

## Ministerio del Interior (BOE n. de / /)

, de de , por el que se establecen medidas para la protección de las infraestructuras críticas.

Los Estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente.

En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.

Hasta tal punto es así, que cualquier interrupción no deseada – incluso de corta duración y debida bien a causas naturales o técnicas, bien a ataques deliberados – podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios públicos esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad, lo que es objeto de especial atención para el Sistema Nacional de Gestión de Situaciones de Crisis.

En su debate de investidura, el Presidente del Gobierno anunció la necesidad de construir una estrategia de seguridad nacional en la que, entre otras cosas, habría que definir objetivos y señalar prioridades para la mejora de nuestra seguridad. En línea con lo anterior, el Ministro del Interior, en su comparecencia de 27 de mayo de 2008 ante la Comisión de Interior del Congreso de los Diputados, señaló que la definición de cualquier estrategia de seguridad debe descansar, en primer lugar, en un análisis riguroso de los riesgos, de las amenazas y de nuestras vulnerabilidades y, en segundo lugar, en un análisis y una evaluación de nuestras fortalezas y debilidades frente a los mismos, en una precisa definición de cuáles son

nuestros objetivos y prioridades estratégicas, en la determinación de nuestras capacidades y, finalmente, en la coordinación y planificación de esfuerzos por parte del Gobierno de la Nación, del resto de las Administraciones Públicas y, en su caso, del sector privado.

Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección se hace imprescindible, por un lado, catalogar el conjunto de aquéllas que prestan servicios públicos esenciales a nuestra sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones (TIC).

En esa línea, se han emprendido diversas actuaciones a nivel nacional, como la elaboración, por la Secretaría de Estado de Seguridad del Ministerio del Interior, de un primer Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, así como la elaboración de un primer Catálogo Nacional de Infraestructuras Estratégicas. Así mismo, con fecha 2 de noviembre de 2007, el Consejo de Ministros aprobó un Acuerdo sobre Protección de Infraestructuras Críticas, por el cual se dio un impulso decisivo en dicha materia mediante la decisión de crear un órgano específico, el Centro Nacional para la Protección de las Infraestructuras Críticas, como órgano director y coordinador de cuantas actividades relacionadas con la protección de infraestructuras críticas tiene encomendadas la Secretaría de Estado de Seguridad. El desarrollo y aplicación de este Acuerdo supone un avance cualitativo de primer orden para garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios públicos esenciales.

En ese sentido, el presente Real Decreto crea formalmente el Centro Nacional para la Protección de las Infraestructuras Críticas como órgano adscrito a la Secretaría de Estado de Seguridad.

Paralelamente, existen también una serie de actuaciones desarrolladas a nivel internacional en el ámbito europeo: tras los terribles atentados de Madrid, el Consejo Europeo de junio de 2004 instó a la Comisión Europea a elaborar una estrategia global sobre protección de infraestructuras críticas. El 20 de octubre de 2004, la Comisión adoptó una Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que les afecten. Con posterioridad, en diciembre de 2004, el Consejo aprobó el PEPIC (Programa europeo de protección de infraestructuras críticas) y puso en marcha una red de información sobre alertas en infraestructuras críticas (Critical Infrastructures Warning Information Network – CIWIN).

En la actualidad, la entrada en vigor de la Directiva 2008/114 del Consejo de la Unión Europea, de 8 de diciembre de 2008, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE), constituye un importante paso en la cooperación en esta materia en el seno de la Unión. En dicha Directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de las mismas, y determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior. Sin embargo, la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración del Estado, de las demás Administraciones Públicas, de otros organismos públicos y del sector privado. Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios públicos esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior.

En consecuencia, y dada la complejidad de la materia, su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la Directiva 2008/114/CE, se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético), mediante la definición y el desarrollo de un sistema y unos procedimientos que aglutinen a todos los sectores públicos y privados afectados y, por otro, la transposición de la citada Directiva al ordenamiento jurídico español y desarrolla las medidas que en ella se recogen, en particular la identificación y clasificación de las Infraestructuras Críticas Europeas (en adelante, ICE), la realización de los análisis de riesgos pertinentes, el establecimiento de planes de seguridad de los operadores y la implementación de los sistemas de comunicación adecuados entre las Administraciones estatales y los responsables de seguridad y enlace de los operadores de ICE.

La finalidad de esta norma es, por tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios públicos esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas. Sobre esta base, se sustentarán el Catálogo Nacional de Infraestructuras Estratégicas (conforme a la comunicación del Consejo de la UE de 20 de octubre de 2004, que señala que cada sector y cada Estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el Plan Nacional de Protección de Infraestructuras Críticas (en adelante, PNPIC), como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.

En su virtud, a propuesta del Ministro del Interior, con la aprobación previa de la Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, 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 XX de XXXX de 20XX,

**DISPONGO :**

## TÍTULO I

### Disposiciones generales

#### **Artículo 1.** *Objeto.*

1. Este Real Decreto tiene por objeto establecer el marco preciso para desarrollar las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de Infraestructuras Críticas, previa identificación y designación de las mismas, impulsando, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras en nuestro país a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo.

2. Asimismo, el presente Real Decreto regula las especiales obligaciones que deben asumir tanto el Estado como los operadores de aquellas infraestructuras que se determinen como Infraestructuras Críticas, según lo dispuesto en el artículo 2, apartados e) y f) del mismo.

## **Artículo 2. Definiciones.**

A los efectos del presente Real Decreto, se entenderá por:

- a) **Servicio público esencial:** el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y de las Administraciones Públicas.
- b) **Sector estratégico:** cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva nacional, que proporciona un servicio público esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo I de esta norma.
- c) **Subsector estratégico:** cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.
- d) **Infraestructuras estratégicas (IE):** las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios públicos esenciales.
- e) **Infraestructuras críticas (IC):** las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos esenciales.
- f) **Infraestructuras críticas europeas (ICE):** aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya interrupción o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114/CE.
- g) **Zona Crítica (ZC):** aquella zona geográfica continua donde estén establecidas varias infraestructuras críticas a cargo de operadores diferentes e

interdependientes, que sea declarada como tal por la Autoridad competente. La declaración de una ZC tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores titulares de IC o ICE radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad.

