T E M A 1 4

MEDIDAS PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS. EL CATÁLOGO NACIONAL DE INFRAESTRUCTURAS CRÍTICAS. EL SISTEMA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS. CIBERSEGURIDAD.

La **Ley 8/2011, de 28 de abril**, por la que se establecen **medidas para la protección de las infraestructuras críticas traspone la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección**, que 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 se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

Esta Ley tiene por objeto establecer 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, para mejorar la prevención, preparación y respuesta de nuestro Estado **frente a atentados terroristas u otras amenazas** que afecten a infraestructuras críticas.

El **Real Decreto 704/2011, de 20 de mayo** aprueba el **Reglamento de protección de las infraestructuras críticas**.

Definiciones.

A los efectos de la presente Ley, se entenderá por:

a) **Servicio 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 las Administraciones Públicas**.

b) **Sector estratégico**: cada una de las **áreas diferenciadas dentro de la actividad laboral**, económica y productiva, que proporciona un **servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país**. Su categorización viene determinada en el **anexo** 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**: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

e) **Infraestructuras críticas**: las **infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas**, por lo que su perturbación o destrucción tendría un **grave impacto sobre los servicios esenciales**.

f) **Infraestructuras críticas europeas**: aquellas **infraestructuras críticas situadas en algún Estado miembro de la Unión Europea**, cuya **perturbación o destrucción afectaría gravemente** al menos a **dos Estados miembros**, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, 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).

g) **Zona crítica**: 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 zona crítica tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores titulares de infraestructuras críticas o infraestructuras críticas europeas radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad del Estado y las Policías Autonómicas de carácter integral.

h) **Criterios horizontales de criticidad**: los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica **se evaluarán en función de**:

1. El número de **personas afectadas**, valorado en función del número potencial de **víctimas mortales o heridos con lesiones graves** y las **consecuencias para la salud pública.**

2. El **impacto económico** en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.

3. El **impacto medioambiental**, degradación en el lugar y sus alrededores.

4. El **impacto público y social**, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, 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 perturbación o destrucción de las infraestructuras que le dan apoyo.

j) **Interdependencias**: los **efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones** o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, 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 **perturbación 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 a la presente Ley.

n) **Nivel de Seguridad**: aquel cuya **activación por el Ministerio del Interior está prevista 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 virtud del cual corresponderá declarar 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.

Ámbito de aplicación.

1. La presente Ley se aplicará a las **infraestructuras críticas ubicadas en el territorio nacional** vinculadas a los sectores estratégicos definidos en el anexo de esta Ley.

2. Se **exceptúan** de su aplicación las **infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad**, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos.

3. La aplicación de esta Ley se efectuará sin perjuicio de:

a) La misión y funciones del Centro Nacional de Inteligencia establecidas en su normativa específica, contando siempre con la necesaria colaboración y complementariedad con aquéllas.

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.

El Catálogo Nacional de Infraestructuras Estratégicas.

El **Ministerio del Interior**, a través de la **Secretaría de Estado de Seguridad**, será el **responsable del Catálogo Nacional de Infraestructuras Estratégicas** (en adelante, el Catálogo), instrumento que contendrá toda la información y valoración de las infraestructuras estratégicas del país, entre las que **se hallarán incluidas aquellas clasificadas como Críticas o Críticas Europeas.**

La competencia para clasificar una infraestructura como estratégica, y en su caso, como infraestructura crítica o infraestructura crítica europea, así como para incluirla en el Catálogo Nacional de Infraestructuras Estratégicas, corresponderá al Ministerio del Interior, a través de la Secretaria de Estado de Seguridad, incluidas las propuestas, en su caso, del órgano competente de las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público en relación con las infraestructuras ubicadas en su demarcación territorial.

El Reglamento de desarrollo de la presente ley amplía lo siguiente en relación al Catálogo:

Contenido del Catálogo.

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.**

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.

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.

Gestión y actualización del Catálogo.

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.**

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.

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.

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.

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**.

El Sistema de Protección de Infraestructuras Críticas

Finalidad.

