Plan Nacional de protección de infraestructuras críticas

F. J. Sánchez Gómez

La dependencia de las sociedades modernas sobre las infraestructuras que posibilitan nuestro modelo de vida actual es creciente. La supresión o anulación de los servicios que aquéllas prestan podrían literalmente paralizar a una sociedad.
Los países avanzados llevan años desarrollando fórmulas para efectuar la protección efectiva de sus infraestructuras críticas. España no es una excepción, y ha emitido recientemente dos importantes documentos en este sentido.
• El Plan Nacional de Protección de las Infraestructuras Críticas, y
• El Acuerdo de Consejo de Ministros de fecha 2 de noviembre de 2007.
De entre las medidas impulsadas por esta normativa, destacan como iniciativas principales la confección del Catálogo Nacional de Infraestructuras y la creación del Centro Nacional de Protección de Infraestructuras Críticas.

There is a growing dependence of modern societies on the infrastructures that make our current life style possible. Restricting or canceling the services that they provide could literally paralyze a society.
For many years, the advanced countries have been developing formulas to effectively protect their critical infrastructures. Spain is no exception, and recently it has released two important documents in this respect.
• The National Critical Infrastructure Protection Plan, and
• The Council of Ministers Resolution dated 2 November 2007.
Of the measures supported by this regulation, the main initiatives are elaboration of the National Infrastructures Catalogue and creation of the National Critical Infrastructure Protection Center.

FERNANDO J. SÁNCHEZ GÓMEZ
es Comandante de la Guardia Civil. Diplomado de Estado Mayor por el Centro Superior de Estudios de la Defensa Nacional (Madrid).
Actualmente es Director del Centro Nacional de Protección de Infraestructuras Críticas de la Secretaría de Estado de Seguridad (Ministerio del Interior)

INTRODUCCIÓN

Nunca las infraestructuras han sido tan importantes y tan trascendentales para el normal funcionamiento de los servicios públicos esenciales y de los principales sistemas de producción como lo son ahora. Hoy en día, la dependencia de las sociedades modernas sobre las infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general es cada vez mayor.

La expansión del Estado del Bienestar en los países occidentales y la revolución que ha supuesto el desarrollo de las nuevas tecnologías desde los años ochenta ha ido desarrollando unas sociedades acostumbradas a un alto y cómodo nivel de vida, con múltiples e inmediatos servicios a su disposición, derivados de unos elevados índices de producción que descansan sobre unas sólidas infraestructuras. Una de las características más reseñables de nuestra sociedad actual, basada en las nuevas tecnologías, es que una aparentemente infinita serie de pequeños detalles debe funcionar correctamente y de forma coordinada para mantener los numerosos procesos que todos damos por hecho como "normales" para seguir con nuestra vida diaria.

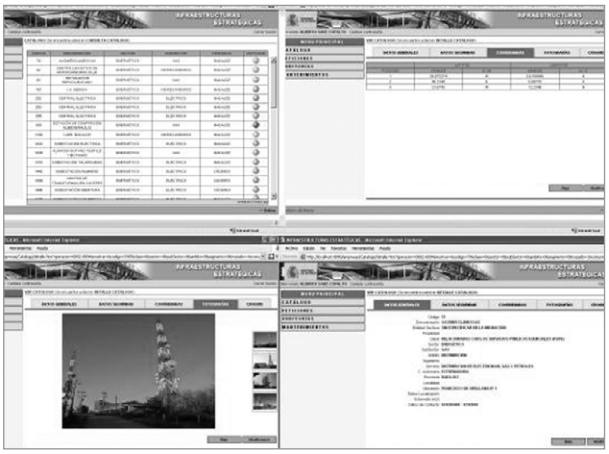
Pero estas infraestructuras, soporte en gran medida de la continuidad de la producción y de la mayoría de los servicios que necesita el ciudadano de la Europa del siglo XXI, fueron establecidas de acuerdo con las necesidades, los criterios y los riesgos de un panorama que ha cambiado por completo en menos de diez años.

Los criterios que guiaron su diseño, construcción y puesta en funcionamiento fueron la rentabilidad, la eficiencia, el mejor servicio a los clientes, el respeto al medio ambiente, y la seguridad encaminada a evitar accidentes o sabotajes, a disminuir los efectos de un posible desastre natural y, en el mejor de los casos, a dificultar atentados terroristas de baja intensidad.