- h) **Criterios horizontales de criticidad:** los parámetros en función a los cuales se determina la criticidad de una infraestructura, valorados en términos de:
1. el **número potencial de víctimas** mortales o de lesiones graves que pueda producir;
  2. el **impacto económico** en función de la magnitud de las pérdidas económicas y/o el deterioro de productos o servicios, incluido el posible impacto medioambiental;
  3. el **impacto público**, por la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.
- i) **Análisis de riesgos:** el estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la interrupción o destrucción de las infraestructuras que le dan apoyo.
- j) **Interdependencias:** los efectos que una interrupción en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y/o en otros sectores, y las repercusiones de ámbito local, regional, nacional o internacional.
- k) **Protección de infraestructuras críticas:** el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.
- l) **Información sensible sobre protección de infraestructuras estratégicas:** los datos específicos sobre infraestructuras estratégicas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la interrupción o la destrucción de éstas.

- m) **Operadores críticos:** las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo al presente Real Decreto.
- n) **Nivel de Seguridad IC:** aquel cuya activación por el Ministerio del Interior está previsto en el Plan Nacional de Protección de Infraestructuras Críticas, de acuerdo con la evaluación general de la amenaza y con la específica que en cada supuesto se efectúe sobre cada infraestructura, en razón al cual corresponderá un grado concreto de intervención de los diferentes organismos responsables en materia de seguridad.
- o) **Catálogo Nacional de Infraestructuras Estratégicas:** La información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.

### **Artículo 3. *Ámbito de aplicación.***

1. Este Real Decreto se aplicará a las infraestructuras críticas ubicadas en el territorio nacional que se hallen afectas a los distintos sectores estratégicos definidos en el anexo I.
2. Quedan expresamente excluidas del ámbito de aplicación del presente Real Decreto aquellas actuaciones cuya regulación corresponde al ámbito de la Protección Civil.
3. Asimismo, se exceptúan de la aplicación del mismo las infraestructuras críticas dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, tanto del Estado como de las Comunidades Autónomas, que se registrarán, a efectos de control administrativo, por su propia normativa o procedimientos.
4. La aplicación de este Real Decreto se efectuará sin perjuicio de:
  - a) La misión y funciones del Centro Nacional de Inteligencia (en adelante, CNI) establecidas en su normativa específica y en un marco de colaboración y complementariedad con éstas.

b) Los criterios y disposiciones contenidos en la Ley 25/1964, de 29 de abril, sobre energía nuclear y normas de desarrollo de la misma, y en la Ley 15/1980, de 22 de abril, de creación del Consejo de Seguridad Nuclear, reformada por la Ley 33/2007, de 7 de noviembre.

c) Lo previsto en el Programa Nacional de Seguridad de la Aviación Civil contemplado en la Ley 21/2003, de 7 de julio, de Seguridad Aérea, y su normativa complementaria.

**Artículo 4.** *Contenido y finalidad del Catálogo Nacional de Infraestructuras Estratégicas.*

1. El Catálogo Nacional de Infraestructuras Estratégicas (en adelante, el Catálogo) contendrá la información y valoración de las diferentes infraestructuras estratégicas del país, que deberán aportar los operadores de aquéllas y el resto de sujetos responsables del sistema de protección de infraestructuras críticas.

2. El Catálogo, clasificado como secreto, contendrá información sensible sobre la protección de las distintas infraestructuras estratégicas del país. Igualmente, contendrá aquellas otras infraestructuras calificadas como Infraestructuras Críticas Europeas con arreglo a la Directiva 2008/114/CE. Su custodia, gestión y mantenimiento corresponderá al Ministerio del Interior.

3. La finalidad principal del Catálogo será permitir diseñar los correspondientes mecanismos de planificación, prevención, protección y reacción y, en caso necesario, activar una respuesta ágil, oportuna y proporcionada, de acuerdo con el nivel y características de la amenaza que se trate.

4. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será el competente para clasificar una infraestructura como estratégica y, en su caso, como IC o ICE, así como para incluirla en el Catálogo previa comprobación de que satisface uno o varios de los criterios horizontales de criticidad previstos en el artículo 2, apartado h) del presente Real Decreto.

## TÍTULO II

### El Sistema de Protección de Infraestructuras Críticas

#### CAPÍTULO I

##### Disposiciones generales

###### **Artículo 5. Composición.**

El Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) se compone de los siguientes agentes:

- a) La Secretaría de Estado de Seguridad del Ministerio del Interior.
- b) El Centro Nacional para la Protección de las Infraestructuras Críticas.
- c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo I de este Real Decreto.
- d) Las Delegaciones del Gobierno en las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.
- e) La Comisión Nacional para la Protección de las Infraestructuras Críticas.
- f) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
- g) Operadores críticos del Sector Público.
- h) Operadores críticos del Sector Privado.

## CAPÍTULO II

### Agentes del sistema de protección de infraestructuras críticas

**Artículo 6.** *La Secretaría de Estado de Seguridad del Ministerio del Interior.*

La Secretaría de Estado de Seguridad es el órgano superior responsable del sistema de seguridad de las infraestructuras críticas nacionales, para lo cual ejercerá las siguientes funciones:

- a) Diseñar y dirigir la estrategia nacional de protección de infraestructuras críticas.
- b) Impulsar y coordinar las actividades que lleven a cabo los ministerios y organismos integrados en el Sistema.
- c) Dirigir la aplicación del Plan Nacional de Protección de Infraestructuras Críticas, y declarar los niveles de seguridad IC a establecer en cada momento, conforme al contenido de dicho Plan.
- d) Aprobar la declaración de una zona como crítica (ZC), a propuesta de las Delegaciones del Gobierno en las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía, y previo informe del Centro Nacional de Protección de Infraestructuras Críticas.
- e) Establecer relaciones y mecanismos de cooperación y comunicación con otros organismos responsables de la protección de las infraestructuras críticas a nivel internacional.
- f) Presidir la Comisión Nacional para la Protección de las Infraestructuras Críticas.
- g) Identificar los diferentes ámbitos de responsabilidad en la protección de infraestructuras críticas; analizar los mecanismos de prevención y respuesta previstos por cada uno de los actores implicados; y divulgar y fomentar la adopción de medidas y procedimientos considerados como "mejores prácticas".

