Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas habilita al Gobierno, en su disposición final cuarta, para dictar el Reglamento de ejecución de desarrollo de la mencionada Ley.

En cumplimiento de este mandato, el presente real decreto se aprueba, en primer lugar, con la finalidad de desarrollar, concretar y ampliar los aspectos contemplados en la citada Ley, máxime cuando del tenor de la misma se desprende no sólo la articulación de un complejo Sistema de carácter interdepartamental para la protección de las infraestructuras críticas, compuesto por órganos y entidades tanto de las Administraciones Públicas como del sector privado, sino el diseño de todo un planeamiento orientado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o actos intencionados provenientes de figuras delictivas como el terrorismo, potenciados a través de las tecnologías de la comunicación.

En segundo lugar, este texto normativo no sólo es coherente con el marco legal del que trae causa, sino que además sirve a los fines del Sistema Nacional de Gestión de Situaciones de Crisis y cumple con la transposición obligatoria de la Directiva 2008/114/CE, del Consejo de la Unión Europea, de 8 de diciembre, en vigor desde el 12 de enero de 2009, sobre la identificación y designación de Infraestructuras Críticas

Europeas y la evaluación de la necesidad de mejorar su protección. A ello obedecen las amplias previsiones que el texto contempla en el ámbito de los diferentes Planes que deben elaborar tanto las Administraciones Públicas –en el caso del Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales y los Planes de Apoyo Operativo– como las empresas, organizaciones o instituciones clasificadas como operadores críticos, a quienes la Ley asigna una serie de obligaciones, entre las que se encuentran la elaboración de sendos instrumentos de planificación: los Planes de Seguridad del Operador y los Planes de Protección Específicos.

Asimismo, la Ley prevé que los operadores críticos designen a un Responsable de Seguridad y Enlace –a quien se exige la habilitación de director de seguridad que concede el Ministerio del Interior al personal de seguridad de las empresas de Seguridad Privada en virtud de lo dispuesto en el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, o habilitación equivalente, según su normativa específica–. Igualmente, se contempla la designación de un Delegado de Seguridad por cada una de las infraestructuras críticas identificadas.

En lo que a su contenido se refiere, el presente real decreto consta de un artículo único, una disposición transitoria única y dos disposiciones finales. Por su parte, el Reglamento consta de 36 artículos estructurados en cuatro Títulos. El Título I contiene las cuestiones generales relativas a su objeto y ámbito de aplicación, y dedica un artículo a la figura del Catálogo Nacional de Infraestructuras Estratégicas, como instrumento de la Secretaría de Estado de Seguridad del Ministerio del Interior que debe aglutinar todos los datos y la valoración de la criticidad de las citadas infraestructuras y que será empleado como base para planificar las actuaciones necesarias en materia de seguridad y protección de las mismas, al nutrirse de las aportaciones de los propios operadores. El

Título II está plenamente dedicado al Sistema de Protección de Infraestructuras Críticas, y desarrolla, entre otras, las previsiones legales relativas a los órganos creados por la Ley, esto es, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), la Comisión Nacional para la Protección de las Infraestructuras Críticas y el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, concretando la composición, competencias y funcionamiento de todos ellos. El Título III se encarga de la regulación de los instrumentos de planificación, centrándose en cada uno de los Planes antes citados, cuyo proceso de elaboración, aprobación y registro, así como sus contenidos materiales, regula con mayor detalle. Finalmente, el Título IV está consagrado a la seguridad de las comunicaciones y a las figuras del Responsable de Seguridad y Enlace y del Delegado de Seguridad de la infraestructura crítica.

La tramitación del presente real decreto ha sido fruto de un intenso diálogo y colaboración entre los distintos Departamentos Ministeriales y organismos afectados, contando también con la aportación de las distintas Comunidades Autónomas y del sector empresarial, tras el trámite de información pública otorgado a todos ellos, lo que ha contribuido a dotar al texto de un extenso y, por otro lado, imprescindible, grado de consenso.

En su virtud, a propuesta del Vicepresidente Primero del Gobierno y Ministro del Interior, con la aprobación previa del Vicepresidente Tercero del Gobierno y Ministro de Política Territorial y Administración Pública, con el informe favorable de la Vicepresidenta Segunda del Gobierno y Ministra de Economía y Hacienda, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 20 de mayo de 2011,

DISPONGO:

Subir

[Bloque 2: #ti]

TÍTULO I

Subir

[Bloque 3: #aunico]

Artículo único. Aprobación del Reglamento de Protección de las infraestructuras críticas.

En desarrollo y ejecución de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, se aprueba el Reglamento de Protección de las Infraestructuras Críticas, cuyo texto se inserta a continuación.

Subir

[Bloque 4: #dtunica]

Disposición transitoria única. Unidades y puestos de trabajo con nivel orgánico inferior a Subdirección General.

Las unidades y puestos de trabajo con nivel orgánico inferior a Subdirección General del Centro Nacional para la Protección de las Infraestructuras Críticas continuarán subsistentes y serán retribuidos con cargo a los mismos créditos presupuestarios, hasta que se aprueben las relaciones de puestos de trabajo adaptadas a la estructura organizativa proyectada en el ámbito de la protección de las infraestructuras críticas. Dicha adaptación en ningún caso podrá generar incremento de gasto público.

Subir

[Bloque 5: #dfprimera]

Disposición final primera. Título competencial.

Este real decreto se dicta al amparo de la competencia atribuida al Estado en materia de seguridad pública en el artículo 149.1.29.ª de la Constitución.

Subir

[Bloque 6: #dfsegunda]

Disposición final segunda. Entrada en vigor.

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Subir

[Bloque 7: #firma]

Dado en Madrid, el 20 de mayo de 2011.

JUAN CARLOS R.

El Vicepresidente Primero del Gobierno y Ministro del Interior,

ALFREDO PÉREZ RUBALCABA

Subir

[Bloque 8: #reglamento]

REGLAMENTO DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Subir

[Bloque 9: #ti-2]

TÍTULO I

Disposiciones generales

Subir

[Bloque 10: #ci]

CAPÍTULO I

Objeto y ámbito de aplicación

Subir

[Bloque 11: #a1]

Artículo 1. Objeto.

1. El presente reglamento tiene por objeto desarrollar el marco previsto en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, a fin de concretar las actuaciones de los distintos órganos integrantes del Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) así como los diferentes instrumentos de planificación del mismo.

