministerio en el plazo de 10 días hábiles, el que podrá ser prorrogado hasta por 5 días.

Recibido el informe técnico, el o la ministra resolverá fundadamente aprobar el plan del operador o requerir modificaciones al mismo. La resolución será notificada al correo electrónico que el operador designe en la presentación de su plan ante el ministerio.

Si el ministerio requiriere modificaciones al plan, el operador deberá efectuar las correcciones que correspondan dentro de un plazo de 10 días, el que podrá ser prorrogado hasta por el mismo periodo de tiempo, previa solicitud del operador.

En contra de la resolución que requiera modificaciones sólo procederá el recurso de reposición dentro del plazo de cinco días hábiles a contar de su notificación. En cuanto a la tramitación, plazos y procedimientos de este recurso se aplicará lo señalado en el artículo 59 de la ley N°19.880.

Estos planes deberán ser actualizados cada vez que el operador sea notificado de su inclusión en el Catálogo nacional de infraestructura crítica.

En caso de que el operador de infraestructura crítica sea, asimismo, entidad obligada a contar con medidas de seguridad privada, según la ley de seguridad privada, ambos planes deberán encontrarse debidamente coordinados, deberá, además comunicar al ministerio encargado de la seguridad pública su doble calidad de entidad obligada a contar con medidas de seguridad y de operador de infraestructura crítica.

TÍTULO III
OBLIGACIONES DE LOS OPERADORES DE INFRAESTRUCTURA CRÍTICA

Artículo 12.- Deber de cumplimiento. Los operadores de infraestructura crítica deberán cumplir con la presentación del Plan de seguridad del operador en los plazos establecidos en la presente ley, incluyendo las modificaciones que le haya hecho la autoridad cuando corresponda, o. Asimismo, los operadores de infraestructura crítica deberán cumplir con las medidas contenidas en el Plan de seguridad del operador.

Artículo 13.- Encargado o encargada de seguridad de la infraestructura crítica. Los operadores de infraestructura crítica deberán designar a una persona encargada de seguridad, cuya designación deberá ser informada al tiempo de presentarse el Plan de seguridad del operador de infraestructura crítica. La persona encargada actuará como contraparte del Ministerio encargado del Gobierno Interior y del Ministerio encargado de la Seguridad Pública y sus respectivos servicios para efectos de lo establecido en la presente ley, y dependerá directamente de la persona que tenga máxima autoridad con facultades administrativas en la entidad operadora, en caso de ser un operador privado, o del jefe de servicio o del organismo, en caso de ser una entidad pública.

Artículo 14. Deberes de reporte. Los operadores de infraestructura crítica deberán reportar al ministerio encargado de la seguridad lo siguiente:

a) Todas las alertas de ataques, incidentes o amenazas de ataques, en un plazo de 24 horas desde que hayan tomado conocimiento de los mismos.

b) Los detalles de los ataques o incidentes una vez que estos hayan transcurrido, en un plazo de 7 días, desde que los mismos hayan comenzado a ocurrir.

c) La identificación de nuevos riesgos, amenazas y vulnerabilidades, en cuanto se tome conocimiento de los mismos.

Asimismo, los operadores de infraestructura que formen parte de un subsector estratégico tendrán el deber de entregar a las autoridades competentes la información solicitada en el marco de la elaboración del Catálogo según lo dispuesto en el artículo 7°.

Artículo 15.- Deber de capacitación. Los operadores de infraestructura crítica deberán contar con capacitaciones del plan referido en el artículo 11 para los trabajadores relacionados directamente con la seguridad de la infraestructura. Sin perjuicio de lo anterior, deberán fomentar el conocimiento de las medidas entre sus trabajadores, cuando ello sea pertinente para su adecuada protección.

TÍTULO IV
INFRACCIONES Y SANCIONES

Artículo 16.- Fiscalización. La fiscalización del cumplimiento de las obligaciones establecidas en la presente ley se realizará por el Ministerio encargado de la Seguridad Pública, a través de la Subsecretaría de Prevención del Delito y de la Autoridad Fiscalizadora, en conformidad con la regulación establecida para las entidades obligadas.