- h) Establecer mecanismos permanentes de comunicación, colaboración, coordinación e información con los operadores, públicos y privados, de las infraestructuras estratégicas nacionales, bajo el principio general de confidencialidad.
- i) Supervisar y coordinar los planes sectoriales y territoriales 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 en los diferentes supuestos de riesgo y los niveles de seguridad IC que se establezcan.
- j) Diseñar las Instrucciones y Protocolos de Colaboración e Instrucciones dirigidos tanto al personal y órganos ajenos al Ministerio del Interior como a los operadores de las infraestructuras estratégicas.
- k) Supervisar, dentro del ámbito de aplicación de este Real Decreto, los proyectos y estudios de interés y coordinar la participación en programas financieros y subvenciones procedentes de la Unión Europea.
- l) Aquellas otras que pudieran acordarse por la Comisión Delegada del Gobierno para situaciones de crisis.

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

1. Se crea el Centro Nacional para la Protección de las Infraestructuras Estratégicas (en adelante, CNPIC), cuyo titular tendrá el nivel que se determine en la relación de puestos de trabajo, como órgano director y coordinador de cuantas actividades relacionadas con la protección de las infraestructuras críticas tiene encomendadas la Secretaría de Estado de Seguridad.
2. El CNPIC depende orgánicamente de la Secretaría de Estado de Seguridad, y desempeñará las siguientes funciones:
  - a) Asistir al Secretario de Estado de Seguridad en la ejecución de sus funciones en materia de protección de las infraestructuras críticas.
  - b) Fijar los procedimientos de alta, baja y modificación, previa validación, de las infraestructuras contenidas en el Catálogo Nacional de Infraestructuras Estratégicas.

- c) Custodiar, mantener y actualizar el Plan Nacional de Protección de Infraestructuras Críticas y el Catálogo Nacional de Infraestructuras Estratégicas.
- d) Determinar la criticidad de las infraestructuras estratégicas incluidas en el Catálogo, y la clasificación interna de cada una de ellas, en función de los criterios horizontales y de los efectos de interdependencias sectoriales. Todo ello, a partir de la información proporcionada por los operadores y por el resto de sujetos responsables del sistema de protección de infraestructuras.
- e) Determinar, previa consulta con los ministerios u organismos del Sistema y los operadores afectados, la condición de potencial ICE de una infraestructura, aplicando los criterios y procedimientos mencionados en el apartado anterior y establecer, en su caso, su clasificación, previo acuerdo con los demás Estados miembros que pudieran verse afectados de forma significativa por la potencial ICE.
- f) Informar al Secretario de Estado de Seguridad las propuestas de las Delegaciones del Gobierno en las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía para la declaración de una zona como crítica (ZC).
- g) Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de la cooperación internacional.
- h) Dirigir y coordinar los análisis de riesgos que se realicen por los organismos especializados, públicos o privados, sobre cada uno de los sectores estratégicos.
- i) Establecer los contenidos mínimos de los Planes de Seguridad de los Operadores y de los Planes de Protección Específicos de infraestructuras críticas establecidos según el Título III de este Real Decreto.
- j) Proponer los ajustes que sean precisos para garantizar la suficiencia y adecuación a los objetivos de la presente norma de los planes y programas que, en su caso, existan y se aprueben en el ámbito sectorial de otros Ministerios u Organismos con el objetivo de garantizar la seguridad de ese sector.
- k) Actuar como órgano de la Administración General del Estado para el contacto y coordinación con los Responsables de Seguridad y Enlace de los operadores críticos, según lo dispuesto en el Título III, Capítulo VI, de este Real Decreto.

- l) Diseñar y establecer mecanismos permanentes de información, comunicación y alerta, asegurando la comunicación mutua y fluida con todas las instituciones y operadores implicados en la protección de infraestructuras críticas.
- m) Presidir, a través de su Director, el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
- n) Establecer un sistema de mando y control activado en situaciones del nivel de seguridad IC que se determine en el Plan Nacional de Protección de Infraestructuras Críticas.
- o) Actuar como Punto Nacional de Contacto, en el marco de la protección de infraestructuras críticas de la Unión Europea y con otros organismos similares de terceros países.
- p) Presentar a la Comisión Europea los informes sobre evaluación de amenazas y los tipos de vulnerabilidades, amenazas y riesgos encontrados en cada uno de los sectores en los que se hayan designado ICE, con arreglo a lo dispuesto en la Directiva 2008/114/CE.
- q) Coordinar los trabajos y la participación en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional, especialmente de la Comisión Europea.
- r) Supervisar el proceso de elaboración de planes de seguridad de los operadores y de sus infraestructuras críticas, determinando, en su caso, el orden de preferencia de las contramedidas y los procedimientos a adoptar para garantizar su protección ante ataques deliberados.
- s) Participar en la realización de ejercicios y simulacros.

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

1. Por cada sector estratégico, se nombrará, al menos, un ministerio, organismo, entidad u órgano de la Administración General del Estado integrado en el Sistema de Protección de Infraestructuras Críticas. El nombramiento o baja de un ministerio u organismo delegado sobre un sector estratégico se efectuará mediante la correspondiente modificación del anexo I al presente Real Decreto.

2. Los ministerios y organismos del Sistema serán los encargados de impulsar, en el ámbito de su competencia, las políticas de seguridad del Gobierno sobre los distintos sectores estratégicos nacionales y de velar por su aplicación, actuando igualmente como puntos de contacto especializados en la materia. Para ello, colaborarán con el Ministerio del Interior a través de la Secretaría de Estado de Seguridad.
3. Un ministerio u organismo del Sistema podrá tener competencias, igualmente, sobre dos o más sectores estratégicos, conforme a lo establecido en el anexo I de este Real Decreto.
4. Los ministerios y organismos del Sistema tendrán las siguientes competencias:
  - a) Colaborar con el Ministerio del Interior en el desarrollo de los análisis de riesgos y, en su caso, la identificación de contramedidas y procedimientos a adoptar sobre los sectores estratégicos de su competencia, así como en la designación de operadores críticos.
  - b) Colaborar con el Ministerio del Interior en el alta, baja y modificación de las infraestructuras de su sector contenidas en el Catálogo Nacional de Infraestructuras Estratégicas, en la puesta a disposición del CNPIC de la información técnica que determine su criticidad, así como en la eventual clasificación de aquéllas como potenciales ICE.
  - c) Participar en el seno del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas en la elaboración de los Planes Estratégicos Sectoriales donde se establezcan las medidas organizativas y técnicas necesarias para prevenir y, en su caso, paliar, las consecuencias de las amenazas que se prevean como resultado de los análisis de riesgos del apartado a). Para la elaboración de dichos planes se podrá contar, en su caso, con el apoyo de los operadores críticos.
  - d) Aprobar con la colaboración del Ministerio del Interior la normativa sectorial que, en el ámbito de sus competencias, garantice la aplicación de las estrategias implantadas, tanto por los poderes públicos como por los diferentes operadores.
  - e) Verificar, en el ámbito de sus competencias, el cumplimiento del Plan Estratégico Sectorial y de las actuaciones que se deriven de éste, salvo 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 u otros organismos públicos, conforme a su legislación específica.