2. Asimismo, regula las especiales obligaciones que deben asumir tanto el Estado como los operadores de aquellas infraestructuras que se determinen como críticas, según lo

dispuesto en el artículo 2, párrafos e) y f) de la citada Ley.

Subir

[Bloque 12: #a2]

Artículo 2. Ámbito de aplicación.

El ámbito de aplicación del presente reglamento será el previsto por el artículo 3 de la Ley 8/2011, de 28 de abril.

Subir

[Bloque 13: #cii]

CAPÍTULO II

El Catálogo Nacional de Infraestructuras Estratégicas

Subir

[Bloque 14: #a3]

Artículo 3. El Catálogo Nacional de Infraestructuras Estratégicas.

1. El Catálogo Nacional de infraestructuras estratégicas (en adelante, el Catálogo) es el registro de carácter administrativo que contiene información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, incluyendo las críticas así como aquéllas clasificadas como críticas europeas que afecten a España, con arreglo a la Directiva 2008/114/CE.

2. La finalidad principal del Catálogo es valorar y gestionar

los datos disponibles de las diferentes infraestructuras, con el objetivo de diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza contra aquéllas y, en caso de ser necesario, activar, conforme a lo previsto por el Plan Nacional de Protección de las Infraestructuras Críticas, una respuesta ágil, oportuna y proporcionada, de acuerdo con el nivel y características de la amenaza de que se trate.

Subir

[Bloque 15: #a4]

Artículo 4. Contenido del Catálogo.

1. En el Catálogo deberán incorporarse, entre otros datos, los relativos a la descripción de las infraestructuras, su ubicación, titularidad y administración, servicios que prestan, medios de contacto, nivel de seguridad que precisan en función de los riesgos evaluados así como la información obtenida de las Fuerzas y Cuerpos de Seguridad.

2. El Catálogo se nutrirá de la información que le faciliten al Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, CNPIC) los operadores de las infraestructuras así como el resto de sujetos responsables del Sistema relacionados en el artículo 5 de la Ley 8/2011, de 28 de abril.

3. El Catálogo Nacional de Infraestructuras Estratégicas tiene, conforme a lo dispuesto en la legislación vigente en materia de secretos oficiales, la calificación de SECRETO, conferida por Acuerdo de Consejo de Ministros de 2 de noviembre de 2007, calificación que comprende, además de los datos contenidos en el propio Catálogo, los equipos, aplicaciones informáticas y sistemas de comunicaciones inherentes al mismo, así como el nivel de habilitación de las

personas que pueden acceder a la información en él contenida.

Subir

[Bloque 16: #a5]

Artículo 5. Gestión y actualización del Catálogo.

1. La custodia, gestión y mantenimiento del Catálogo Nacional de infraestructuras estratégicas corresponde al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad.

2. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será responsable de clasificar una infraestructura como estratégica y, en su caso, como infraestructura crítica o infraestructura crítica europea, así como de incluirla por vez primera en el Catálogo, previa comprobación de que cumple uno o varios de los criterios horizontales de criticidad previstos en el artículo 2, apartado h) de la Ley 8/2011, de 28 de abril.

3. El proceso de identificación de una infraestructura como crítica se realizará por el CNPIC, que podrá recabar la participación y el asesoramiento del interesado, así como de los agentes del Sistema competentes, a los que informará posteriormente del resultado de tal proceso.

4. La clasificación de una infraestructura como crítica europea supondrá la obligación adicional de comunicar su identidad a otros Estados miembros que puedan verse afectados de forma significativa por aquélla, de acuerdo con lo previsto por la Directiva 2008/114/CE. En tal caso, las notificaciones, en reciprocidad con otros Estados miembros, se realizarán por el CNPIC, de acuerdo con la clasificación de seguridad que corresponda según la normativa vigente.

5. En los casos en que se produzca una modificación relevante que afecte a las infraestructuras inscritas y que sea de

interés a los efectos previstos en el presente reglamento, los operadores críticos responsables de las mismas facilitarán, a través de los medios puestos a su disposición por el Ministerio del Interior, los nuevos datos de aquéllas al CNPIC, que deberá validarlos con carácter previo a su incorporación al Catálogo. En todo caso, la actualización de los datos disponibles deberá hacerse con periodicidad anual.

Subir

[Bloque 17: #tii]

TÍTULO II

Los agentes del Sistema de Protección de Infraestructuras Críticas

Subir

[Bloque 18: #a6]

Artículo 6. La Secretaría de Estado de Seguridad.

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las Infraestructuras Críticas Nacionales, para lo cual su titular, u órgano en quien delegue, ejercerá las siguientes funciones:

a) Diseñar y dirigir la estrategia nacional de protección de infraestructuras críticas.

b) Aprobar el Plan Nacional de Protección de las Infraestructuras Críticas y dirigir su aplicación, declarando en su caso los niveles de seguridad a establecer en cada momento, conforme al contenido de dicho Plan y en coordinación con el Plan de Prevención y Protección Antiterrorista.

c) Aprobar los Planes de Seguridad de los Operadores y sus actualizaciones a propuesta del CNPIC, tomando en su caso, como referencia, las actuaciones del órgano u organismo competente para otorgar a aquéllos las autorizaciones correspondientes en virtud de su normativa sectorial.

d) Aprobar los diferentes Planes de Protección Específicos o las eventuales propuestas de mejora de éstos a propuesta del CNPIC, en los términos de lo dispuesto en el artículo 26 de este reglamento.

e) Aprobar los Planes de Apoyo Operativo, así como supervisar y coordinar la implantación de los mismos y de aquellas otras medidas de prevención y protección que deban activarse tanto por las Fuerzas y Cuerpos de Seguridad y por las Fuerzas Armadas, en su caso, como por los propios responsables de seguridad de los operadores críticos.

f) Aprobar, previo informe del CNPIC, la declaración de una zona como crítica, a propuesta de las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

g) Identificar los diferentes ámbitos de responsabilidad en la protección de infraestructuras críticas; analizando los mecanismos de prevención y respuesta previstos por cada uno de los actores implicados.

h) Emitir las instrucciones y protocolos de colaboración dirigidos tanto al personal y órganos ajenos al Ministerio del Interior como a los operadores de las infraestructuras estratégicas, así como fomentar la adopción de buenas prácticas.

i) Responder del cumplimiento de las obligaciones y compromisos asumidos por España en el marco de la Directiva

2008/114/CE, sin perjuicio de las competencias que corresponden al Ministerio de Asuntos Exteriores y de Cooperación.

j) Supervisar, dentro del ámbito de aplicación de este reglamento, los proyectos y estudios de interés y coordinar la participación en programas financieros y subvenciones procedentes de la Unión Europea.

k) Colaborar con los Ministerios y organismos integrados en el Sistema en la elaboración de toda norma sectorial que se dicte en desarrollo de la Ley 8/2011, de 28 de abril y del presente reglamento.

l) Cualesquiera otras funciones que, eventualmente, pudieran acordarse por la Comisión Delegada del Gobierno para Situaciones de Crisis.