Artículo 17.- Clases de infracciones. Las infracciones a esta ley se clasifican en gravísimas, graves o leves y solo podrán ser sancionadas con multas en conformidad con el procedimiento sancionatorio establecido para las entidades obligadas.

En caso de que la entidad sancionada sea una institución pública, la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado respectivo se regirá por lo dispuesto en el artículo 21.

Artículo 18.- Infracciones gravísimas. Sin perjuicio de los delitos e infracciones establecidas en otras leyes, son infracciones gravísimas:

a) Presentar antecedentes falsos ante el ministerio encargado del gobierno interior, el ministerio encargado de la seguridad pública, y sus respectivos servicios, o ante la Autoridad Fiscalizadora, ya sea en la presentación del plan del operador, en el contexto de una fiscalización sobre el cumplimiento de las normas legales o reglamentarias, o en cualquier otra circunstancia.

b) No presentación del plan del operador.

c) No implementar las medidas establecidas en las letras b), c), d), e) y f) del artículo 11 de la presente ley.

d) No contar con encargado o encargada de seguridad de la infraestructura crítica o contar con una persona distinta a la informada.

e) Oponerse u obstaculizar las labores de la Autoridad Fiscalizadora.

f) No reportar una alerta de ataque, incidente o amenaza de ataque.

Artículo 19.- Infracciones graves. Son infracciones graves:

a) No presentar, dentro de los plazos establecidos en esta ley, el plan del operador de infraestructura crítica, o las modificaciones que fueren requeridas.

b) Implementar las medidas establecidas en las letras b), c), d), e) y f) del artículo 11 de esta ley en una forma distinta de la aprobada.

c) Reportar una alerta de ataque, incidente o amenaza de ataque en forma distinta a la establecida en el artículo 14 letra a) de la presente ley.

d) Incumplir con los demás deberes de reporte establecidos en el artículo 14 de la presente ley.

e) No subsanar las irregularidades señaladas por las autoridades fiscalizadoras durante posibles fiscalizaciones, en el plazo otorgado por la Subsecretaría de Prevención del Delito para ello.

f) No realizar las capacitaciones de conformidad con lo establecido en el artículo 15 de la presente ley.

Artículo 20.- Infracciones leves. Son infracciones leves:

a) No implementar los ejercicios de simulacros y análisis o hacerlo en una forma distinta a la aprobada.

b) Cumplir de forma extemporánea con los deberes de reporte establecidos en el artículo 14 letras b) y c) de la presente ley.

c) Cualquier otro acto u omisión que contravenga las obligaciones establecidas en esta ley y que no constituyan infracción gravísima o grave, de acuerdo con lo previsto en los artículos anteriores.

Artículo 21.- Fiscalización y sanciones respecto de entidades públicas. La autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado, deberá informar a la Subsecretaría de Prevención del Delito del estado del cumplimiento de las obligaciones señaladas en el título III, de acuerdo con las instrucciones y plazos que fije dicha Subsecretaría.

La autoridad o jefatura que incumpla lo dispuesto en el inciso anterior o las disposiciones establecidas en el título III de la presente ley, será sancionado por la Contraloría General de la República con multa de 20% a 50% de su remuneración. Al efecto, dicho organismo incoará un sumario administrativo de acuerdo con su ley orgánica y establecerá la multa que corresponda. El porcentaje de la multa se determinará considerando la gravedad de la infracción de acuerdo con lo señalado en los artículos anteriores.

Para efectos de este artículo, la Subsecretaría de Prevención del Delito, informará a la Contraloría General de la República el incumplimiento de la obligación señalada en el inciso primero, como, asimismo, los eventuales incumplimientos a las disposiciones establecidas en la presente ley.

La Contraloría General de la República, deberá requerir a la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado que corresponda, para que, dentro del plazo de diez días hábiles, informe el estado de cumplimiento de las disposiciones señaladas.