- f) Participar, a solicitud del CNPIC, 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, y, especialmente, en la Comisión Europea.
- g) Determinar la persona titular de un ministerio u organismo delegado que vaya a presidir los Grupos de Trabajo Sectoriales sobre Protección de Infraestructuras Críticas que en su caso se creen.
- h) Custodiar la información sensible sobre protección de infraestructuras estratégicas de que dispongan, en aplicación de la normativa vigente sobre materias clasificadas y secretos oficiales.

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

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

- a) Coordinar la actuación de las Fuerzas y Cuerpos de Seguridad 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) Verificar la realización por parte de los operadores, del Plan de Protección Específico de las IC o ICE existentes en su Comunidad Autónoma o Ciudad en su caso, así como llevar a cabo la inspección de éstas en el ámbito exclusivo de la protección de infraestructuras críticas.
- c) Proponer la declaración de zona crítica (ZC), en base a la existencia de varias IC o ICE en una zona geográfica continua, con el fin de lograr una mejor protección coordinada entre los diferentes operadores titulares y las Fuerzas y Cuerpos de Seguridad.
- d) Establecer, a través del Cuerpo Policial con competencia en la demarcación, y en colaboración con el responsable de seguridad de la infraestructura, un Plan de Apoyo Operativo por cada una de las IC y de las ICE dotadas de un Plan de Protección Específico.

- e) Custodiar la información sensible sobre protección de infraestructuras estratégicas de que dispongan, en aplicación de la normativa vigente.
- f) Verificar, en el ámbito de sus competencias, el cumplimiento de los Planes Sectoriales vigentes en materia de protección de infraestructuras críticas, así como las actuaciones derivadas de ellos, salvo las que constituyan medidas de seguridad ya establecidas en determinadas infraestructuras o que deban ser realizadas por otros órganos de la Administración u otros organismos públicos, conforme a su legislación específica.

2. Las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público podrán desarrollar, sobre las infraestructuras ubicadas en su demarcación territorial, las facultades determinadas en el punto anterior, sin perjuicio de que las respectivas Delegaciones del Gobierno tengan conocimiento de la información sensible y de los planes a los que se refiere el presente artículo.

#### **Artículo 10.** *Comisión Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, Comisión PIC) como órgano colegiado adscrito a la Secretaría de Estado de Seguridad, con el fin de desempeñar 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) Velar por la aplicación efectiva de las disposiciones del presente Real Decreto por parte de todos los sujetos responsables del sistema de protección de infraestructuras críticas.
- c) Aprobar, a propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas, los diferentes Planes Estratégicos Sectoriales.
- d) Designar a los operadores críticos a propuesta del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
- e) Aprobar los Planes de Seguridad del Operador de los operadores críticos a propuesta del Grupo de Trabajo Interdepartamental para la Protección de las

Infraestructuras Críticas, tomando en su caso, como referencia, las actuaciones del organismo regulador que pudiera ser competente en la autorización del operador.

- f) Aprobar, a propuesta del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, los informes sobre evaluación de amenazas y los tipos de vulnerabilidades, amenazas y riesgos encontrados en cada uno de los sectores en los que se hayan designado ICE, con arreglo a lo dispuesto en la Directiva 2008/114/CE, previamente a su presentación a la Comisión Europea.
- g) Aquellas otras que se estimen precisas en el marco de la cooperación interministerial para la protección de las infraestructuras críticas.

2. La Comisión PIC será presidida por el Secretario de Estado de Seguridad y estará compuesta por:

- a) El Director General de la Policía y de la Guardia Civil del Ministerio del Interior.
- b) El Director General del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis de Presidencia del Gobierno.
- c) El Director General de Protección Civil y Emergencias del Ministerio del Interior.
- d) El Director General de Política de Defensa del Ministerio de Defensa.
- e) Un Director General del CNI, designado por el Secretario de Estado Director.
- f) El Director Técnico de Protección Radiológica del Consejo de Seguridad Nuclear.
- g) Uno o dos representantes por cada uno de los ministerios integrados en el Sistema, con rango igual o superior a Director General, designados por el titular del Departamento ministerial correspondiente, en razón del sector de actividad material que corresponda.

h) Un representante de aquellas Comunidades Autónomas con competencias estatutariamente asumidas para la protección de personas y bienes y el mantenimiento del orden público.

i) El Director del CNPIC, con funciones de Secretario.

3. Además de los miembros mencionados en el apartado anterior, también podrán asistir a las reuniones de la Comisión PIC, por decisión de su Presidente, con voz pero sin voto, otras personas cuyo asesoramiento sea conveniente en algún aspecto concreto, en razón de los temas a tratar.

4. La Comisión PIC se reunirá al menos una vez 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 estará radicada en el CNPIC.

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

**Artículo 11.** *Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

1. El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (Grupo de Trabajo PIC) tendrá las siguientes funciones:

a) Efectuar el seguimiento periódico de las medidas y planes implantados en aplicación de este Real Decreto.

b) Elaborar, con el asesoramiento técnico pertinente, los diferentes Planes Estratégicos Sectoriales conforme a lo previsto en el Título III, Capítulo II, de este Real Decreto.

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

d) Supervisar y coordinar la realización de los estudios técnicos y los análisis de riesgos y vulnerabilidades que lleven a cabo los operadores críticos.

- e) Evaluar, tras la emisión de los correspondientes informes técnicos especializados, los Planes de Seguridad del Operador de los operadores críticos y proponerlos, en su caso, para su aprobación a la Comisión PIC.
- f) Proponer a la Comisión PIC los informes sobre evaluación de amenazas y los tipos de vulnerabilidades, amenazas y riesgos encontrados en cada uno de los sectores en los que se hayan designado ICE, con arreglo a lo dispuesto en la Directiva 2008/114/CE, para su presentación a la Comisión Europea.
- g) Efectuar los estudios y trabajos que, para la protección de infraestructuras críticas, le encomiende la Comisión PIC. Para ello podrá contar, si es necesario, con el apoyo de personal técnico especializado.