Subir

[Bloque 19: #a7]

Artículo 7. El Centro Nacional para la Protección de las Infraestructuras Críticas.

El CNPIC del Ministerio del Interior, orgánicamente dependiente de la Secretaría de Estado de Seguridad, tendrá el nivel orgánico que se determine en la correspondiente relación de puestos de trabajo, y desempeñará las siguientes funciones:

a) Asistir al Secretario de Estado de Seguridad en la ejecución de sus funciones en materia de protección de infraestructuras críticas, actuando como órgano de contacto y coordinación con los agentes del Sistema.

b) Ejecutar y mantener actualizado el Plan Nacional de Protección de las Infraestructuras Críticas conforme a lo previsto en el artículo 16 de este reglamento.

c) Determinar la criticidad de las infraestructuras estratégicas incluidas en el Catálogo.

d) Mantener operativo y actualizado el Catálogo, estableciendo los procedimientos de alta, baja y modificación de las infraestructuras, tanto nacionales como europeas, que en él se incluyan en virtud de los criterios horizontales y de los efectos de interdependencias sectoriales a partir de la información que le suministren los operadores y el resto de agentes del Sistema, así como establecer su clasificación interna.

e) Llevar a cabo las siguientes funciones respecto a los instrumentos de planificación previstos en este reglamento:

Dirigir y coordinar los análisis de riesgos que se realicen por los organismos especializados, públicos o privados, sobre cada uno de los sectores estratégicos en el marco de los Planes Estratégicos Sectoriales, para su estudio y deliberación por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

Establecer los contenidos mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo y supervisar el proceso de elaboración de éstos, recomendando, en su caso, el orden de preferencia de las contramedidas y los procedimientos a adoptar para garantizar su protección ante ataques deliberados.

Evaluar, tras la emisión de los correspondientes informes técnicos especializados, los Planes de Seguridad del Operador y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.

Analizar los Planes de Protección Específicos facilitados por los operadores críticos respecto a las diferentes infraestructuras críticas o infraestructuras críticas europeas de su titularidad y proponerlos, en su caso, para su

aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.

Validar los Planes de Apoyo Operativo diseñados para cada una de las infraestructuras críticas existentes en el territorio nacional por el Cuerpo Policial estatal o, en su caso, autonómico competente, previo informe, respectivamente, de las Delegaciones del Gobierno en las Comunidades Autónomas o de las Comunidades Autónomas que tengan competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

f) Elevar al Secretario de Estado de Seguridad, u órgano en quien delegue, las propuestas para la declaración de una zona como crítica que se efectúen.

g) Implantar, bajo el principio general de confidencialidad, mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema.

h) Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos instrumentos de cooperación internacional para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior o a otros organismos autorizados.

i) Participar en la realización de ejercicios y simulacros en el ámbito de la protección de las infraestructuras críticas.

j) Coordinar los trabajos y la participación de expertos en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional.

k) Ser, en el ámbito de la Protección de las Infraestructuras Críticas, el Punto Nacional de Contacto con organismos internacionales y con la Comisión Europea, así como elevar a ésta, previa consulta al Centro Nacional de Coordinación

Antiterrorista, los informes sobre evaluación de amenazas y tipos de vulnerabilidades y riesgos encontrados en cada uno de los sectores en los que se hayan designado infraestructuras críticas europeas, en los plazos y condiciones marcados por la Directiva.

l) Ejecutar las acciones derivadas del cumplimiento de la Directiva 2008/114/CE en representación de la Secretaría de Estado de Seguridad.

Subir

[Bloque 20: #a8]

Artículo 8. Los Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas.

Los ministerios y organismos del Sistema a los que se refiere el artículo 8 de la Ley 8/2011, de 28 de abril tendrán las siguientes competencias:

a) Participar, a través del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, con el apoyo, en su caso, de los operadores, en la elaboración de los Planes Estratégicos Sectoriales, así como proceder a su revisión y actualización en los términos previstos en este reglamento.

b) Verificar, en el ámbito de sus competencias, el cumplimiento de los Planes Estratégicos Sectoriales y de las actuaciones derivadas de éstos, con excepción de las que se correspondan con medidas de seguridad concretas establecidas en infraestructuras específicas, o las que deban ser realizadas por otros órganos de la Administración General del Estado, conforme a su legislación específica.

c) Colaborar con la Secretaría de Estado de Seguridad tanto en la designación de los operadores críticos como en la

elaboración de toda norma sectorial que se dicte en desarrollo de la Ley 8/2011, de 28 de abril, así como del presente reglamento.

d) Proporcionar asesoramiento técnico a la Secretaría de Estado de Seguridad en la catalogación de las infraestructuras dentro de su sector de competencia, poniendo a disposición del CNPIC en su caso la información técnica que ayude a determinar su criticidad, para su inclusión, exclusión o modificación en el Catálogo.

e) Custodiar, en los términos de la normativa sobre materias clasificadas y secretos oficiales, la información sensible sobre protección de infraestructuras estratégicas de la que dispongan en calidad de agentes del Sistema.

f) Designar a una persona para participar en los Grupos de Trabajo Sectoriales que, eventualmente, puedan crearse en el ámbito de la protección de infraestructuras críticas.

g) Participar, a solicitud del CNPIC o por iniciativa propia, en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas relacionadas con su sector de coordinación, en los ámbitos nacional e internacional.

h) Colaborar con la Secretaría de Estado de Seguridad en las acciones derivadas del cumplimiento de la Directiva 2008/114/CE, conforme a lo dispuesto en el artículo 7, apartado l), de este reglamento.

i) Participar en el proceso de clasificación de una infraestructura como crítica, incluyendo el ejercicio de la facultad de propuesta a tal fin.

Subir

[Bloque 21: #a9]

Artículo 9. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.