1. El **Sistema de Protección de Infraestructuras Críticas** (en adelante, el Sistema) se compone de una **serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos**.

2. Son **agentes del Sistema**, con las funciones que se determinen reglamentariamente, los siguientes:

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 de esta Ley.

d) Las **Comunidades Autónomas** y las **Ciudades con Estatuto de Autonomía**.

e) Las **Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía**.

f) Las **Corporaciones Locales**, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.

g) La **Comisión Nacional para la Protección de las Infraestructuras Críticas**.

h) El **Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas**.

i) Los **operadores críticos del sector público y privado**.

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, Unión Europea 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.

El Centro Nacional para la Protección de las Infraestructuras Críticas.

1. Se crea el **Centro Nacional para la Protección de las Infraestructuras Críticas** (en adelante, el **CNPIC**) como órgano ministerial **encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad** en relación con la protección de las Infraestructuras Críticas en el territorio nacional.

2. El CNPIC **dependerá 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 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**.

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** (***funciones asumidas en la actualidad por el CITCO***).

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 (***funciones asumidas en la actualidad por el CITCO***), 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.

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

Por cada sector estratégico, se designará, al menos, un ministerio, organismo, entidad u órgano de la Administración General del Estado integrado en el Sistema. El nombramiento, alta o baja en éste de un ministerio u organismo con responsabilidad sobre un sector estratégico se efectuará mediante la modificación del anexo de la presente Ley.

Los ministerios y organismos del Sistema serán los encargados de impulsar, en el ámbito de sus competencias, **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**.

Un ministerio u organismo del Sistema podrá tener competencias, igualmente, sobre dos o más sectores estratégicos, conforme a lo establecido en el anexo de la presente Ley.

Los **ministerios y organismos del Sistema** 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.

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.

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.

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.

Comunidades Autónomas y Ciudades con Estatuto de Autonomía.

Las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten 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.

En todo caso, las Comunidades Autónomas mencionadas en el apartado anterior **participarán en el proceso de declaración de una zona como crítica, en la aprobación del Plan de Apoyo Operativo que corresponda, y en las reuniones del Grupo de Trabajo Interdepartamental.** Asimismo, **serán miembros de la Comisión Nacional para la Protección de las Infraestructuras Críticas**.

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.

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**.

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.

Comisión Nacional para la Protección de las Infraestructuras Críticas.

Se crea la **Comisión Nacional para la Protección de las Infraestructuras Críticas** (en adelante, la **Comisión**) como **órgano colegiado adscrito a la Secretaría de Estado de Seguridad**.

La Comisión **será la competente para aprobar los diferentes Planes Estratégicos Sectoriales así como para designar a los operadores críticos, a propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas**.

La Comisión Nacional para la Protección de las Infraestructuras Críticas 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 aquellas otras tareas que se estimen precisas en el marco de la cooperación interministerial para la protección de las infraestructuras críticas.

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**.

El **Director General 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.

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.

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.

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

Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

El Sistema contará con un **Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas** (en adelante, el Grupo de Trabajo).

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**.

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.

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, 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**.

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.

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.

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.

Operadores críticos.

Los **operadores** considerados **críticos** en virtud de esta Ley deberán **colaborar con las autoridades competentes del Sistema**, con el fin de **optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados**.

Será **requisito para la designación de los operadores críticos**, tanto del **sector público como del privado**, que **al menos una de las infraestructuras que gestionen reúna la consideración de Infraestructura Crítica**, mediante la correspondiente propuesta de la que, en todo caso, el CNPIC informará al operador antes de proceder a su clasificación definitiva.

Los operadores críticos serán los **agentes integrantes del Sistema procedentes tanto del sector público como del sector privado**.

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**.

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.

e) **Designar a un Responsable de Seguridad y Enlace**.

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.

g) **Facilitar las inspecciones** que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial.

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.

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 en el 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 el reglamento, debiendo comunicar dicha decisión al CNPIC.

Instrumentos y comunicación del Sistema

Instrumentos de planificación del Sistema.