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

- a) Uno o dos representantes 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 del Ministerio del Interior, designado por el Director de la Dirección Adjunta Operativa de dicho cuerpo.
- c) Un representante de la Dirección Adjunta Operativa de la Guardia Civil del Ministerio del Interior, designado por el Director de la Dirección Adjunta Operativa de dicho cuerpo.
- d) Un representante del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis de Presidencia del Gobierno, designado por el Subsecretario de la Presidencia del Ministerio de la Presidencia.
- e) Un representante del Estado Mayor Conjunto del Ministerio de 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 de la Dirección General de Protección Civil y Emergencias del Ministerio del Interior, designado por el Director General de dicho organismo.

- h) Un representante del Consejo de Seguridad Nuclear, designado por el Presidente de dicho organismo.
- i) Un representante de aquellas Comunidades Autónomas con competencias estatutariamente asumidas para la protección de personas y bienes y el mantenimiento del orden público.
- j) Un representante del CNPIC, con funciones de Secretario.

3. Además de los miembros mencionados en el apartado anterior, también podrán asistir a las reuniones del Grupo PIC, por decisión de su Presidente, con voz pero sin voto, otras personas cuyo asesoramiento sea conveniente en algún aspecto concreto, en razón de los temas a tratar.

4. El Grupo de Trabajo PIC 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 estará radicada en el CNPIC.

5. Para el ejercicio de las competencias que este Real Decreto atribuye al Grupo de Trabajo PIC, podrán constituirse grupos de trabajo sectoriales para los sectores incluidos en el anexo I, en los que podrán participar los operadores críticos y otros actores y, en todo caso, el CNPIC y el correspondiente ministerio u organismo del Sistema.

## CAPÍTULO II

### Otros agentes del sistema de protección de infraestructuras críticas

#### *Artículo 12. Operadores críticos del Sector Público.*

1. Para la designación de un operador crítico del sector público, bastará con que al menos una de las infraestructuras que gestione reúna la consideración de infraestructura crítica, tras la aplicación de los criterios horizontales de criticidad por el órgano competente. En todo caso, el operador deberá ser oportunamente informado por el CNPIC de la clasificación o de la propuesta de clasificación de sus infraestructuras como IC, o como ICE.

2. Con carácter previo, el Ministerio del Interior, a través del CNPIC, y en coordinación con el ministerio u organismo del Sistema del que dependa el potencial operador crítico, notificará a éste su intención de declararlo como tal a partir de los datos disponibles sobre la criticidad de sus infraestructuras. Una vez notificado, el operador dispondrá de un plazo de dos meses a partir del día siguiente a su recepción para presentar sus observaciones al respecto.
3. La Comisión PIC designará a los operadores críticos del sector público en cada uno de los sectores estratégicos definidos, a propuesta del Grupo de Trabajo PIC y una vez consultados los ministerios y organismos del Sistema correspondientes.
4. Las notificaciones previas, la resolución de clasificación de un operador como crítico y las clasificaciones de IC o de ICE se realizarán de acuerdo con la clasificación de seguridad que corresponda según la normativa vigente.
5. Los operadores considerados críticos en virtud de este Real Decreto deberán colaborar con las autoridades competentes del Ministerio del Interior y de los diferentes ministerios y organismos del Sistema, con el fin de optimizar la protección de las IC y de las ICE por ellos gestionados y, especialmente:
  - a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo Nacional de Infraestructuras Estratégicas, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del Ministerio del Interior.
  - b) Colaborar, en su caso, con el Grupo de Trabajo PIC 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 conforme a lo previsto en el Título III, Capítulo III, de este Real Decreto.
  - d) Elaborar un Plan de Protección Específico por cada una de las infraestructuras consideradas críticas en el Catálogo, según se dispone en el Título III, Capítulo IV, de este Real Decreto.
  - e) Designar a un Responsable de Seguridad y Enlace de acuerdo a lo establecido en el Título III, Capítulo VI, de este Real Decreto.

- f) Designar a un Delegado de Seguridad por cada una de las infraestructuras de su titularidad que sean consideradas IC o ICE por el Ministerio del Interior, de acuerdo a lo establecido en el Título III, Capítulo VI, de este Real Decreto, comunicando dicha designación a los órganos correspondientes, en virtud del artículo 28 de este Real Decreto.
- g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y las medidas de seguridad que se han de implantar conforme al presente Real Decreto, solventando en el menor tiempo posible las deficiencias encontradas.

### **Artículo 13. Operadores críticos del Sector Privado.**

1. Para la designación de un operador crítico del sector privado, bastará con que al menos una de las infraestructuras por él gestionadas reúna la consideración de IC. En todo caso, el operador deberá ser oportunamente informado de la clasificación o de la propuesta de clasificación de sus infraestructuras como IC, o como ICE.
2. Con carácter previo, el Ministerio del Interior, a través del CNPIC, notificará al operador su intención de declararlo operador crítico a partir de los datos disponibles sobre la criticidad de sus infraestructuras. Una vez notificado, el operador dispondrá de un plazo de dos meses a partir del día siguiente a su notificación para presentar sus observaciones al respecto. Dicha notificación se hará, en su caso, de manera coordinada con el organismo u organismos reguladores con competencias en las autorizaciones de los operadores.
3. La Comisión PIC designará, a propuesta del Grupo de Trabajo PIC, consultados los ministerios y organismos del Sistema correspondientes, a los operadores críticos del sector privado en cada uno de los sectores estratégicos definidos.
4. Las notificaciones previas, la resolución de clasificación de un operador crítico y las clasificaciones de IC o de ICE se realizarán de acuerdo con la clasificación de seguridad que corresponda según la normativa vigente.

5. Los operadores considerados críticos en virtud de este Real Decreto deberán colaborar con las autoridades competentes del Ministerio del Interior y de los diferentes ministerios y organismos del Sistema, con el fin de optimizar la protección de las IC o ICE por ellos gestionados y, especialmente:
- a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo Nacional de Infraestructuras Estratégicas, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del citado Ministerio.
  - b) Colaborar, en su caso, con el Grupo de Trabajo PIC 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 conforme a lo previsto en el Título III, Capítulo III, de este Real Decreto.
  - d) Elaborar un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo Nacional de Infraestructuras, según se dispone en el Título III, Capítulo IV, de este Real Decreto.
  - e) Designar a un Responsable de Seguridad y Enlace de acuerdo a lo establecido en el Título III, Capítulo VI, de este Real Decreto.
  - f) Designar a un Delegado de Seguridad por cada una de las infraestructuras de su titularidad que sean consideradas IC o ICE por el Ministerio del Interior, de acuerdo a lo establecido en el Título III, Capítulo VI, de este Real Decreto, comunicando dicha designación a los órganos correspondientes, en virtud del artículo 28 de este Real Decreto.
  - g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y las medidas de seguridad que se han de implantar, en cumplimiento de este Real Decreto, solventando en el menor tiempo posible las deficiencias encontradas.