Bajo la autoridad del Secretario de Estado de Seguridad, y en el ejercicio de sus competencias, los Delegados del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, respecto de las infraestructuras críticas localizadas en su territorio, las siguientes facultades:

a) Coordinar la actuación de las Fuerzas y Cuerpos de Seguridad del Estado ante una alerta de seguridad, y velar por la aplicación del Plan Nacional de Protección de Infraestructuras Críticas en caso de activación de éste.

b) Colaborar, en función de su ámbito territorial de actuación, con otros órganos de la Administración u organismos públicos competentes conforme a su legislación específica, así como con las delegaciones territoriales de otros ministerios y organismos del Sistema en las acciones que se desarrollen para el cumplimiento de los Planes Sectoriales vigentes en materia de protección de infraestructuras críticas.

c) Participar en la implantación de los diferentes Planes de Protección Específicos en aquellas infraestructuras críticas o infraestructuras críticas europeas existentes en su territorio, en los términos en los que se expresa el Capítulo IV del Título III de este reglamento.

d) Intervenir, a través del Cuerpo Policial estatal competente, y en colaboración con el responsable de seguridad de la infraestructura, en la implantación de los diferentes Planes de Apoyo Operativo en aquellas infraestructuras críticas o infraestructuras críticas europeas existentes en su territorio, conforme a lo establecido en el Capítulo V del Título III de este reglamento.

e) Proponer a la Secretaría de Estado de Seguridad a través del CNPIC la declaración de zona crítica sobre la base de la

existencia de varias infraestructuras críticas o infraestructuras críticas europeas en una zona geográfica continua, con el fin de lograr una protección coordinada entre los diferentes operadores titulares y las Fuerzas y Cuerpos de Seguridad.

f) Custodiar la información sensible sobre protección de infraestructuras estratégicas de que dispongan en calidad de agentes del Sistema, en aplicación de la normativa vigente sobre materias clasificadas y secretos oficiales.

Subir

[Bloque 22: #a10]

Artículo 10. Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.

1. Las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, las facultades previstas en los párrafos c), d, e) y f) del artículo anterior dada la existencia en ellas de Cuerpos policiales autonómicos, y sin perjuicio de que las respectivas Delegaciones del Gobierno en dichas Comunidades Autónomas tengan conocimiento de la información sensible y de los planes a que se refiere el presente reglamento.

2. En todo caso, la coordinación de las actuaciones que se lleven a cabo en materia de protección de las infraestructuras críticas entre las Fuerzas y Cuerpos de Seguridad del Estado y los Cuerpos policiales de las Comunidades Autónomas con competencias en materia de seguridad, se regirá por lo estipulado en los acuerdos de las Juntas de Seguridad correspondientes.

3. Las Comunidades Autónomas no incluidas en el apartado

primero del presente artículo participarán en el Sistema y en los órganos colegiados del mismo de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

4. De acuerdo con lo dispuesto en sus Estatutos de Autonomía, las Ciudades de Ceuta y Melilla, a través de sus Consejos de Gobierno y de acuerdo con la Delegación de Gobierno respectiva, podrán emitir los oportunos informes y propuestas en relación con la adopción de medidas específicas sobre las infraestructuras críticas y críticas europeas situadas en su territorio.

Subir

[Bloque 23: #a11]

Artículo 11. La Comisión Nacional para la Protección de las Infraestructuras Críticas.

1. La Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) desempeñará las siguientes funciones:

a) Preservar, garantizar y promover la existencia de una cultura de seguridad de las infraestructuras críticas en el ámbito de las Administraciones públicas.

b) Promover la aplicación efectiva de las disposiciones de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas por parte de todos los sujetos responsables del sistema de protección de infraestructuras críticas, a partir de los informes emitidos al respecto por parte del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

c) Llevar a cabo las siguientes actuaciones a propuesta del Grupo de Trabajo:

Aprobar los Planes Estratégicos Sectoriales.

Designar a los operadores críticos.

Aprobar la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, estableciendo sus objetivos y sus marcos de actuación.

d) Impulsar aquéllas otras tareas que se estimen precisas en el marco de la cooperación interministerial para la protección de las infraestructuras críticas.

2. La Comisión será presidida por el Secretario de Estado de Seguridad, y sus miembros serán:

a) En representación del Ministerio del Interior:

El Director General de la Policía y de la Guardia Civil.

El Director General de Protección Civil y Emergencias.

El Director del CNPIC, que ejercerá las funciones de Secretario de la Comisión.

b) En representación del Ministerio de Defensa, el Director General de Política de Defensa.

c) En representación del Centro Nacional de Inteligencia, un Director General designado por el Secretario de Estado-Director de aquél.

d) En representación del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, su Director.

e) En representación del Consejo de Seguridad Nuclear, el Director Técnico de Protección Radiológica.

f) En representación de cada uno de los ministerios integrados en el Sistema, una persona con rango igual o superior a Director General, designada por el titular del Departamento ministerial correspondiente en razón del sector de actividad

material que corresponda.

3. Además de los miembros mencionados en el apartado anterior, asistirá a las reuniones de la Comisión un representante con voz y voto por cada una de las Comunidades Autónomas que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público. También participará, igualmente con voz y voto, un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones.

En su caso, y cuando su presencia y criterio resulte imprescindible por razón de los temas a tratar, podrán ser convocados, por decisión de su presidente, organismos, expertos u otras Administraciones públicas.

4. La Comisión se reunirá al menos una vez al año, con carácter ordinario, y de forma extraordinaria cuando así se considere oportuno previa convocatoria de su Presidente, quien determinará el orden del día de la reunión en los términos previstos para los órganos colegiados en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La secretaría de la Comisión radicará en el Director del CNPIC.

5. La Comisión será asistida por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

Subir

[Bloque 24: #a12]

Artículo 12. El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

1. El Grupo de Trabajo Interdepartamental para la Protección

de las Infraestructuras Críticas (en adelante, el Grupo de Trabajo) desempeña las siguientes funciones:

a) Elaborar, con la colaboración de los agentes del Sistema afectados y el asesoramiento técnico pertinente, los diferentes Planes Estratégicos Sectoriales para su presentación a la Comisión, conforme a lo previsto en el Título III, Capítulo II, de este reglamento.

b) Proponer a la Comisión la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

c) Proponer a la Comisión la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, supervisando, coordinando y efectuando el seguimiento de los mismos y de sus trabajos e informando oportunamente de los resultados obtenidos a la Comisión.

d) Efectuar los estudios y trabajos que, en el marco de este reglamento, le encomiende la Comisión. Para ello podrá contar, si es necesario, con el apoyo de personal técnico especializado.