Sin embargo, la fuerte ofensiva del terrorismo internacional a raíz de los atentados del 11 de septiembre, su insistencia en Europa Occidental principalmente con los atentados de Madrid y Londres, y el carácter masivo e indiscriminado de sus acciones terroristas, ha cambiado absolutamente el escenario de seguridad de occidente, configurando un panorama en el que determinados objetivos, por la mayor repercusión que su destrucción o alteración podrían producir sobre la vida, la salud o el bienestar de los ciudadanos o de los propios Estados, se convierten en baluartes de nuestra civilización y del propio Estado del Bienestar y, por tanto, requieren un tratamiento diametralmente opuesto del que venían recibiendo, especialmente en materia de seguridad.

CONCEPTO DE INFRAESTRUCTURA CRÍTICA

El reciente Acuerdo del Consejo de Ministros, de 2 de noviembre pasado, sobre Protección de Infraestructuras Críticas, ha supuesto un importante impulso a las iniciativas que, desde hace varios años, lleva desarrollando la Secretaría de Estado de Seguridad del Ministerio del Interior en una materia cuya trascendencia y complejidad no escapa a nadie.



Fichas Catálogo infraestructuras.

Numerosos países de nuestro entorno, incluida España, están trabajando intensamente sobre la optimización de la protección de sus infraestructuras críticas, en íntima relación con las empresas y organismos gestores de las mismas, sin cuya estrecha colaboración no podría llevarse a cabo un esfuerzo de esta índole. En este contexto, es preciso definir, para centrar adecuadamente el tema, qué es lo que se entiende como Infraestructura Crítica, tanto en el ámbito nacional como en el de la Unión Europea, donde nuestro país debe enmarcar las iniciativas que al respecto se lancen, independientemente del carácter confidencial que debe tener cualquier información sobre las infraestructuras estratégicas propias nacionales, y que tiene una difusión estrictamente interna.

Las **infraestructuras críticas**, así, son aquellas **instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los órganos del Estado**. Las infraestructuras críticas están presentes en numerosos sectores de la economía: actividades bancarias y financieras, transporte y distribución, energía, servicios, salud, abastecimiento de alimentos y agua potable, comunicaciones, administraciones públicas y órganos de gobierno, etc.

En los países desarrollados como el nuestro, las infraestructuras críticas nacionales están muy interconectadas y son sumamente interdependientes. A esta situación han contribuido la consolidación corporativa, la racionalización industrial, prácticas de eficiencia empresarial y la concentración de la población en las zonas urbanas. Estas infraestructuras críticas dependen cada vez más de tecnologías de la información como Internet, la radionavegación y la comunicación por satélite. Los problemas que pueden desencadenarse en cascada a través de estas infraestructuras interdependientes, tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves de los servicios esenciales.

Por otra parte, la seguridad integral de las infraestructuras de la mayoría de los sectores estratégicos (y, muy concretamente, de los relacionados con la energía, los transportes, las finanzas y los procesos industriales) no recae únicamente sobre la protección física de las instalaciones, sino que depende cada vez en mayor medida de los Sistemas de Información (principalmente, de los Sistemas SCADA, para la supervisión y control de los datos adquiridos), cuya seguridad no puede ser proporcionada mediante un despliegue físico, sino a través de una protección cibernética. Resulta así que cada vez es más complicado disociar la protección física de la protección contra las amenazas de carácter lógico, siendo inevitable enfocar el problema de la seguridad de nuestras infraestructuras desde una perspectiva integral.

INICIATIVAS PUESTAS EN MARCHA EN MATERIA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

El Consejo Europeo de junio de 2004 instó a la Comisión Europea a elaborar una estrategia global sobre protección de infraestructuras críticas. El 20 de octubre de 2004, la Comisión adoptó la **Comunicación sobre Protección de las Infraestructuras Críticas en la lucha contra el terrorismo**, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que afecten a las infraestructuras críticas (IC).

En las conclusiones del Consejo sobre prevención, preparación y respuesta a los ataques terroristas y en el Programa de solidaridad de la UE sobre las consecuencias de las amenazas y ataques terroristas, adoptado por el Consejo en diciembre de 2004, se respalda el propósito de la Comisión de lanzar un Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) y se aprueba la creación por la Comisión de una Red de información sobre alertas en infraestructuras críticas (CIWIN).