TÍTULO V
ATRIBUCIONES Y DEBERES DE LAS FUERZAS ARMADAS EN LA PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA EN CONFORMIDAD AL ARTÍCULO 32 N°21 DE LA CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA

Artículo 22.- De la protección de la infraestructura crítica por parte de las Fuerzas Armadas. Las Fuerzas Armadas se harán cargo de la protección de la infraestructura crítica cuando así lo determine el Presidente de la República, a través de un decreto supremo fundado, suscrito por los Ministros del Interior y Seguridad Pública y de Defensa Nacional, de conformidad a lo dispuesto en el artículo 32 N° 21 de la Constitución Política de la República, en el área determinada por dicho decreto supremo. Las Fuerzas Armadas que se encuentren a cargo de la protección de la infraestructura crítica dentro del área referida, actuarán de conformidad a las atribuciones y deberes regulados en la presente ley que se le otorguen en el decreto supremo y a las instrucciones que establezca el Ministerio del Interior en el decreto supremo.

El ejercicio de las atribuciones establecidas en la presente ley, en ningún caso implicará la suspensión, restricción o limitación de los derechos y garantías consagrados en la

Constitución o en tratados internacionales de derechos humanos, ratificados por Chile y que se encuentren vigentes.

Las eventuales afectaciones sólo podrán enmarcarse en el cumplimiento del deber de resguardo del orden público para la protección de la infraestructura crítica de conformidad a las atribuciones establecidas en esta ley.

El uso de la fuerza estará siempre sujeto a los deberes, principios y reglas establecidos en la legalidad vigente.

Artículo 23.- Atribuciones del Oficial General. El Oficial General al mando de las Fuerzas Armadas y de Seguridad y Orden Público, designado por el Presidente de la República para la protección de la infraestructura crítica determinada, contará con las siguientes atribuciones:

1) Asumir el mando de las Fuerzas Armadas y de Orden y Seguridad Pública, que se encuentren desplegadas para la protección de la infraestructura crítica determinada para los efectos de velar por el orden público y de reparar o precaver el daño o peligro para la infraestructura crítica que haya dado origen a su protección, debiendo observar las facultades administrativas de las autoridades institucionales con competencia en el área especificada en el decreto supremo.

2) Disponer el control de la entrada y salida del perímetro estrictamente necesario en torno a la infraestructura crítica a proteger, que en ningún caso podrá exceder el alcance de los medios probables de ataque utilizados y que en cualquier caso deberá encontrarse dentro del área especificada por el decreto supremo señalado en el artículo 17 de esta ley.

3) Dictar las directrices e instrucciones a las Fuerzas Armadas y de Orden y Seguridad Pública bajo su mando necesarias para el mantenimiento del orden en el área determinada en el decreto supremo para la protección de la infraestructura crítica.

4) Velar por el conocimiento y respeto de los derechos humanos y de los deberes, principios y la aplicación de las reglas de uso de la fuerza de conformidad a la legalidad vigente.

5) Dictar instrucciones a las Fuerzas Armadas y de Orden y Seguridad Pública desplegadas para la protección de la infraestructura crítica con el objeto de evitar la divulgación de antecedentes de carácter militar.

6) Coordinar con todos los funcionarios del Estado, de sus empresas o de las municipalidades que se encuentren en la zona con el objeto de mantener la protección o subsanar el daño en la infraestructura crítica.

Artículo 24.- Control de entrada y salida. Las Fuerzas Armadas podrán controlar la entrada y salida del perímetro estrictamente necesario en torno a la infraestructura crítica a proteger, que en ningún caso podrá exceder el alcance de los medios probables de ataque utilizados y que en cualquier caso deberá encontrarse dentro del área especificada por el decreto supremo señalado en el artículo 22 de esta ley.

Artículo 25.- Control de identidad y registro. Las Fuerzas Armadas podrán controlar la identidad de cualquier persona que pretenda ingresar o se encontrare dentro de los límites territoriales de las áreas determinadas para la protección de la infraestructura crítica. Asimismo, podrán llevar a cabo el registro de sus vestimentas, equipaje o vehículo, en los términos señalados en los artículos 85 y 86 del Código Procesal Penal.

El control se limitará a los casos en que exista algún indicio de que la persona hubiere cometido o intentado cometer un crimen, simple delito o falta; de que se dispusiere a cometerlo; o se contare con algún antecedente que permita inferir que la persona tiene una orden de detención pendiente o en el caso de la persona que se encapuche o emboce para ocultar, dificultar o disimular su identidad. Sin perjuicio de lo anterior, las Fuerzas estarán facultades para practicar el control de identidad previsto en el artículo 12 de la ley Nº 20.931, así como la facultad prevista en el artículo 12 bis de la misma ley.

