FACULTAD DE DERECHO
Universidad de Málaga

PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS: UN ANÁLISIS DE DERECHO COMPARADO

Trabajo de Fin de Grado presentado por Francisco Javier Galindo Sierra siendo tutor del mismo el/la Profesora María del Pilar Castro López

Vº Bº del Tutor: Estudiante:

Fdo: Fdo:

En Málaga, a 10, de junio, de 2016

FACULTAD DE DERECHO. UNIVERSIDAD DE MÁLAGA

TRABAJO DE FIN DE GRADO (CURSO ACADÉMICO 2015/2016)

TÍTULO: Protección de infraestructuras críticas: un análisis de derecho comparado

AUTOR: Francisco Javier Galindo Sierra

TUTOR ACADÉMICO: María del Pilar Castro López

RESUMEN: Gran parte de los suministros y servicios esenciales de los países son proporcionados por las infraestructuras críticas. El corte de suministro de una de ellas puede provocar que se produzca la caída en cadena de otros servicios, incluso en otros países. Es por ello que la protección de las infraestructuras críticas, dado su carácter interdependiente, complejo y del carácter privado de la gran mayoría, es de vital importancia para la seguridad nacional.

PALABRAS CLAVE: Infraestructuras críticas, seguridad, seguridad nacional, servicios esenciales, prevención, políticas de seguridad, amenazas, riesgos, protección.

ABSTRACT: The main part of countries supplies and essential services are provided by critical infrastructure. The supplies interruption of one of them can cause the systems breakdown in other countries. For this reason the critical infrastructure protection, for their interdependent, complex and the vast majority private character, is vitally important to national security.

KEYWORDS: Critical infrastructure, security, national security, essential services, prevention, security policies, threats, risks, protection.

ÍNDICE

Abreviaturas

CCN: Centro Criptológico Nacional.

CERT: Computer Emergency Response Team.

CNPIC: Centro Nacional de Protección de Infraestructuras Críticas.

IC: Infraestructuras Críticas.

ICE: Infraestructuras Críticas Europeas.

LOPSC: Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana.

LPIC: Ley 8/2011, de 28 de abril, por la que se establecen Medidas de Protección de Infraestructuras Críticas.

LSN: Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

OPAQ: Organización para la Prohibición de las Armas Químicas.

PEPIC: Programa Europeo de Protección de Infraestructuras Críticas.

PNPIC: Plan Nacional de Protección de Infraestructuras Críticas.

SPIC: Sistema de Protección de Infraestructuras Críticas.

TNP: Tratado de No Proliferación Nuclear.

1. INTRODUCCIÓN.

Una de las ventajas del carácter multidisciplinar de la Criminología es que ofrece la posibilidad de realizar estudios de muy distinta índole. En nuestro caso esa formación multidisciplinar del criminólogo nos ha permitido abordar un análisis de las infraestructuras críticas (en adelante, IC) y de la problemática que plantea su protección, cuyo estudio cabría encuadrar en al ámbito del Derecho Administrativo.

Hasta el momento, y pese al desarrollo legislativo de que han sido objeto en la última década en numerosos países, las infraestructuras críticas están pasando inadvertidas para los investigadores. En nuestro país la bibliografía existente al respecto es más bien escasa y la mayor parte de ella suele limitarse a describir a grandes rasgos la regulación sobre la materia. También se echan en falta estudios comparativos significativos entre los sistemas de protección de las IC de diferentes países.

En otro orden de cosas, la mayoría de la ciudadanía desconoce qué son las Infraestructuras Críticas y la esencialidad de su protección para el normal funcionamiento del Estado, circunstancia en la que, sin duda, influye el hecho de que apenas existan referencias a las mismas en los medios de comunicación, vía por la que la mayoría de las personas adquieren conocimiento de los asuntos.

Lo expuesto anteriormente justifica la elección del objeto de estudio del presente Trabajo de Fin de Grado que pretende analizar la situación actual de las infraestructuras críticas tanto a nivel nacional como internacional.

Para ello hemos realizado una revisión de la legislación española en materia de infraestructuras críticas (Ley 8/2011, de 28 de abril y Real Decreto 704/2011, de 20 de Mayo), que se enmarca en el Sistema de Seguridad Nacional (Ley 36/2015, de 28 de septiembre), prestando especial atención al cumplimiento de los estándares europeos en relación a las IC, establecidos por la la Directiva 114/2008/CE.