En noviembre de 2005, la Comisión aprobó el **Libro Verde sobre un programa europeo** para la protección de infraestructuras críticas (PEPIC), que expone las posibilidades de acción de la Comisión para la creación del programa PEPIC y la red CIWIN, y que fue oportunamente contestado por las autoridades españolas, colaborando a la mejora de la estrategia común a seguir. En diciembre de 2005, el Consejo de Justicia y Asuntos de Interior (JAI) instó a la Comisión a presentar una propuesta sobre el PEPIC, basada en un planteamiento global que diera preferencia a la lucha contra amenazas terroristas.

A principios de diciembre 2006 la Comisión presentó una Comunicación sobre el Programa Europeo de Protección de Infraestructuras Críticas y un proyecto de Directiva para la identificación y designación de infraestructuras críticas europeas (ICE) y evaluación de la necesidad de mejorar su protección, que está siendo objeto de discusión actualmente.

El propósito de la propuesta de Directiva, que actualmente está siendo objeto de discusión, es mejorar los niveles de protección de las infraestructuras críticas transfronterizas estableciendo un procedimiento de identificación y designación así como incentivar que cada infraestructura europea de carácter transfronterizo tenga un plan de seguridad y un oficial responsable de seguridad.

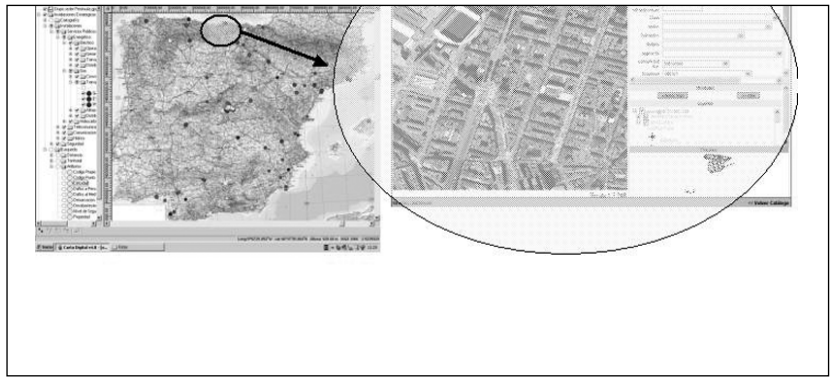
Estos pasos que se han venido dando en el ámbito de la UE han servido para alentar el desarrollo de la planificación y organización del sistema nacional de protección de nuestras infraestructuras críticas, adaptándose en lo posible a las disposiciones europeas.

En España, las medidas normativas puestas en marcha desde el

Ministerio del Interior y la Secretaría de Estado de Seguridad, son fundamentalmente dos, ambas de 2007, año en el que han culminado una serie de estudios y trabajos iniciados por las FCSE en años anteriores:

— Por un lado, el Plan Nacional de Protección de las Infraestructuras Críticas, aprobado por el Secretario de Estado de Seguridad, con fecha 7 de mayo de 2007, que:
  - Efectúa una definición sobre qué tipo de instalación se debe considerar Infraestructura Estratégica, y cuáles son los sectores afectados;
  - plantea el diseño de un Catálogo de Infraestructuras a nivel nacional, donde éstas aparezcan clasificadas en base a una serie de parámetros, tras la realización de un análisis de riesgos adecuado;
  - marca, en línea con el Plan Antiterrorista, varios niveles de seguridad (estableciendo, por cada uno de ellos, las medidas a adoptar por las FCSE y otras fuerzas (policiales y FAS, principalmente) para cada uno de los niveles de activación, en estrecha colaboración;
  - encarga a la Dirección General de la Policía y de la Guardia Civil la elaboración de un **Plan Estatal Conjunto de Protección de las Infraestructuras Críticas**, con especial consideración de las medidas de protección y respuesta frente a atentados terroristas y criminales (este Plan debe tener su desglose en los respectivos **Planes Territoriales y Sectoriales**), y
  - designa al Secretario de Estado de Seguridad como autoridad superior de dirección y control de todas las medidas previstas en el Plan.
— Y, por otra parte, el **Acuerdo de Consejo de Ministros de fecha 2 de noviembre de 2007**, mediante el cual:
  - Se designa a la Secretaría de Estado de Seguridad como organismo responsable de la dirección, coordinación y supervisión de la protección de las infraestructuras críticas nacionales;
  - se establece el desarrollo del Plan Nacional de Protección de las Infraestructuras Críticas;
  - se ordena la clasificación como SECRETO y la actualización del Catálogo Nacional de Infraestructuras Estratégicas, y
  - se crea el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