## TÍTULO III

### Instrumentos de protección

#### CAPÍTULO I

#### Plan Nacional de Protección de Infraestructuras Críticas

##### **Artículo 14.** *Finalidad y objetivos.*

1. El Plan Nacional de Protección de Infraestructuras Críticas es el plan elaborado por la Secretaría de Estado de Seguridad del Ministerio del Interior en el que se establecen los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones públicas y para articular las medidas preventivas necesarias, con el fin de asegurar la protección permanente, actualizada y homogénea de nuestro sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

##### **Artículo 15.** *Aprobación y registro del Plan.*

1. El Plan Nacional de Protección de Infraestructuras Críticas será aprobado por Resolución del Secretario de Estado de Seguridad, y quedará registrado en el CNPIC, así como en aquellos otros organismos que necesiten conocer del mismo, previa autorización del Secretario de Estado de Seguridad.

## CAPÍTULO II.

### Planes Estratégicos Sectoriales

#### Artículo 16. *Elaboración y contenido.*

1. El Grupo de Trabajo PIC, coordinado por el CNPIC, elaborará, en colaboración con los respectivos ministerios y organismos del Sistema, y con la participación de los operadores críticos, un Plan Estratégico por cada uno de los sectores o subsectores de actividad que se determinen.
2. 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.
3. Cada Plan Estratégico Sectorial deberá contener, al menos, los siguientes extremos:
  - a) Análisis de riesgos, vulnerabilidad y consecuencias.
  - b) Medidas organizativas y técnicas necesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los escenarios que se prevean.
  - c) Planes operativos para abordar posibles escenarios adversos.
  - d) Medidas preventivas y de mantenimiento, tales como, entre otras, ejercicios y simulacros, preparación e instrucción del personal, árboles de comunicación, y planes de evacuación.
  - e) Medidas de coordinación con el Plan Nacional de Protección de Infraestructuras Críticas.
4. Los Planes Estratégicos Sectoriales podrán constituirse teniendo en cuenta otros planes o programas ya existentes, creados en base a su propia legislación específica sectorial. Cuando los referidos planes o programas sectoriales reúnan los

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

#### **Artículo 17. *Aprobación y registro.***

1. Cada Plan Estratégico Sectorial deberá ser aprobado por la Comisión PIC en el plazo máximo de dieciocho meses a partir de la entrada en vigor de este Real Decreto. Su revisión y actualización se efectuará cada dos años, o cuando circunstancias extraordinarias lo aconsejen.

2. Los ministerios y organismos del Sistema llevarán un registro donde obren los Planes Estratégicos Sectoriales de los que sean competentes, que deberán mantener permanentemente actualizado. El CNPIC conservará un registro central de todos los Planes Estratégicos Sectoriales existentes, elaborado a partir de los obrantes en cada ministerio u organismo del Sistema.

### **CAPÍTULO III.**

#### **Planes de Seguridad del Operador**

#### **Artículo 18. *Elaboración y contenido.***

1. Los operadores críticos deberán, en un plazo de seis meses desde su designación, elaborar un Plan de Seguridad del Operador donde se defina la política general de dicho operador para la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.

2. El Plan de Seguridad del Operador deberá contener, al menos, la determinación de todas las IC y de las ICE del operador, así como las contramedidas implantadas y aquéllas que se proponen para su mejor protección.

3. El Plan de Seguridad del Operador deberá fundamentarse en un análisis de riesgos apropiado en el que se contemplen, de una manera global, tanto las amenazas físicas como lógicas. Así mismo, deberá diferenciar entre las medidas genéricas de protección de carácter permanente y aquellas de carácter temporal y gradual, definidas en el propio plan como a corto, medio o largo plazo, que podrán implantarse con la activación por el Secretario de Estado de Seguridad de un nivel de seguridad de los previstos en el Plan Nacional de Protección de Infraestructuras Críticas.

4. La Secretaría de Estado de Seguridad del Ministerio del Interior, a través del CNPIC, establecerá los contenidos mínimos del Plan de Seguridad del Operador, así como el modelo en el que basar dichos trabajos. En todo caso, cumplirá las directrices marcadas por el respectivo Plan Estratégico Sectorial.

#### **Artículo 19. *Aprobación y registro.***

1. La Comisión PIC, previo informe del Grupo de Trabajo PIC, 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. El Plan de Seguridad del Operador será revisado y actualizado con periodicidad anual, o cuando tenga lugar la inclusión o la baja de una IC o ICE en el Catálogo Nacional de Infraestructuras Estratégicas.

3. Los ministerios y organismos del Sistema llevarán un registro donde obren los Planes de Seguridad del Operador de los que sean competentes, que deberán mantener permanentemente actualizado. El CNPIC conservará un registro central de todos los Planes de Seguridad del Operador existentes, elaborado a partir de los obrantes en cada ministerio u organismo del Sistema.

## CAPÍTULO IV.

### Planes de Protección Específicos

#### **Artículo 20.** *Elaboración.*

1. La clasificación de una nueva infraestructura como IC no sólo conllevará para el operador la obligación de incluirla, en su Plan de Seguridad del Operador, sino el deber de elaborar un Plan de Protección Específico para dicha infraestructura, en el plazo máximo de seis meses desde dicha clasificación.
2. La clasificación de una infraestructura como ICE supondrá la obligación adicional de comunicar su identidad a otros Estados miembros que puedan verse afectados de forma significativa por aquella, 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.
3. Los Planes de Protección Específicos deberán establecerse a partir de los respectivos Planes de Seguridad del Operador a los que estén adscritos, y serán revisados y actualizados, con carácter anual, según el calendario que establezca el CNPIC.
4. En el momento en que un operador sea designado como crítico deberá presentar, en un plazo de dieciocho meses a partir de dicha designación, un Plan de Protección Específico de cada una de las infraestructuras consideradas críticas por el Ministerio del Interior. La presentación de dichos planes se hará en el citado Ministerio, a través de las respectivas Delegaciones del Gobierno en las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía, quedando depositados en el CNPIC.