2. El Grupo de Trabajo estará presidido por el Director del CNPIC, y estará compuesto por:

a) Un representante de cada uno de los ministerios del Sistema, designados por el titular del departamento ministerial correspondiente.

b) Un representante de la Dirección Adjunta Operativa del Cuerpo Nacional de Policía, designado por el titular de ésta.

c) Un representante de la Dirección Adjunta Operativa de la Guardia Civil, designado por el titular de aquélla.

d) Un representante de la Dirección General de Protección Civil y Emergencias del Ministerio del Interior, designado por el titular de ésta.

e) Un representante del Estado Mayor Conjunto de la Defensa, designado por el Jefe del Estado Mayor de la Defensa.

f) Un representante del Centro Nacional de Inteligencia, designado por el Secretario de Estado Director de dicho Centro.

g) Un representante del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, designado por el titular del Ministerio de la Presidencia u órgano en quien delegue, a propuesta del Director del Gabinete de la Presidencia del Gobierno.

h) Un representante del Consejo de Seguridad Nuclear, designado por el Presidente de dicho organismo.

i) Un representante del CNPIC, con funciones de Secretario.

3. Además de los miembros mencionados en el apartado anterior, asistirá a las reuniones del Grupo de Trabajo un representante, con voz y voto por cada una de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y para el mantenimiento del orden público. Asimismo, participará con voz y voto un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones.

Por decisión de su presidente, podrán asistir aquellas otras Administraciones Públicas, organismos o expertos cuyo asesoramiento técnico se estime preciso en razón de los temas a tratar.

4. El Grupo de Trabajo se reunirá al menos dos veces al año, con carácter ordinario, y de forma extraordinaria cuando así se considere oportuno a convocatoria de su Presidente, quien determinará el orden del día de la reunión. La secretaría radicará en uno de los funcionarios que prestan servicios en el CNPIC, por decisión de su Director.

5. Para el ejercicio de las competencias que este reglamento atribuye al Grupo de Trabajo, podrán constituirse otros grupos de trabajo sectoriales para los sectores o subsectores incluidos en el anexo de la Ley 8/2011, de 28 de abril, en los que podrán participar, además del CNPIC y el correspondiente ministerio u organismo del Sistema, los operadores críticos y otros agentes del Sistema.

Subir

[Bloque 25: #a13]

Artículo 13. Operadores Críticos.

1. Los operadores críticos serán los agentes integrantes del Sistema, que, procedentes tanto del sector público como del sector privado, reúnan las condiciones establecidas en el artículo 13 de la Ley 8/2011, de 28 de abril.

2. En aplicación de lo previsto en la citada Ley, corresponde a los operadores críticos:

a) Prestar su colaboración técnica a la Secretaría de Estado de Seguridad, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo. Por ello, deberán actualizar los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento o previa validación del CNPIC.

b) Colaborar, en su caso, con el Grupo de Trabajo, en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador y proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo que establece el Capítulo III, Título III del presente reglamento.

d) Elaborar un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo así como proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo establecido en el Capítulo IV, Título III del presente reglamento.

e) Designar a un Responsable de Seguridad y Enlace, en virtud de lo dispuesto en el artículo 34 del presente reglamento.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por la Secretaría de Estado de Seguridad, comunicando su designación a los órganos correspondientes en virtud de lo dispuesto en el artículo 35 del presente reglamento.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial, en el marco de lo establecido en el Título III de este reglamento.

Subir

[Bloque 26: #a14]

Artículo 14. Designación de los operadores críticos.

1. Para la designación de una empresa u organismo como operador crítico, bastará con que al menos una de las infraestructuras por él gestionadas reúna la consideración de infraestructura crítica, en aplicación de los criterios previstos en el artículo 2, apartado h), de la Ley 8/2011, de 28 de abril. En tal caso, el CNPIC, elaborará una propuesta de resolución y la notificará al titular o administrador de aquéllas.

2. La citada propuesta contendrá la intención de designar al titular o administrador de la instalación o instalaciones como operador crítico.

3. El interesado dispondrá de un plazo de quince días a contar desde el día siguiente a la recepción de la notificación para remitir al CNPIC las alegaciones que considere procedentes, transcurrido el cual la Comisión, a propuesta del Grupo de Trabajo, dictará la resolución en la que se designará, en su caso, a dicho operador, como crítico. Esta resolución podrá ser recurrida en alzada ante el Secretario de Estado de Seguridad, y, eventualmente, con posterioridad, ante la jurisdicción contencioso-administrativa, en los términos generales previstos en la legislación vigente en materia de procedimiento administrativo y del orden jurisdiccional contencioso-administrativo.

4. Las comunicaciones con el interesado tendrán en cuenta, en todo caso, la clasificación de seguridad que corresponda según la normativa vigente.

Subir

[Bloque 27: #a15]

Artículo 15. Interlocución con los operadores críticos.

1. Los operadores críticos del Sector Privado tendrán en el CNPIC el punto directo de interlocución con la Secretaría de Estado de Seguridad en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto este reglamento.

2. En aquellos casos en que los operadores críticos del Sector Público estén vinculados o dependan de una Administración pública, el órgano de dicha Administración que ostente competencias por razón de la materia podrá constituirse en el interlocutor con el Ministerio del Interior a través del CNPIC en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto en este reglamento, debiendo comunicar dicha

decisión al CNPIC.

Subir

[Bloque 28: #tiii]

TÍTULO III

Instrumentos de planificación

Subir

[Bloque 29: #ci-2]

CAPÍTULO I

El Plan Nacional de Protección de las Infraestructuras Críticas

Subir

[Bloque 30: #a16]

Artículo 16. Finalidad, elaboración y contenido.

1. El Plan Nacional de Protección de las Infraestructuras Críticas es el instrumento de programación del Estado elaborado por la Secretaría de Estado de Seguridad y dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad.

2. El Plan Nacional de Protección de las Infraestructuras Críticas establecerá los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones públicas en coordinación con los operadores críticos, articulando las medidas preventivas necesarias para

asegurar la protección permanente, actualizada y homogénea de nuestro sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

3. Asimismo, el Plan preverá distintos niveles de seguridad e intervención policial, que se activarán, en cada caso, en función de los resultados de la evaluación de la amenaza y coordinadamente con el Plan de Prevención y Protección Antiterrorista en vigor, al cual deberá adaptarse.

Los distintos niveles de seguridad contendrán la adopción graduada de dispositivos y medidas de protección ante situaciones de incremento de la amenaza contra las infraestructuras estratégicas nacionales y requerirán el concurso de las Fuerzas y Cuerpos de Seguridad, las Fuerzas Armadas, en su caso, y los responsables de los organismos o titulares o gestores de las infraestructuras a proteger.