De entre todas estas medidas, destacan como iniciativas de mayor interés, la confección del Catálogo Nacional de Infraestructuras y la creación, en el seno de la Secretaría de Estado de Seguridad, del CNPIC. Ambas se desarrollan brevemente a continuación:



Sistema GIS Base de Datos.

CATÁLOGO NACIONAL DE INFRAESTRUCTURAS ESTRATÉGICAS

A mediados de 2004, las FCSE iniciaron los trabajos de planeamiento correspondientes a la elaboración de un Plan de Seguridad de Instalaciones Estratégicas. Este Plan, que pretendía integrar las medidas de seguridad de todas las infraestructuras sensibles de la nación y definir sus posibles incrementos ante distintas situaciones de amenaza, tenía una primera fase de definición y desarrollo de un Catálogo Nacional de Infraestructuras Estratégicas. Para el desarrollo de dicha fase se conformaron grupos de trabajo mixtos, por sectores, entre representantes de la Guarda Civil y del Cuerpo nacional de Policía, de un lado, y de las empresas afectadas, de otro.

Tras la integración de las bases de datos de ambos Cuerpos y la creación de un aplicativo de gestión por parte de la Secretaría de Estado de Seguridad, el Catálogo Nacional de Infraestructuras Estratégicas está, a día de hoy, listo para ser puesto en funcionamiento en el momento en que se disponga de los medios humanos y materiales que posibiliten su gestión.

El Catálogo Nacional de Infraestructuras se sustenta en una Base de Datos Geográfica sobre Mapa Digital, donde se hallan reflejadas de forma completa y sistemática las instalaciones de numerosas empresas y organismos identificadas a día de hoy, repartidas por todo el Territorio Nacional, independientemente de su demarcación policial. Ligado a la Base de Datos Geográfica se encuentra un software de explotación, que permite representar y consultar los datos atendiendo a su componente geográfica.

Este Catálogo es un documento vivo, en el cual de forma permanente se pueden ir actualizando datos y dar de alta y de baja las instalaciones que se determinen, con arreglo a los protocolos que se establezcan al efecto, Existen, en línea con la normativa europea, **12 sectores estratégicos** en los cuales se hallan incluidas todas las instalaciones del Catálogo.

De entre las funcionalidades del sistema, merece la pena resaltar:

— La posibilidad de efectuar la priorización de las infraestructuras, con arreglo a una serie de parámetros y el grado de afección sobre éstos. La conjunción de varios parámetros basados en técnicas de análisis de riesgos, permite sacar una conclusión valorada de la importancia de la instalación, que se ha denominado **criticidad**. Esta clasificación diferencia entre diferentes tipos de instalaciones con arreglo a su criticidad.
— Debido a su estructura, grandes posibilidades técnicas para la actualización permanente de la información de la Base, mediante su inclusión en una red o web interna de carácter restringido, a la cual podrán tener acceso en un futuro próximo las empresas y órganos gestores o propietarios de las infraestructuras recogidas, así como las FCSE y los organismos que se determinen en su momento.

CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (CNPIC)

El desarrollo e implementación de estrategias y políticas de protección de infraestructuras críticas es responsabilidad de los gobiernos de las naciones. En los países de nuestro entorno, la gestión de estas actividades es asignada a departamentos gubernamentales como el DHS norteamericano, la Secretaría General para la Defensa Nacional (SGDN) francesa, el CPNI del Reino Unido, el PSEPC canadiense o el NCC holandés.