Para practicar el examen de vestimentas, se comisionará a personas del mismo género, de ser posible, y se deberá ejecutar con respeto a los derechos humanos que le asisten conforme con la Constitución y la ley.

Artículo 26.- Detención. Las Fuerzas, podrán practicar detenciones en los términos descritos en los artículos 129, 130, 131 y 134 del Código Procesal Penal, con la sola finalidad de poner a la persona a disposición de las Fuerzas de Orden y Seguridad Pública, lo que se llevará a cabo en el más breve plazo posible. Asimismo, darán cumplimiento al deber de información al detenido prescrito en el artículo 135 del mismo código.

Asimismo, podrá ser detenido quien hubiere cometido alguna de las faltas contempladas en los artículos 495 N° 1 y 496 N° 1 del Código Penal, cuando hubiere transgredido la orden de autoridad respecto a las restricciones de entrada o salida, o cuando desobedeciere una orden de detenerse, sea respecto de una persona a pie o del conductor de un vehículo, en las zonas delimitadas para la protección de la infraestructura crítica.

Artículo 27.- Deber de publicidad. Todas las medidas que se adopten para la protección de la infraestructura crítica y que afecten el normal desarrollo de las actividades de la población deberán ser difundidas o comunicadas, en la forma que la autoridad determine, lo que en ningún caso podrá implicar discriminación entre medios de comunicación.

Artículo 28.- Principios y deberes en el uso de la fuerza. Los integrantes de las Fuerzas Armadas y Fuerzas de Orden y Seguridad dispuestas para la protección de la infraestructura crítica deberán guiar su actuación en el uso de la fuerza por los siguientes principios y deberes, sin perjuicio de lo previsto en otras disposiciones jurídicas que sean aplicables:

a) Principio de legalidad: La acción que realicen las Fuerzas debe efectuarse dentro del marco de la Constitución Política de la República, la ley y los tratados internacionales en materia de derechos humanos ratificados por Chile y que se encuentren vigentes, y debe efectuarse atendiendo un objetivo legítimo relativo a la protección de la Infraestructura crítica.

b) Principio de necesidad: En el cumplimiento del deber de proteger la Infraestructura crítica se puede utilizar la fuerza solo cuando sea estrictamente necesaria para cumplir el deber.

c) Principio de proporcionalidad: El tipo y nivel de fuerza empleada y el daño que puede razonablemente resultar, debe considerar la gravedad de la ofensa y ser proporcional al objetivo del mandato constitucional de protección de la Infraestructura crítica de conformidad con las instrucciones contenidas en el respectivo decreto supremo.

d) Principio de gradualidad: Siempre que la situación operativa lo permita, se deben realizar todos los esfuerzos procedentes para resolver situaciones potenciales de confrontación, a través de la comunicación, persuasión, negociación, disuasión y empleo de medios disuasivos y, en última instancia, armas de fuego.

e) Principio de responsabilidad: El uso de la fuerza, fuera de los parámetros permitidos por la ley, no solo conlleva las responsabilidades individuales por las acciones y omisiones incurridas, sino, cuando corresponda, también las demás establecidas en el ordenamiento jurídico.

f) Deber de advertencia: Antes de recurrir al uso de la fuerza o empleo del arma de fuego, se deben tomar todas las medidas razonables para disuadir a toda persona o grupo de cometer una agresión que atente contra algún integrante de las Fuerzas Armadas y Fuerzas de Orden y Seguridad Pública, contra las Fuerzas en su totalidad, contra el deber de protección de la Infraestructura crítica, o que alteren el orden y seguridad pública, o que producto de ello afecte a otras personas o sus derechos.

g) Deber de evitar daño colateral: Cuando se recurra al uso de la fuerza, se deben tomar las medidas necesarias para evitar daños colaterales, en particular respecto de la vida e integridad física de las personas. Se procurará la debida asistencia de primeros auxilios a las personas afectadas.

h) Cumplimiento del deber y legítima defensa: Ninguna de las disposiciones de la presente ley limita el derecho a repeler ataques a la integridad física o la vida, ni la justificación del uso de la fuerza por el cumplimiento del deber.

i) Deber de información: El mando deberá informar, en el más breve plazo, al Ministerio del Interior y Seguridad Pública y al Ministerio de Defensa Nacional de cualquier incidente en que se haya hecho uso de la fuerza.