Subir

[Bloque 31: #a17]

Artículo 17. Aprobación, registro y clasificación.

1. El Plan Nacional de Protección de las Infraestructuras Críticas será aprobado por resolución del titular de la Secretaría de Estado de Seguridad y quedará registrado en el CNPIC, sin perjuicio de que aquellos otros organismos que necesiten conocer del mismo sean autorizados para acceder a él por el Secretario de Estado de Seguridad.

2. El Plan estará clasificado conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente tal clasificación en el instrumento de su aprobación.

Subir

[Bloque 32: #a18]

Artículo 18. Revisión y actualización.

1. El Plan Nacional de Protección de las Infraestructuras Críticas será revisado cada cinco años por la Secretaría de Estado de Seguridad.

2. La modificación de alguno de los datos o instrucciones incluidos en el Plan Nacional de Protección de las Infraestructuras Críticas obligará a la automática actualización del mismo, que se llevará a cabo por el CNPIC y requerirá la aprobación expresa del Secretario de Estado de Seguridad.

Subir

[Bloque 33: #cii-2]

CAPÍTULO II

Los Planes Estratégicos Sectoriales

Subir

[Bloque 34: #a19]

Artículo 19. Finalidad, elaboración y contenido.

1. Los Planes Estratégicos Sectoriales son los instrumentos de estudio y planificación con alcance en todo el territorio nacional que permitirán conocer, en cada uno de los sectores contemplados en el anexo de la Ley 8/2011, de 28 de abril, cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de

su inactividad y las medidas estratégicas necesarias para su mantenimiento.

2. El Grupo de Trabajo, coordinado por el CNPIC, elaborará con la participación y asesoramiento técnico de los operadores afectados, en su caso, un Plan Estratégico por cada uno de los sectores o subsectores de actividad que se determinen.

3. Los Planes Estratégicos Sectoriales estarán basados en un análisis general de riesgos donde se contemplen las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten al sector o subsector en cuestión en el ámbito de la protección de las infraestructuras estratégicas.

4. Cada Plan Estratégico Sectorial contendrá, como mínimo, los siguientes extremos:

a) Análisis de riesgos, vulnerabilidades y consecuencias a nivel global.

b) Propuestas de implantación de medidas organizativas y técnicas necesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los diferentes escenarios que se prevean.

c) Propuestas de implantación de otras medidas preventivas y de mantenimiento (por ejemplo, ejercicios y simulacros, preparación e instrucción del personal, articulación de los canales de comunicación precisos, planes de evacuación o planes operativos para abordar posibles escenarios adversos).

d) Medidas de coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

5. Los Planes Estratégicos Sectoriales podrán constituirse teniendo en cuenta otros planes o programas ya existentes, creados sobre la base de su propia legislación específica sectorial. Cuando los referidos planes o programas sectoriales

reúnan los extremos a los que se refiere el apartado cuarto, podrán adoptarse los mismos como Plan Estratégico Sectorial del sector o subsector correspondiente.

Subir

[Bloque 35: #a20]

Artículo 20. Aprobación, registro y clasificación.

1. Los Planes Estratégicos Sectoriales deberán ser aprobados por la Comisión en el plazo máximo de doce meses a partir de la entrada en vigor del presente real decreto.

2. El CNPIC gestionará y custodiará un registro central de todos los Planes Estratégicos Sectoriales existentes, una vez éstos sean aprobados por la Comisión. Los ministerios y organismos del Sistema tendrán acceso a los Planes de aquellos sectores para los que sean competentes.

3. Los Planes Estratégicos Sectoriales estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes.

Subir

[Bloque 36: #a21]

Artículo 21. Revisión y actualización.

1. Los Planes Estratégicos Sectoriales deberán ser revisados cada dos años por los ministerios y organismos del Sistema.

2. La modificación de alguno de los datos incluidos en los Planes Estratégicos Sectoriales obligará a la automática

actualización de éstos, que se llevará a cabo por los ministerios y organismos del Sistema que sean competentes en el sector afectado y será posteriormente aprobada por la Comisión.

Subir

[Bloque 37: #ciii]

CAPÍTULO III

Los Planes de Seguridad del Operador

Subir

[Bloque 38: #a22]

Artículo 22. Finalidad, elaboración y contenido.

1. Los Planes de Seguridad del Operador son los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.

2. En el plazo de seis meses a partir de la notificación de la resolución de su designación, cada operador crítico deberá haber elaborado un Plan de Seguridad del Operador y presentarlo al CNPIC, que lo evaluará y lo informará para su aprobación, si procede, por el Secretario de Estado de Seguridad u órgano en el que éste delegue.

3. Los Planes de Seguridad del Operador deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas tanto físicas como lógicas identificadas

sobre cada una de las tipologías de sus activos.

4. La Secretaría de Estado de Seguridad del Ministerio del Interior, a través del CNPIC, establecerá, con la colaboración de los Ministerios del Sistema y organismos dependientes, los contenidos mínimos de los Planes de Seguridad del Operador, así como el modelo en el que basar la elaboración de éstos.

Subir

[Bloque 39: #a23]

Artículo 23. Aprobación, registro y clasificación.

1. El Secretario de Estado de Seguridad, u órgano en el que éste delegue, previo informe del CNPIC, aprobará el Plan de Seguridad del Operador o las propuestas de mejora del mismo, notificando la resolución al interesado en el plazo máximo de dos meses.

2. Junto a la resolución de aprobación o modificación, el CNPIC, tomando en su caso como referencia las actuaciones del organismo regulador competente en virtud de la normativa sectorial aplicable, efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de preferencia de las medidas y los procedimientos a adoptar.

3. El CNPIC gestionará y custodiará un registro central de todos los Planes de Seguridad del Operador existentes, una vez éstos sean aprobados por el Secretario de Estado de Seguridad. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

4. Los Planes de Seguridad del Operador estarán clasificados conforme a lo que establece la legislación vigente en materia

de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los operadores críticos responsables de la elaboración de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Subir

[Bloque 40: #a24]

Artículo 24. Revisión y actualización.

1. Los Planes de Seguridad del Operador deberán ser revisados cada dos años por los operadores críticos y aprobados por el CNPIC. Éste podrá requerir en cualquier momento información concreta sobre el estado de implantación del Plan de Seguridad del Operador.

2. La modificación de alguno de los datos incluidos en los Planes de Seguridad del Operador obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.