Con el acercamiento a las estrategias, planes de protección y normativa reguladora de las Infraestructuras Críticas otros países, concretamente Australia, Canadá, Estados Unidos, Reino Unido, Francia y Bélgica, hemos pretendido determinar los puntos comunes y las diferencias entre el sistema español y los sistemas de estos países.

Junto al análisis normativo, hemos acudido al uso de la técnica de revisión bibliográfica, perteneciente a la metodología cualitativa, para conocer el estado actual de las investigaciones sobre las infraestructuras críticas.

La primera parte del Trabajo de Fin de Grado se centra en el Sistema de Seguridad Nacional y las amenazas y riesgos a los que está expuesto en el mundo actual, en general, y en España, en particular. La segunda parte se ocupa ya específicamente del Sistema de Protección de Infraestructuras Críticas español y la tercera de los sistemas de protección de las infraestructuras críticas de los países citados anteriormente.

Gracias a la investigación realizada, hemos podido constatar, como ya se ha advertido al comienzo, que la mayor parte de la bibliografía sobre el tema objeto de estudio es de carácter meramente descriptivo del marco normativo de las IC. Si bien somos conscientes de las dificultades que entrañan otro tipo de enfoques, creemos que el presente Trabajo de Fin de Grado podría proporcionar una base sobre la cual se puedan realizar otro tipo de investigaciones empíricas de diferente metodología, para la comprobación de los resultados logrados en materia de prevención, reacción e intervención y colaborar en la mejora de los sistemas en los diferentes niveles

(legislativos, operativo, cooperativo), además de contribuir al fomento de la cultura de la seguridad.

2. SEGURIDAD NACIONAL: CONCEPTO, AMENAZAS, NECESIDAD DE UN SISTEMA DE SEGURIDAD NACIONAL.

2.1 Delimitación conceptual.

Para comenzar, vamos a realizar una aproximación conceptual al término "seguridad" desde el punto de vista doctrinal, jurisprudencial y legal, para centrarnos posteriormente en el que es objeto de estudio: el concepto de seguridad nacional.

Muchas son las definiciones de seguridad que pueden encontrarse en la literatura especializada, así Blanco Navarro, De la Corte Ibáñez y Jaime Jiménez se refieren al término seguridad en un sentido amplio, identificándola con:

> "Una aspiración que conecta con las motivaciones humanas básicas de perseverar en la propia existencia, obtener placer y bienestar y, asimismo, evitar el dolor, o cualquier otra forma de daño, junto con las emociones que pueden anticiparlos y acompañarlos, como la ansiedad, el miedo o el terror. Deseamos encontrarnos y sentirnos libres de todo daño o amenaza, tanto en el presente como en el futuro, y llamamos seguridad a las condiciones que posibilitan y garantizan el cumplimiento de ese deseo"[1].

La Exposición de Motivos de la Ley 36/2015, de 28 de Septiembre, de Seguridad Nacional (en adelante, LSN) destaca la importancia de la seguridad en la actualidad afirmando que la misma "constituye la base sobre la cual la sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones".

Por su parte, el Tribunal Constitucional en su Sentencia 33/1982 define la seguridad pública como "la actividad dirigida a la protección de personas y bienes (seguridad en sentido estricto) y al mantenimiento de la tranquilidad u orden ciudadano, que son finalidades inseparables y mutuamente condicionadas", definición que se reitera en las SSTC 117/1984, 123/1984, 59/1985 y 104/1989, puntualizando en esta última que la actividad de seguridad pública engloba "un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido". Ello evidencia que para el TC el concepto de seguridad pública es un concepto o categoría genérica de contenido múltiple y heterogéneo.

A nivel legal, la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana (en adelante, LOPSC) destaca en su Preámbulo la importancia de la seguridad ciudadana, a la que se califica como "uno de los elementos esenciales del Estado de Derecho", en cuanto garantía del libre ejercicio por la ciudadanía de los derechos y libertades reconocidos y amparados por las constituciones democráticas. Ahora bien, el Preámbulo de la citada Ley no diferencia el concepto de seguridad ciudadana, objeto de la misma, de otros afines como el de seguridad pública, antes al contrario, se afirma que "la doctrina y la jurisprudencia han venido interpretando, con matices, estos dos conceptos como sinónimos, entendiendo por tales la actividad

[1] BLANCO NAVARRO, J.M., DE LA CORTE IBÁÑEZ, L. y JAIME JIMENEZ, O.; "Aproximación a la seguridad nacional" En DE LA CORTE IBÁÑEZ, L. y BLANCO NAVARRO, J.M. (Coords), *Seguridad nacional, amenazas y respuestas*, Lid, Madrid, 2014, pág 23.

dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad ciudadana", que es, como acabamos de ver, la definición de seguridad pública postulada por el TC.