La **Protección de las Infraestructuras Críticas** frente a las eventuales amenazas que puedan ponerlas en situación de riesgo requiere la adopción y aplicación de los siguientes **planes de actuación**:

a) El Plan Nacional de Protección de las Infraestructuras Críticas

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.

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.

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**.

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**.

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.

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

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**.

b) Los Planes Estratégicos Sectoriales

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**.

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.

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.

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**.

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.

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**.

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.

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.

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

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.

c) Los Planes de Seguridad del Operador

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.

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.

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.

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.**

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.

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.

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.

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.

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.

d) Los Planes de Protección Específicos

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**.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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, la normativa de Seguridad Privada o cualquier otra reglamentación sectorial específica que le sea de aplicación.

Las **instalaciones Nucleares e Instalaciones Radiactivas** que se consideren críticas integrarán sus Planes de Protección Específicos en los respectivos Planes de Protección Física.

Las **instalaciones portuarias** integrarán sus Planes de Protección Específicos en los Planes de Protección de Puertos.

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. 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.

e) Los Planes de Apoyo Operativo

Los **Planes de Apoyo Operativo deberán ser elaborados por el Cuerpo Policial estatal o, en su caso, autonómico, con competencia en la demarcación, para cada una de las infraestructuras clasificadas como Críticas o Críticas Europeas dotadas de un Plan de Protección Específico, debiendo contemplar las medidas de vigilancia, prevención, protección o reacción a prestar, de forma complementaria a aquellas previstas por los operadores críticos**.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

Plan de Prevención y Protección Antiterrorista

Los **Niveles de Alerta Antiterrorista** fueron introducidos en España por primera vez por el **Plan de Prevención y Protección Antiterrorista de 9 de marzo de 2005**.

El actual sistema de niveles entró en vigor en **mayo del 2015** como consecuencia de la publicación de la **Instrucción 3/2015 de la Secretaría de Estado de Seguridad**.

El **Plan de Prevención y Protección Antiterrorista** establece las **directrices generales** que, partiendo de un esfuerzo permanente en el ámbito preventivo, **permitan asegurar la detección, seguimiento, análisis y evaluación continuada del riesgo de atentado terrorista, así como la puesta en marcha y coordinación de los dispositivos preventivos en caso necesario**, entendidos éstos como el conjunto de acciones llevadas a cabo con anterioridad a que se materialice un atentado terrorista con el objetivo de evitar que se produzca.

El **Nivel de Alerta Antiterrorista** consiste en **una escala compuesta por varios niveles complementarios, cada uno de los cuales se encuentra asociado a un grado de riesgo**, en función de la valoración de la amenaza terrorista que se aprecie en cada momento.

La clasificación prevista en el Plan de Prevención y Protección Antiterrorista cuenta con **cinco niveles de activación** asociados a un determinado nivel de riesgo: el **Nivel 1** corresponde a **riesgo bajo**, el **Nivel 2** a **riesgo moderado**, el **Nivel 3** a **riesgo medio**, el **Nivel 4** a **riesgo alto** y el **Nivel 5** a **riesgo muy alto**.

La activación de cada NAA compete al ministro del Interior, a través de la Secretaría de Estado de Seguridad, en base a los informes de valoración de la amenaza y otras circunstancias asociadas a la misma que elabora un comité integrado por expertos en la lucha antiterrorista.

La activación de cada NAA depende de la valoración de la amenaza y otras circunstancias asociadas a la misma. Por un lado, la amenaza se valorará en función de la intención, la capacidad y la probabilidad de comisión de un atentado terrorista. Por otro, su correlación se valorará en función de la vulnerabilidad de los potenciales objetivos de ataque y su posible impacto o repercusión.

CIBERSEGURIDAD

Seguridad de las comunicaciones.

La **Secretaría de Estado de Seguridad arbitrará los sistemas de gestión que permitan una continua actualización y revisión de la información disponible en el Catálogo por parte del CNPIC**, así como su difusión a los organismos autorizados.

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.

Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

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.

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.

La **Presidencia del Gobierno facilitará el uso de la Malla B, sistema soporte de comunicaciones estratégicas seguras del Sistema Nacional de Gestión de Crisis 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.