Subir

[Bloque 41: #civ]

CAPÍTULO IV

Los Planes de Protección Específicos

Subir

[Bloque 42: #a25]

Artículo 25. Finalidad, elaboración y contenido.

1. Los Planes de Protección Específicos son los documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.

2. En el plazo de cuatro meses a partir de la aprobación del Plan de Seguridad del Operador, cada operador crítico deberá haber elaborado un Plan de Protección Específico por cada una de sus infraestructuras críticas así consideradas por la Secretaría de Estado de Seguridad y presentarlo al CNPIC. Igual procedimiento y plazos se establecerán cuando se identifique una nueva infraestructura crítica.

3. Los Planes de Protección Específicos de las diferentes infraestructuras críticas incluirán todas aquellas medidas que los respectivos operadores críticos consideren necesarias en función de los análisis de riesgos realizados respecto de las amenazas, en particular, las de origen terrorista, sobre sus activos, incluyendo los sistemas de información.

4. Cada Plan de Protección Específico deberá contemplar la adopción tanto de medidas permanentes de protección, sobre la base de lo dispuesto en el párrafo anterior, como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta sobre una o varias infraestructuras por él gestionadas.

5. La Secretaría de Estado de Seguridad, a través del CNPIC,

establecerá los contenidos mínimos de los Planes de Protección Específicos, así como el modelo en el que fundamentar la estructura y la compleción de éstos que, en todo caso, cumplirán las directrices marcadas por sus respectivos Planes de Seguridad del Operador.

Subir

[Bloque 43: #a26]

Artículo 26. Aprobación, registro y clasificación.

1. La Secretaría de Estado de Seguridad notificará al interesado, en el plazo máximo de dos meses contados a partir de la recepción, su resolución con la aprobación de los diferentes Planes de Protección Específicos o de las eventuales propuestas de mejora de éstos. Previamente, a través del CNPIC, se recabará informe preceptivo de las Delegaciones del Gobierno en las respectivas Comunidades Autónomas o en las Ciudades con Estatuto de Autonomía en el que se considerará, en su caso, el criterio de los órganos competentes de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, así como del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente.

2. Junto a la resolución de aprobación o modificación, el CNPIC, basándose en los informes mencionados en el punto anterior, efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de preferencia de las medidas y los procedimientos a adoptar sobre las infraestructuras afectadas.

3. Las Delegaciones del Gobierno en las Comunidades Autónomas

y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean aprobados por el Secretario de Estado de Seguridad, todos los Planes de Protección Específicos de las infraestructuras críticas o infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro central de todos los Planes de Protección Específicos existentes. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

4. Los Planes de Protección Específicos estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o a parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los agentes del Sistema responsables de la elaboración de los respectivos planes y aquellos encargados de su registro deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Subir

[Bloque 44: #a27]

Artículo 27. Revisión y actualización.

1. Los Planes de Protección Específicos deberán ser revisados cada dos años por los operadores críticos, revisión que deberá

ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, y por el CNPIC.

2. La modificación de alguno de los datos incluidos en los Planes de Protección Específicos obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.

Subir

[Bloque 45: #a28]

Artículo 28. Aplicación y seguimiento.

1. Los Delegados del Gobierno en las Comunidades Autónomas velarán por la correcta ejecución de los diferentes Planes de Protección Específicos y tendrán facultades de inspección en el ámbito de la protección de infraestructuras críticas. Dichas facultades deberán desarrollarse, en su caso, de forma coordinada con las facultades inspectoras del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente.

2. En aquellas Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, las facultades de inspección serán ejercidas por sus órganos competentes, sin perjuicio de lo dispuesto en la legislación sectorial aplicable y de la necesaria coordinación con las Delegaciones del Gobierno en dichas Comunidades y los otros organismos reguladores competentes en virtud de su normativa

sectorial.

3. En ejercicio de ese seguimiento, los organismos competentes podrán en todo momento requerir del responsable de las infraestructuras críticas o infraestructuras críticas europeas la situación actualizada de la implantación de las medidas propuestas en las resoluciones de aprobación o modificación de los Planes de Protección Específicos elaborados en caso de variación de las circunstancias que determinaron su adopción, o bien para adecuarlos a la normativa vigente que les afecte, dando cuenta del resultado de ello a la Secretaría de Estado de Seguridad, a través del CNPIC.

4. Las facultades de inspección en las instalaciones portuarias, así como en aquellos otros puntos o establecimientos considerados críticos que se encuentren integrados en un puerto, serán establecidas de acuerdo con lo previsto en el Real Decreto 1617/2007, de 7 de diciembre.

Subir

[Bloque 46: #a29]

Artículo 29. Compatibilidad con otros planes existentes.

1. La elaboración de los Planes de Protección Específicos para cada una de las infraestructuras críticas se efectuará sin perjuicio del obligado cumplimiento de lo exigido por el Código Técnico de la Edificación, aprobado por el Real Decreto 314/2006, de 17 de marzo, el Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección de los centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia, la normativa de Seguridad Privada o cualquier otra reglamentación sectorial específica que le sea de aplicación.

2. Las instalaciones Nucleares e Instalaciones Radiactivas que

se consideren críticas reguladas en el Reglamento sobre instalaciones nucleares y radiactivas, aprobado por el Real Decreto 1836/1999 de 3 de diciembre, modificado por el Real Decreto 35/2008 de 18 de enero, integrarán sus Planes de Protección Específicos en los respectivos Planes de Protección Física rigiéndose, en lo relativo a su aprobación y evaluación, por lo establecido en su normativa sectorial específica, sin perjuicio de lo que le sea de aplicación según la Ley 8/2011, de 28 de abril.

3. Las instalaciones portuarias, así como aquellos otros puntos o establecimientos considerados críticos que se encuentren integrados en un puerto, conforme a lo dispuesto en el Real Decreto 1617/2007, de 7 de diciembre, por el que se establecen medidas para la mejora de la protección de los puertos y el transporte marítimo, integrarán sus Planes de Protección Específicos en los Planes de Protección de Puertos previstos en el citado Real Decreto rigiéndose, en lo relativo a su aprobación y evaluación, por lo establecido en esa norma, sin perjuicio de lo que le sea de aplicación según la Ley 8/2011, de 28 de abril.