Artículo 29.- Reglas del uso de la fuerza. Los oficiales generales al mando de las Fuerzas Armadas y Fuerzas de Orden y Seguridad Pública dispuestas para la protección de la infraestructura crítica implementarán las siguientes Reglas de Uso de la Fuerza y, en el ejercicio de sus atribuciones, podrán precisarlas de acuerdo con las circunstancias, de conformidad a los principios y deberes enunciados en el artículo anterior:

Regla Nº 1. Empleo disuasivo de vehículos militares, porte de armas y despliegue de fuerzas.

Regla Nº 2. Identificarse como parte de las Fuerzas Armadas o de Orden y Seguridad Pública de Chile, según corresponda. Efectuar negociación, demostración visual, advertencias verbales.

Regla Nº 3. Empleo disuasivo de fumígenos (granadas de humo, gas pimienta o lacrimógeno, entre otros), sistemas de sonido, luz o agua.

Regla Nº 4. Empleo disuasivo de dispositivos o armamentos no letales: bastones, dispositivos eléctricos, proyectiles de pintura, de gas pimienta y lacrimógeno, y otros análogos.

Regla Nº 5. Empleo de armamento antidisturbios, sin disparar a quemarropa ni apuntar directo al rostro, evitando apuntar a la parte superior del torso.

Regla Nº 6. Preparar el arma de fuego con clara intención de utilizarla.

Regla Nº 7. Usar armas de fuego como último recurso, cuando las medidas anteriormente señaladas resultaren insuficientes, y sólo en el caso de enfrentamiento con personas que utilicen o se apresten a utilizar armas de fuego u otras armas letales, o pongan en peligro, de algún otro modo, la vida de otras personas, y no pueda reducirse o detenerse a la persona aplicando medidas menos extremas.

Podrá hacerse uso de la fuerza potencialmente letal cuando, con la intención de dañar gravemente infraestructura crítica, se usaren medios que por su naturaleza sean de amplio poder destructivo y puedan causar estragos, lo que hace presumir que la concreción de su uso causaría los efectos contra la vida e integridad física señalados en el inciso anterior; o como medida extrema procedente solo cuando resulten insuficientes las medidas establecidas en las etapas previas para el cumplimiento del deber de protección de la infraestructura crítica en caso de ataque inminente.

Deberá evitarse el uso de armas de fuego, especialmente, en presencia de menores de edad.

Regla N° 8. Deber de informar. Deberá informarse, en el más breve plazo, al Ministerio del Interior y Seguridad Pública de cada incidente que haya ocurrido con ocasión del uso de la fuerza.

Regla N° 9. Si a propósito del uso de la fuerza resultaren personas heridas, deberán prestársele los auxilios necesarios para resguardar su salud.

Las reglas anteriormente señaladas no obstan a la aplicación del Código Penal y del Código de Justicia Militar, entendiéndose que forman parte de la normativa aplicable.

TÍTULO VII
NORMAS ADECUATORIAS

Artículo 30.- Agrégase, en el artículo 25 de la ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional, un literal k), nuevo, del siguiente tenor: “k) Prestar asesoría militar en el trabajo y conducción estratégica que demande el despliegue de las Fuerzas Armadas, en el ejercicio de la atribución especial dispuesta en el artículo 32 N° 21 de la Constitución Política de la República, para la protección de la infraestructura crítica y para el resguardo de las áreas de las zonas fronterizas del país.”.

DISPOSICIONES TRANSITORIAS

Artículo transitorio.- Los artículos 28 y 29 de la presente ley mantendrán su vigencia mientras no entre en vigencia una ley general que norme el uso de la fuerza por la Fuerzas de Orden y Seguridad Pública y Fuerzas Armadas.”.

Dios guarde a V.E.

GABRIEL BORIC FONT
Presidente de la República

CAROLINA TOHÁ MORALES
Ministra del Interior
y Seguridad Pública

MAYA FERNÁNDEZ ALLENDE
Ministra de Defensa Nacional

ÁLVARO ELIZALDE SOTO
Ministro
Secretaria General de la Presidencia