#### **Artículo 21.** *Contenido y aplicación.*

1. El Plan de Protección Específico de una IC o ICE supondrá, con base en el pertinente análisis de riesgos de la instalación o sistema, la adopción de medidas permanentes de protección y de medidas temporales y graduadas, en razón a la

amenaza específica que se detecte en cada momento. Se contemplarán, de existir, tanto las amenazas físicas como aquellas de carácter lógico.

2. El Plan de Protección Específico deberá, asimismo, prever el plazo de ejecución de dichas medidas, que en el caso de las permanentes vendrán determinadas por lo especificado en el artículo 20 de este Real Decreto, y en el de las graduales, por la activación del Plan Nacional de Protección de Infraestructuras Críticas, o bien por las comunicaciones que las autoridades competentes puedan efectuar en relación a una amenaza concreta sobre una o varias infraestructuras.

3. El Ministerio del Interior, a través del CNPIC, establecerá los contenidos mínimos del Plan de Protección Específico, así como el modelo sobre el que basar dichos trabajos.

4. Los órganos competentes podrán, en todo momento, requerir del responsable de las IC o ICE, correcciones, modificaciones o actualizaciones de los Planes de Protección Específicos elaborados, en caso de variación de las circunstancias que determinaron su adopción o para adecuarlos a la normativa vigente que les afecte.

5. Los Delegados del Gobierno en las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía 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. Dichas facultades deberán desarrollarse, en su caso, de forma coordinada con el organismo u organismos reguladores con competencias en las autorizaciones de los operadores y tomando en consideración las facultades de inspección atribuidas a aquéllos.

## **Artículo 22.** *Compatibilidad con otros planes existentes.*

1. Los operadores elaborarán el preceptivo Plan de Protección Específico para cada una de sus infraestructuras que, conforme a lo dispuesto en este Real Decreto, se consideren críticas, independientemente del cumplimiento de lo exigido por el Código Técnico de la Edificación, la Norma Básica de Autoprotección, la normativa de Seguridad Privada o cualquier otra Reglamentación Sectorial Específica que le sea de aplicación.

2. 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 dicho 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 el presente Real Decreto.

3. 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 y en el Real Decreto 550/2006, de 5 de mayo, sin perjuicio de que el Ministerio del Interior, a través de su representante en el Comité Nacional de Seguridad de la Aviación Civil pueda proponer contenidos adicionales, de conformidad con lo establecido en el apartado 3 del artículo 21. Por su parte, se considerará Plan de Seguridad del Operador el previsto en el Programa Nacional de Seguridad para la Aviación Civil, pudiendo el Ministerio del Interior, a través de su representante en el Comité Nacional de Seguridad de la Aviación Civil proponer contenidos adicionales, de conformidad con lo establecido en el artículo 18. Todo ello, sin perjuicio de lo que le sea de aplicación según el presente Real Decreto.

### **Artículo 23. *Aprobación y registro.***

1. El Ministerio del Interior, previo informe de las Delegaciones del Gobierno en las respectivas Comunidades Autónomas y las Ciudades con Estatuto de Autonomía, y teniendo en cuenta las actuaciones de los organismos reguladores que pudieran ser competentes en las autorizaciones del operador, notificará al interesado, en el plazo máximo de dos meses, su resolución con la aprobación de los diferentes Planes de Protección Específicos o las eventuales propuestas de mejora de éstos.

2. Las Delegaciones del Gobierno en las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía y, en su caso, el órgano competente de cada Comunidad Autónoma, llevarán un registro donde obren todos los Planes de Protección Específicos de las IC y de las ICE localizadas en su demarcación, y que deberán mantener permanentemente actualizado. El CNPIC conservará un registro central de los Planes de Protección Específicos de la totalidad de las IC y de las ICE de la nación, en base a los obrantes en cada Delegación del Gobierno.

## CAPÍTULO V.

### Plan de Apoyo Operativo

#### **Artículo 24.** *Elaboración y contenido.*

1. Por cada una de las IC y de las ICE dotadas de un Plan de Protección Específico, la Delegación del Gobierno en la Comunidad Autónoma o Ciudad con Estatuto de Autonomía 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 con competencia en la demarcación, con la colaboración del responsable de seguridad de la infraestructura.
2. Sobre la base del Plan de Protección Específico, el Plan de Apoyo Operativo deberá contemplar, si la instalación lo precisa, las medidas planificadas de vigilancia, prevención, protección y reacción a prestar por las Administraciones públicas en caso de activación del Plan Nacional de Protección de Infraestructuras Críticas o de la existencia de una amenaza inminente sobre dicha infraestructura. Estas medidas serán complementarias a aquellas de carácter gradual que hayan sido previstas en el Plan de Protección Específico por el operador crítico.
3. El Ministerio del Interior, a través del CNPIC, establecerá los contenidos mínimos del Plan de Apoyo Operativo de la IC o ICE, así como el modelo sobre el que basar dichos trabajos.
4. El Ministerio del Interior, a través del CNPIC, podrá remitir al Ministerio de Defensa copia de los Planes de Apoyo Operativos de aquellas IC o ICE que, en caso de activación del Plan Nacional de Protección de Infraestructuras Críticas, y a los efectos de coordinar los correspondientes apoyos, en su caso, de las Fuerzas Armadas, se considere oportuno, previo estudio de los mencionados apoyos.

## **Artículo 25. *Aprobación y registro.***

1. Los Planes de Apoyo Operativos deberán ser validados por la Secretaría de Estado de Seguridad, a través del CNPIC.
2. Las Delegaciones del Gobierno en las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía y, en su caso, el órgano competente de cada Comunidad Autónoma, llevarán un registro donde obren todos los Planes de Apoyo Operativos de las IC e ICE localizadas en su demarcación, y que deberán mantener permanentemente actualizado. El CNPIC conservará un registro central de los Planes de Apoyo Operativos de la totalidad de las IC y de las ICE de la nación, en base a los obrantes en cada Delegación del gobierno.

## **CAPÍTULO VI.**

### **Comunicaciones entre los operadores críticos y las Administraciones públicas**

## **Artículo 26. *Seguridad de las comunicaciones.***

1. La Secretaría de Estado de Seguridad del Ministerio del Interior arbitrará los sistemas de gestión que permitan una continua actualización y revisión de la información disponible en el Catálogo Nacional de Infraestructuras Estratégicas por parte del CNPIC, así como su difusión a los organismos autorizados. Dichos sistemas serán administrados por el CNPIC, que contará con los apoyos necesarios de todos los organismos afectados e implicados.
2. Las Administraciones públicas velarán por la garantía de la confidencialidad de los datos sobre infraestructuras estratégicas a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada.
3. Los sistemas, las comunicaciones y la información objeto de este Real Decreto contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

4. La Presidencia del Gobierno facilitará el uso de la Malla B como sistema de comunicaciones seguras sobre el que las autoridades y centros concernidos puedan acceder a la información disponible en el Catálogo Nacional de Infraestructuras Estratégicas, sobre la premisa general de necesidad de conocer y con los niveles de acceso que se determinen.