4. En el caso de aeropuertos, aeródromos e instalaciones de navegación aérea se considerarán Planes de Protección Específicos los respectivos Programas de Seguridad de los aeropuertos aprobados conforme a lo dispuesto en la Ley 21/2003, de 7 de julio, de Seguridad Aérea modificada por la Ley 1/2011, de 4 de marzo por la que se establece el Programa Estatal de Seguridad Operacional para la Aviación Civil y se modifica la Ley 21/2003, de 7 de julio de Seguridad Aérea y en el Real Decreto 550/2006, de 5 de mayo, por el que se designa la autoridad competente responsable de la coordinación y seguimiento del Programa Nacional de Seguridad para la Aviación Civil y se determina la organización y funciones del Comité Nacional de Seguridad de la Aviación Civil. No obstante, el Ministerio del Interior, a través de su representante en el Comité Nacional de Seguridad de la

Aviación Civil podrá proponer contenidos adicionales, de conformidad con lo establecido en el artículo 25, apartado quinto de este real decreto.

Subir

[Bloque 47: #cv]

CAPÍTULO V

Los Planes de Apoyo Operativo

Subir

[Bloque 48: #a30]

Artículo 30. Finalidad, elaboración y contenido.

1. Los Planes de Apoyo Operativo son los documentos operativos donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas.

2. Por cada una de las infraestructuras críticas e infraestructuras críticas europeas dotadas de un Plan de Protección Específico y sobre la base a los datos contenidos en éste, la Delegación del Gobierno en la Comunidad Autónoma o, en su caso, el órgano competente de la Comunidad Autónoma, supervisará la realización de un Plan de Apoyo Operativo por parte del Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate. Para su elaboración, que deberá realizarse en un plazo de cuatro meses a partir de la aprobación del respectivo Plan de Protección Específico, se contará con la colaboración del responsable de seguridad de la infraestructura.

3. Sobre la base de sus correspondientes Planes de Protección Específicos, los Planes de Apoyo Operativo deberán contemplar, si las instalaciones lo precisan, las medidas planificadas de vigilancia, prevención, protección y reacción que deberán adoptar las unidades policiales y, en su caso, de las Fuerzas Armadas, cuando se produzca la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien de confirmarse la existencia de una amenaza inminente sobre dichas infraestructuras. Estas medidas serán siempre complementarias a aquellas de carácter gradual que hayan sido previstas por los operadores críticos en sus respectivos Planes de Protección Específicos.

4. El CNPIC establecerá los contenidos mínimos de los Planes de Apoyo Operativo, así como el modelo en el que fundamentar la estructura y desarrollo de éstos, que se basarán en la parte que les corresponda en la información contenida en los respectivos Planes de Protección Específicos.

5. El Ministerio de Defensa podrá acceder a los Planes de Apoyo Operativo de aquellas infraestructuras críticas o infraestructuras críticas europeas que, en caso de activarse el Plan Nacional de Protección de las Infraestructuras Críticas y a los efectos de coordinar los correspondientes apoyos de las Fuerzas Armadas, se considere oportuno, previo estudio conjunto de los mencionados apoyos.

Subir

[Bloque 49: #a31]

Artículo 31. Aprobación, registro y clasificación.

1. Los Planes de Apoyo Operativo serán validados y aprobados por la Secretaría de Estado de Seguridad, a través del CNPIC.

2. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el

órgano competente de cada Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean validados, todos los Planes de Apoyo Operativo de las infraestructuras críticas e infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro central de todos los Planes de Apoyo Operativo existentes. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

3. Los Planes de Apoyo Operativo estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o a parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los agentes del Sistema responsables de la elaboración y registro de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Subir

[Bloque 50: #a32]

Artículo 32. Revisión y actualización.

1. Los Planes de Apoyo Operativo deberán ser revisados cada dos años por el Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate, revisión que deberá ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en

las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, requiriendo la aprobación expresa del CNPIC.

2. La modificación de alguno de los datos incluidos en los Planes de Apoyo Operativo obligará a la automática actualización de éstos, que se llevará a cabo mediante el procedimiento previsto en el apartado primero.

Subir

[Bloque 51: #tiv]

TÍTULO IV

Comunicaciones entre los operadores críticos y las Administraciones públicas

Subir

[Bloque 52: #a33]

Artículo 33. Seguridad de las comunicaciones.

1. El CNPIC será el responsable de administrar los sistemas de gestión de la información y comunicaciones que se diseñen en el ámbito de la protección de las infraestructuras críticas, que deberá contar para ello con el apoyo y colaboración de los agentes del Sistema y de todos aquellos otros organismos o entidades afectados.

2. La seguridad de los sistemas de información y comunicaciones previstos en este real decreto será acreditada y, en su caso, certificada por el Centro Criptológico Nacional del Centro Nacional de Inteligencia, de acuerdo con las

competencias establecidas en su normativa específica.

3. La Presidencia del Gobierno facilitará el uso de la Malla B, sistema soporte de comunicaciones estratégicas seguras del Sistema Nacional de Gestión de Crisis y de la Presidencia del Gobierno, a través del cual los agentes del Sistema autorizados podrán acceder a la información disponible en el Catálogo, con los niveles de acceso que se determinen.

Subir

[Bloque 53: #a34]

Artículo 34. El Responsable de Seguridad y Enlace.

1. En el plazo de tres meses desde su designación como operadores críticos, los mismos nombrarán y comunicarán a la Secretaría de Estado de Seguridad, a través del CNPIC, el nombre del Responsable de seguridad y enlace en los términos y con los requisitos previstos por el artículo 16 de la Ley 8/2011, de 28 de abril.

2. El Responsable de Seguridad y Enlace representará al operador crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento, canalizando, en su caso, las necesidades operativas e informativas que surjan al respecto.

Subir

[Bloque 54: #a35]

Artículo 35. El Delegado de Seguridad de la infraestructura crítica.

1. En el plazo de tres meses desde la identificación como

crítica o crítica europea, de una de sus infraestructuras, los operadores críticos comunicarán a las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia e identidad de un Delegado de Seguridad para dicha infraestructura.

2. El Delegado de Seguridad constituirá el enlace operativo y el canal de información con las autoridades competentes en todo lo referente a la seguridad concreta de la infraestructura crítica o infraestructura crítica europea de que se trate, encauzando las necesidades operativas e informativas que se refieran a aquélla.

Subir

[Bloque 55: #a36]

Artículo 36. Seguridad de los datos clasificados.

Los datos clasificados relativos a las infraestructuras de los operadores críticos cumplirán, en todo caso, con los requerimientos de seguridad establecidos por el Secretario de Estado Director del Centro Nacional de Inteligencia, de acuerdo con la normativa específica aplicable.