El Responsable de Seguridad y Enlace.

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 todo caso, **el Responsable de Seguridad y Enlace designado 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 con la habilitación equivalente, según su normativa específica.

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.

El Delegado de Seguridad de la Infraestructura Crítica.

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**.

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.

Seguridad de los datos clasificados.

El **operador crítico deberá garantizar la seguridad de los datos clasificados relativos a sus propias infraestructuras**, mediante los medios de protección y los sistemas de información adecuados que reglamentariamente se determinen.

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.

Directiva UE-NIS

El día 6 de Julio de 2016 se aprobó por el **Parlamento Europeo y el Consejo**, la directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS.

El **objetivo** de la Directiva es **lograr un nivel común de seguridad de redes y sistemas de información dentro de la Unión Europea** a través de la mejora de la ciberseguridad a nivel nacional, el aumento de la cooperación a nivel de la Unión Europea y la gestión de riesgos y las obligaciones de notificación de incidentes para los operadores de servicios esenciales y los proveedores servicios digitales.

En particular se encuentran **dentro del ámbito de esta directiva los operadores que prestan servicios de energía, transporte, financiero, salud, agua, dominios de internet, puntos neutros de intercambio de internet, plataformas de comercio electrónico, *cloud computing* y motores de búsqueda**. Además, algunos proveedores de servicios de Internet o motores de búsqueda y servicios de *Cloud Computing*, también tendrán que garantizar la seguridad de su infraestructura e informar sobre incidentes graves. Sin embargo otros proveedores de servicios, como por ejemplo los relacionados con las redes sociales, no estarán sujetos a esta norma.

La Directiva obliga a los Estados a determinar conforme a una serie de parámetros **cuáles** de entre los proveedores que prestan esos servicios **son las empresas obligadas,**

señalar la autoridad competente o los equipos de respuesta a incidentes de seguridad informática a nivel nacional (**CSIRT**, *Computer Security Incident Response Teams*) y a la **creación de un mecanismo de cooperación a nivel europeo**.

Las **propuestas** clave de la Directiva NIS son:

1. Que **cada país adopte una estrategia de ciberseguridad y una autoridad competente**.

2. **Crear un mecanismo de cooperación** para compartir información sobre seguridad en toda la Unión Europea.

3. **Que los operadores de infraestructuras críticas**, como energía y transporte, y los proveedores de servicios (plataformas de correo electrónico, redes sociales, motores de búsqueda), **adopten las medidas necesarias para gestionar sus riesgos de seguridad** e informen sobre los incidentes de seguridad que sufran las autoridades nacionales competentes.

OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

El Convenio Marco de Colaboración en materia de ciberseguridad, de 4 de octubre de 2012, entre la Secretaría de Estado de Seguridad y la Secretaría de Estado para el avance digital, tiene por objeto mejorar las capacidades de ciberseguridad en el ámbito de los Ministerios concernidos y de sus órganos y unidades dependientes.

La colaboración mutua, conforme al mencionado Convenio, ***se llevará a cabo mediante la coordinación del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y de las Fuerzas y Cuerpos de Seguridad del Estado, por parte de la Secretaría de Estado de Seguridad, con el Instituto Nacional de Ciberseguridad (INCIBE), por parte de la Secretaría de Estado de Digitalización e Inteligencia Artificial***. El espacio de dicha colaboración se sustenta en el apoyo en la resolución de incidentes y en la mitigación de sus efectos, así como en el intercambio de información de interés.

El eje de esta colaboración **se apoya**, a su vez, **en el Centro de Respuesta a Incidentes Cibernéticos** (**CSIRT**), ubicado en León y gestionado por INCIBE. Dicho Centro, denominado originariamente CERT de Seguridad e Industria (CERT-SI), **ahora INCIBE-CERT**, es un órgano de carácter nacional con un ámbito de actuación que incluye los ciudadanos, las empresas y la red académica española.

En el marco del Convenio Marco de Colaboración, **el INCIBE-CERT tiene la finalidad de prestar apoyo de carácter técnico a la Secretaría de Estado de Seguridad** y a sus órganos dependientes y, muy especialmente, en materia de protección de infraestructuras críticas y en las actividades de lucha contra la ciberdelincuencia y el ciberterrorismo.