5. La seguridad de los sistemas de información y comunicaciones objeto de este Real Decreto será acreditada y en su caso certificada por el Centro Criptológico Nacional, de acuerdo con las competencias establecidas en su normativa específica.

#### **Artículo 27.** *El Responsable de Seguridad y Enlace.*

1. Los operadores críticos, en el plazo de tres meses desde su designación, nombrarán y comunicarán al Ministerio del Interior así como al Ministerio u organismo del Sistema competente en el sector que corresponda, a un Responsable de Seguridad y Enlace con la Administración, que, en todo caso, deberá contar con la habilitación de Director de Seguridad, expedida por el Ministerio del Interior, según lo previsto en la normativa de Seguridad Privada, o la habilitación equivalente, según su normativa específica.

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

#### **Artículo 28.** *El Delegado de Seguridad de la infraestructura crítica.*

1. Los operadores con infraestructuras consideradas IC o ICE por el Ministerio del Interior comunicarán a las Delegaciones del Gobierno y, en su caso, al órgano competente de la Comunidad Autónoma donde aquéllas se ubiquen, en el plazo de tres meses, la existencia 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 concerniente a la seguridad concreta de la IC o ICE de que se trate, encauzando las necesidades operativas e informativas a este respecto.

## **Artículo 29.** *Seguridad de los datos clasificados.*

El operador crítico deberá garantizar la seguridad de los datos clasificados en relación a sus propias infraestructuras, mediante los medios de protección y los sistemas de información adecuados que, en todo caso, cumplirán con los requerimientos de seguridad establecidos por el Secretario de Estado Director del CNI, de acuerdo con la normativa específica de aplicación.

## **Disposición adicional primera.** *Normativa y régimen económico aplicable a la Comisión Nacional para la Protección de las Infraestructuras Críticas y al Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

En lo no previsto en el presente Real Decreto, se estará a lo dispuesto para el funcionamiento de 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. Así mismo, el funcionamiento y los trabajos de la Comisión Nacional para la Protección de las Infraestructuras Críticas, así como del Grupo de Trabajo Interdepartamental previstos en la presente norma se llevarán a cabo con cargo a las dotaciones presupuestarias y los medios personales y tecnológicos del Ministerio del Interior, sin que suponga incremento alguno del gasto público.

## **Disposición adicional segunda.** *Clasificación de los Planes.*

Los Planes contenidos en el Título III del presente Real Decreto tendrán la clasificación que les corresponda en virtud de la normativa vigente en la materia, la cual deberá constar de forma expresa en el instrumento de su aprobación.

## **Disposición transitoria primera.** *Actuaciones ya existentes en materia de Protección de Infraestructuras Críticas.*

Aquellos operadores responsables de IC o ICE que ya dispusieran, a la fecha de entrada en vigor del presente Real Decreto, de los Planes de Seguridad del Operador o de los Planes de Protección Específicos, deberán presentarlos ante los órganos de la Administración Pública competentes, para su autorización en los plazos que por los mismos se establezcan.

**Disposición transitoria segunda.** *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 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 de este Real Decreto. Dicha adaptación, en ningún caso, podrá generar incremento de gasto público.

**Disposición final primera.** *Título competencial.*

Este Real Decreto se dicta al amparo de la competencia atribuida al Estado en virtud del artículo 149.1.29º de la Constitución Española en materia de seguridad pública.

**Disposición final segunda.** *Incorporación de derecho comunitario.*

Mediante este Real Decreto se incorpora al derecho español la Directiva Directiva 2008/114/CE del Consejo de la Unión Europea, de 8 de diciembre de 2008, sobre la identificación y clasificación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

**Disposición final tercera.** *Habilitación para el desarrollo reglamentario.*

El Secretario de Estado de Seguridad, previo informe de la Comisión Nacional para la Protección de las Infraestructuras Críticas, dictará cuantas disposiciones sean necesarias para la aplicación y desarrollo del presente Real Decreto.

Las eventuales modificaciones que se efectúen en el anexo I del presente Real Decreto en virtud de lo dispuesto en el artículo 8 de éste se efectuarán por Orden conjunta del Ministro del Interior y del titular del Ministerio interesado.

**Disposición final cuarta.** *Entrada en vigor.*

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

## ANEXO I: SECTORES ESTRATÉGICOS Y MINISTERIOS / ORGANISMOS DEL SISTEMA COMPETENTES

SECTOR	MINISTERIO / ORGANISMO DEL SISTEMA
ADMINISTRACIÓN	Mº PRESIDENCIA Mº INTERIOR Mº DEFENSA CENTRO NACIONAL DE INTELIGENCIA
ESPACIO	Mº DEFENSA
INDUSTRIA NUCLEAR	Mº INDUSTRIA, TURISMO Y COMERCIO CONSEJO DE SEGURIDAD NUCLEAR
INDUSTRIA QUÍMICA	Mº INTERIOR
INSTALACIONES DE INVESTIGACIÓN	Mº CIENCIA E INNOVACIÓN Mº MEDIO AMBIENTE Y MEDIO RURAL Y MARINO
AGUA	Mº MEDIO AMBIENTE Y MEDIO RURAL Y MARINO Mº SANIDAD Y POLÍTICA SOCIAL
ENERGÍA	Mº INDUSTRIA, TURISMO Y COMERCIO
SALUD	Mº SANIDAD Y POLÍTICA SOCIAL Mº CIENCIA E INNOVACIÓN
TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC)	Mº INDUSTRIA, TURISMO Y COMERCIO Mº DEFENSA CENTRO NACIONAL DE INTELIGENCIA Mº CIENCIA E INNOVACIÓN
TRANSPORTE	Mº FOMENTO
ALIMENTACIÓN	Mº MEDIO AMBIENTE Y MEDIO RURAL Y MARINO Mº SANIDAD Y POLÍTICA SOCIAL Mº INDUSTRIA, TURISMO Y COMERCIO
SISTEMA FINANCIERO Y TRIBUTARIO	Mº ECONOMÍA Y HACIENDA