En esta misma línea, la creación del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), es uno de los hitos más importantes puestos en marcha por el **Acuerdo de Consejo de Ministros del 2 de noviembre de 2007**. Este Centro tendrá como cometidos principales:

— La custodia, el mantenimiento y actualización del Plan de Seguridad de Infraestructuras Críticas y el Catálogo Nacional de Infraestructuras Es-

Central nuclear de Vandellós I.

tratégicas. La variación de los datos del catálogo será efectuada en base a las modificaciones que las empresas y organismos, así como las FCSE, aporten sobre las propias instalaciones, con la necesaria validación del CNPIC de las propuestas remitidas, según el protocolo que al efecto se defina.

— La recogida, análisis, integración y valoración de la información procedente de instituciones públicas, servicios policiales, sectores estratégicos, y de la cooperación internacional.
— La valoración de la amenaza y análisis de riesgos sobre las instalaciones estratégicas.
— El diseño y establecimiento de mecanismos de información, comunicación y alerta, que deberán asegurar la comunicación mutua y fluida entre todas las instituciones implicadas en la protección de objetivos estratégicos (públicas y privadas), estableciendo reuniones periódicas y diseñando un boletín de información interno, preferiblemente mediante una Intranet o página web restringida, sobre asuntos o incidentes relacionados con la seguridad de estos objetivos. Así mismo, dichos mecanismos deberán determinar también los procedimientos de comunicación de alertas o variación del nivel de seguridad.
— Soporte de Mando y Control en una Sala de Operaciones, cuya activación deberá estar prevista ante situaciones de activación del nivel que se determine del Plan de Protección de Infraestructuras Críticas.
— Materializar el Punto Nacional de Contacto, en el marco de la Protección de Infraestructuras Críticas de la Unión Europea (Programa Europeo de Protección de Infraestructuras Críticas –PEPIC- y red de información y alerta sobre infraestructuras críticas –CIWIN-), y con otros organismos similares de terceros países.
— Coordinar los trabajos y la participación en los diferentes grupos de trabajo y reuniones en el ámbito de la Comisión Europea.
— Supervisar el proceso de elaboración de planes de intervención en materia de infraestructuras críticas y participar en la realización de ejercicios y simulacros.
— Supervisar y coordinar los planes sectoriales y territoriales de prevención y protección que deban activarse en los diferentes supuestos de riesgo y niveles de seguridad que se establezcan, tanto por las Fuerzas y Cuerpos de Seguridad como por los propios responsables de las operadoras.

— Elaborar los correspondientes Protocolos de Colaboración, sobre infraestructuras predefinidas, con personal y organismos ajenos al Ministerio del Interior.
— Supervisar los proyectos y estudios de interés en la protección de infraestructuras críticas, y coordinar la participación en programas financieros y subvenciones procedentes de la Unión Europea.

CONCLUSIONES

Para luchar contra el terrorismo global que amenaza a nuestra sociedad, en el que todo y todos somos potenciales objetivos, ya no es suficiente con *policías, puertas blindadas y pistolas*, por utilizar el vocabulario *de la calle*. Este reto solo se superará contando con información **veraz, fiable y oportuna** en todo momento. Para ello, es necesario compartir esa información entre todos los agentes implicados y hacerlo en ambas direcciones y en ambos sentidos. En el sentido horizontal, debe compartirse información entre las propias empresas, entre los propios sectores, y también entre los servicios de información y fuerzas de seguridad; en sentido vertical, la información debe discurrir también entre los responsables de la seguridad pública a todos los niveles y los propietarios y gestores de las infraestructuras críticas.

La implantación de organismos como el CNPIC, que canalicen y aúnen los esfuerzos de las administraciones, por un lado, y del sector público, por otro, es fundamental hoy en día. Estos organismos deben poder coordinar las actividades de los agentes implicados en la protección de las Infraestructuras Críticas, tanto en el sector público como el privado, para la elaboración de planes generales de protección, así como de planes específicos de sector. Para la elaboración e implantación eficaz de dichos planes es necesario fomentar las relaciones entre el sector público y privado (PPPs: *Public-Private Partnerships*) y la cooperación internacional, estableciendo los mecanismos adecuados para el intercambio de información y conocimiento a todos los niveles.

Sobre esa piedra angular, de responsabilidad compartida, y donde cada uno de los actores de las administraciones públicas y la empresa privada tenga su acceso a la información que necesite conocer, es sobre la que se debe edificar un proyecto tan ambicioso como complejo, pero a la vez, tan necesario. ■