Todo ello requiere que para la ejecución de las distintas actividades de carácter técnico que se derivan del referido Convenio, se disponga de un mecanismo que garantice un enlace apropiado y la coordinación técnica de los distintos órganos dependientes de esta Secretaría de Estado, entre sí y con aquéllos pertenecientes a la Secretaría de Estado para el Avance digital, y muy especialmente con el INCIBE-CERT.

El Real Decreto 734/2020, de 4 de agosto., por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, establece en su artículo *2.1.b) que al Secretario de Estado de Seguridad le corresponde "el ejercicio del mando de las Fuerzas y Cuerpos de Seguridad del Estado, la coordinación y la supervisión de los servicios y misiones que les corresponden". En particular, el citado real decreto establece en su artículo 2.3.a) que* ***el Gabinete de Coordinación y Estudios "es el órgano de apoyo y asesoramiento a través del cual el Secretario de Estado de Seguridad ejerce su función de coordinación y supervisión de la actuación de las Fuerzas y Cuerpos de Seguridad del Estado****"*.

Con el fin de efectuar un adecuado cumplimiento de las actividades de ciberseguridad derivadas de lo estipulado por la Estrategia de Seguridad Nacional y por la Estrategia de Ciberseguridad Nacional, en lo que se refiere a las competencias del Ministerio del Interior, y teniendo en cuenta los compromisos adquiridos con otros Departamentos Ministeriales y organismos, la Secretaría de Estado de Seguridad debe disponer de mecanismos eficaces que garanticen la coordinación de sus órganos subordinados.

Por todo ello, mediante la **Instrucción 15/2014, de la Secretaría de Estado de Seguridad,** se procede a crear, en el seno de esta Secretaría de Estado, un mecanismo que coordina, desde el punto de vista técnico, todas las actividades procedimentales e informativas necesarias para llevar a cabo de forma eficiente los cometidos que los diferentes órganos dependientes desarrollan en el ámbito de la ciberseguridad. **Este órgano se denomina Oficina de Coordinación Cibernética (*ahora Oficina de Coordinación de Ciberseguridad).***

La Oficina de Coordinación de Ciberseguridad permite una mejora sistémica y organizativa y una mayor eficiencia en la gestión de la ciberseguridad en esta Secretaría de Estado, fortaleciendo el papel del Ministerio del Interior en la gestión y ejecución de aquellos aspectos de la Estrategia de Ciberseguridad Nacional que se encuentran dentro de su competencia.

Esta instrucción tiene por objeto la creación de la Oficina de Coordinación de Ciberseguridad, consignándola como el órgano técnico de coordinación de la Secretaría de Estado de Seguridad en materia de ciberseguridad. La Oficina de Coordinación de Ciberseguridad actúa también como enlace con las autoridades competentes designadas, tanto nacional como internacionalmente, en este campo, de conformidad con las competencias asignadas a la Secretaría de Estado de Seguridad.

La **Oficina de Coordinación de Ciberseguridad** se estructura en un **grupo de análisis y tratamiento de la información**, **otro de análisis de amenazas y vulnerabilidades** y un **tercer grupo de monitorización del estado de la ciberseguridad**.

Se encuentra integrada orgánicamente en el Centro Nacional para la Protección de las Infraestructuras Críticas, dependiendo funcionalmente del Secretario de Estado de Seguridad.

La Oficina de Coordinación de Ciberseguridad **asesora al Secretario de Estado de Seguridad** en materia de ciberseguridad, aportando la información estratégica y técnica necesaria que facilita su proceso de toma de decisiones.

La Oficina de Coordinación de Ciberseguridad es también **responsable de la coordinación técnica entre la Secretaría de Estado y sus organismos dependientes y el INCIBE-CERT**. Para ello, dispone de los mecanismos de intercambio de información seguros necesarios para comunicarse tanto con dicho CERT como con las distintas unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado, agilizando la difusión de información que pueda ser de interés para cualquiera de las partes.

Los **objetivos** de la Oficina de Coordinación de Ciberseguridad son:

1. **Desarrollar mecanismos de coordinación de respuesta ante ciberincidentes** que recaigan en los ámbitos competenciales del Ministerio del Interior, teniendo capacidades para llevar a cabo los siguientes cometidos:

-Aportar las respuestas técnicas apropiadas, a través de la **activación de los protocolos existentes con otros CERT y equipos de respuesta a incidentes, nacionales e internacionales**. Todo ello, en colaboración con los responsables técnicos de los sistemas afectados y con el objeto de facilitar la adecuada gestión del incidente y la posterior resolución y recuperación de los sistemas implicados.

-**Proporcionar a las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado aquella información técnica** extraída de las actividades del CERT de Seguridad e Industria, o de aquellos otros agentes que en este campo puedan ser de utilidad, sin perjuicio de que aquéllas lleven a cabo, en uso de sus atribuciones y de manera exclusiva, las labores de investigación y persecución del delito, si esto fuese necesario.

-**Recibir y procesar datos relevantes que, procedentes de las actividades de las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado, puedan ser de interés en materia de ciberseguridad** y, muy especialmente, aquella información que sobre tipologías o patrones de ataque puedan suponer una mejora de la gestión de incidentes.

-**Establecer**, sin perjuicio de los ya habilitados para las Fuerzas y Cuerpos de Seguridad del Estado en uso de sus atribuciones, **cauces de intercambio de información entre otros actores, públicos y privados, nacionales e internacionales, diferentes a los contemplados en los puntos anteriores**, siempre que sean competentes en el ámbito de la ciberseguridad. En concreto, la Oficina de Coordinación de Ciberseguridad deberá garantizar que existan unas relaciones fluidas de carácter técnico e informativo, tanto a través de medios manuales como telemáticos, con objeto de disponer de los datos más actualizados, de cara a poder agilizar la gestión y respuesta de incidentes.

2. **Conocer el estado general de situación sobre ciberamenazas y avances tecnológicos**, contando para ello con la información aportada por publicaciones especializadas, fuentes abiertas y restringidas y por aquellos actores públicos y privados relevantes. Para ello, desarrollará los siguientes cometidos en materia de ciberseguridad:

Realizar estudios y análisis de situación genéricos y específicos.

Desarrollar guías, procedimientos y buenas prácticas de ámbito técnico.

Planificar, ejecutar y comunicar procedimientos específicos de resolución de incidentes relacionados con vulnerabilidades concretas.

Difundir notas informativas sobre aspectos de carácter técnico que requieran una especial atención.

Establecer canales de intercambio de información permanentes en lo relativo a estudios, vulnerabilidades, alertas, amenazas e incidentes, tanto a nivel nacional como internacional.

Los órganos y unidades dependientes de la Secretaría de Estado de Seguridad habilitarán los mecanismos pertinentes para facilitar la comunicación a la Oficina de Coordinación de Ciberseguridad de aquellos aspectos que en materia de ciberseguridad les sean de aplicación, conforme a lo estipulado en esta Instrucción. Entre estos mecanismos deberá contarse un protocolo para el intercambio de información entre ambas partes.

INCIBE-CERT

El INCIBE-CERT es, siguiendo las siglas en inglés, Capacidad de Respuesta a incidentes de Seguridad de la Información del Ministerio de Asuntos Económicos y Transformación Digital y del Ministerio del Interior. Por Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015, **el INCIBE-CERT es el CERT Nacional competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas**.

Operado técnicamente por INCIBE, y bajo la coordinación del CNPIC e INCIBE, el INCIBE- CERT se constituyó (*con el nombre de CERTSI*) en el año 2012 a través de un Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la Secretaría de Estado de Seguridad y la actual Secretaría de Estado de Digitalización e Inteligencia Artificial. Actualmente es regulado mediante Acuerdo de 21 de octubre de 2015, suscrito por ambas Secretarías de Estado.

Los operadores de infraestructuras críticas, públicos o privados, designados en virtud de la aplicación de la Ley 8/2011, tienen en el INCIBE-CERT su punto de referencia para la resolución técnica de incidentes de ciberseguridad que puedan afectar a la prestación de los servicios esenciales, según establece la Resolución de 8 de septiembre de 2015 (publicada en el BOE de 19 de septiembre), de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.

INCIBE

El **Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente de Red.es y del Ministerio de Asuntos Económicos y Transformación Digital** de España.

INCIBE tiene el **objetivo** de **desarrollar la Sociedad de la Información mediante la innovación y el desarrollo de proyectos relacionados con la ciberseguridad nacional e internacional**.

CONSEJO NACIONAL DE CIBERSEGURIDAD

Es un **órgano de apoyo del Consejo de Seguridad Nacional**, de pendiente de **Presidencia del Gobierno**.

Está **presidido por el Secretario de Estado Director del Centro Nacional de Inteligencia (CNI)**.

Se reúne a iniciativa de su presidente **como mínimo con carácter bimestral** o **cuantas veces lo considere necesario** atendiendo a las circunstancias que afecten a la Ciberseguridad.

Funciones:

- **Apoyar la toma de decisiones del Consejo de Seguridad Nacional en materia de ciberseguridad** mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

- **Reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias relacionadas con el ámbito de la ciberseguridad, así como entre los sectores público y privado**.

- **Contribuir a la elaboración de propuestas normativas en el ámbito de la ciberseguridad para su consideración por el Consejo de Seguridad Nacional**.

- **Prestar apoyo al Consejo de Seguridad Nacional en su función de verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional** en lo relacionado con la ciberseguridad y promover e impulsar sus revisiones.

- **Verificar el grado de cumplimiento de la Estrategia de Ciberseguridad Nacional** e informar al Consejo de Seguridad Nacional.

- **Realizar la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad** y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.

- Contribuir a la disponibilidad de los recursos existentes y realizar los estudios y análisis sobre los medios y capacidades de las distintas Administraciones Públicas y Agencias implicadas con la finalidad de catalogar las medidas de respuesta eficaz en consonancia con los medios disponibles y las misiones a realizar, todo ello en coordinación con los órganos y autoridades directamente competentes y de acuerdo con las competencias de las diferentes Administraciones Públicas implicadas en el ámbito de la ciberseguridad.

- Facilitar la coordinación operativa entre los órganos y autoridades competentes cuando las situaciones que afecten a la Ciberseguridad lo precisen y mientras no actúe el Comité Especializado de Situación.

- Todas aquellas otras funciones que le encomiende el Consejo de Seguridad Nacional.

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Objeto

1. El presente real decreto-ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes.

2. Así mismo, establece un marco institucional para la aplicación de este real decreto-ley y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario.

Definiciones:

a) **Redes y sistemas de información**, cualquiera de los elementos siguientes:

1.º Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones;

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales;

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

b) **Seguridad de las redes y sistemas de información**: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

c) **Servicio esencial**: 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 las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

d) **Operador de servicios esenciales**: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.

e) **Servicio digital**: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

f) **Proveedor de servicios digitales**: persona jurídica que presta un servicio digital.

g) **Riesgo**: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen.

h) **Incidente**: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

i) **Gestión de incidentes**: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

j) **Representante**: persona física o jurídica establecida en la Unión Europea que ha sido designada expresamente para actuar por cuenta de un proveedor de servicios digitales no establecido en la Unión Europea, a la que, en sustitución del proveedor de servicios digitales, pueda dirigirse una autoridad competente nacional o un CSIRT, en relación con las obligaciones que, en virtud de este real decreto-ley, tiene el proveedor de servicios digitales.

k) **Norma técnica**: una norma en el sentido del artículo 2.1 del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea.

l) **Especificación**: una especificación técnica en el sentido del artículo 2.4 del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012.

m) **Punto de intercambio de Internet** («IXP», por sus siglas en inglés de «Internet eXchange Point»): una instalación de red que permite interconectar más de dos sistemas autónomos independientes, principalmente para facilitar el intercambio de tráfico de Internet. Un IXP permite interconectar sistemas autónomos sin requerir que el tráfico de Internet que pasa entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, y sin modificar ni interferir de otra forma en dicho tráfico.

n) **Sistema de nombres de dominio** («DNS», por sus siglas en inglés de «Domain Name System»): sistema distribuido jerárquicamente que responde a consultas proporcionando información asociada a nombres de dominio, en particular, la relativa a los identificadores utilizados para localizar y direccionar equipos en Internet.

o) **Proveedor de servicios de DNS**: entidad que presta servicios de DNS en Internet.

p) **Registro de nombres de dominio de primer nivel**: entidad que administra y dirige el registro de nombres de dominio de Internet en un dominio específico de primer nivel.

q) **Mercado en línea**: servicio digital que permite a los consumidores y a los empresarios, tal y como se definen respectivamente en los artículos 3 y 4 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado mediante el Real Decreto Legislativo 1/2007, de 16 de noviembre, celebrar entre sí contratos de compraventa o de prestación de servicios en línea con empresarios, ya sea en un sitio web específico del servicio de mercado en línea, o en un sitio web de un empresario que utilice servicios informáticos proporcionados al efecto por el proveedor del servicio de mercado en línea.

r) **Motor de búsqueda en línea**: servicio digital que permite a los usuarios hacer búsquedas de, en principio, todos los sitios web o de sitios web en una lengua en concreto, mediante una consulta sobre un tema en forma de palabra clave, frase u otro tipo de entrada, y que, en respuesta, muestra enlaces en los que puede encontrarse información relacionada con el contenido solicitado.

s) **Servicio de computación en nube**: servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir.

ESTRATEGIA DE CIBERSEGURIDAD 2019

Desarrollada por la Orden PCI/487/2019 de 26 de abril y estructurada en cinco capítulos:

*1.- **El ciberespacio, más allá de un espacio común global**.*

*2.- **Las amenazas y desafíos del ciberespacio**.* En el que se definen y enumeran las ciberamenazas.

*3.- **Propósitos, principios y objetivos para la ciberseguridad**.* El propósito de la Estrategia es fijar las directrices generales de ciberseguridad para que alcancen los objetivos de 2017. Los principios rectores de la estrategia son cuatro: **Unidad de acción, anticipación, eficiencia y resiliencia.** Los objetivos son:

- Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.

- Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso

- Protección del ecosistema empresarial y social y de los ciudadanos

- Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas

- Seguridad del ciberespacio en el ámbito internacional

*4.- **Líneas de acción y medidas**.* Se establecen siete líneas de acción:

- Línea de Acción 1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio. Esta línea de acción responde al **Objetivo I** de la Estrategia.

- Línea de Acción 2. Garantizar la seguridad y resiliencia de los activos estratégicos para España. Esta línea de acción responde al **Objetivo I** de la Estrategia.

- Línea de Acción 3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio. Esta línea de acción responde al **Objetivo II** de la Estrategia.

- Línea de Acción 4. Impulsar la ciberseguridad de ciudadanos y empresas. Esta línea de acción responde al **Objetivo III** de la Estrategia.

- Línea de Acción 5. Potenciar la industria española de ciberseguridad y la generación y retención de talento para el fortalecimiento de la autonomía digital. Esta línea de acción responde al **Objetivo IV** de la Estrategia

- Línea de Acción 6. Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacional. Esta línea de acción responde al **Objetivo V** de la Estrategia.

- <u>Línea de Acción 7</u>. Desarrollar una cultura de ciberseguridad. Las medidas incluidas en esta Línea de Acción contribuirán al Plan de Cultura de Seguridad Nacional y responde al **objetivo IV** de la Estrategia.

*5.- **La ciberseguridad en el sistema de Seguridad Nacional**.* La **estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional** está constituida por los siguientes componentes:

1. El Consejo de Seguridad Nacional.

2. El Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis.

3. El Consejo Nacional de Ciberseguridad.

4. La Comisión Permanente de Ciberseguridad.

5. Foro Nacional de Ciberseguridad.

6. Las Autoridades públicas competentes y los CSIRT de referencia nacionales.