Por último, el concepto de seguridad nacional se configura legalmente, concretamente en la citada LSN, como concepto general omnicomprensivo del de seguridad pública y que, como acabamos de indicar, legalmente se asimila al de seguridad ciudadana. La LSN define la seguridad nacional como "acción del Estado dirigida a proteger la libertad y bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos" (artículo 3), cuyos componentes fundamentales serían "la Defensa Nacional, la Seguridad Pública y la Acción Exterior, que se regulan por su normativa específica" (artículo 9).

2.2 Las amenazas a la seguridad nacional: contexto actual.

Las amenazas que pueden poner en riesgo los intereses vitales y estratégicos de España se han visto incrementados en los últimos años. Según la "Estrategia de Seguridad Nacional de 2013"[2] los riesgos y amenazas principales para la seguridad nacional serían los conflictos armados, el terrorismo, las ciberamenazas, el crimen organizado, la inestabilidad económica y financiera, la vulnerabilidad energética, la proliferación de armas de destrucción masiva, los flujos migratorios irregulares, espionaje, emergencias y catástrofes, vulnerabilidad en el espacio marítimo y por último la vulnerabilidad de las infraestructuras críticas y servicios esenciales. El dinamismo del entorno tanto en el ámbito nacional como internacional y el aumento y diversificación de la tipología de las amenazas, han hecho necesaria la mejora de nuestros sistemas de protección, así como su adecuación a la normativa europea. El conflicto territorial ucranio-ruso y la guerra civil de Siria, en los que se ha requerido en numerosas ocasiones la intervención de la Organización del Tratado del Atlántico Norte (OTAN)[3], son claros ejemplos de la situación de inestabilidad que existe en este momento a nivel internacional.

Aunque el Estado español, por su pertenencia a la ONU, OTAN y a la UE[4], así como en cumplimiento de los Convenios Internacionales que tiene suscritos puede llegar a participar en conflictos exteriores a gran escala, hasta el momento las intervenciones realizadas por nuestro país se limitan a la vigilancia, control y adiestramiento de tropas extranjeras.

A nivel interno España ha sufrido durante más de 50 años el terrorismo de ETA[5], cuyos atentados han causado 829 fallecidos, según el Ministerio del Interior, cifra que

---

[2] CONSEJO DE MINISTROS. Estrategia de Seguridad Nacional, un proyecto compartido. Disponible en: «http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf»

[3] Otros aliados como EE.UU, Francia, Bélgica y Reino Unido ya participan en la guerra civil de Siria, bombardeando posiciones del DAESH (acrónimo de "Estado Islámico de Irak y el Levante" en árabe)

[4] Sobre las implicaciones que para la estrategia de seguridad nacional supone nuestra integración en la UE puede verse GUINEA, M., "La estrategia de seguridad nacional 2013: Una evaluación desde la perspectiva de la pertenencia a la Unión Europea", *UNISCI Discussion Papers*. May. 2014, núm. 35, págs. 37 y ss.

[5] Esta banda armada pretendía mediante el uso de la violencia, lograr la independencia de Euskal Herria (País Vasco) y formar un país cuyo territorio se situaría donde actualmente se encuentra el País Vasco y territorios franceses lindantes.

la Asociación de Víctimas del Terrorismo (AVT) eleva a 858. En los últimos tiempos hemos asistido a la expansión de una nueva amenaza terrorista, el terrorismo yihadista. El 11 de Septiembre de 2001 se producía en Estados Unidos el ataque de mayor impacto hasta la fecha en occidente, con el secuestro de cuatro aviones por el grupo terrorista AL-QAEDA[6], que se saldó con 3019 muertos y más de 6000 heridos. El terrorismo yihadista también ha golpeado a nuestro país, concretamente el 11 de Marzo de 2004 tuvo lugar el ataque terrorista de Al-QAEDA en cuatro trenes de cercanías en Madrid que ocasionó 193 víctimas mortales, afortunadamente nuestro país no ha vuelto a sufrir ningún ataque terrorista de corte yihadista. En los últimos años, ha cobrado especial relevancia el terrorismo del autodenominado "Estado Islámico", conocido en el contexto internacional como "DAESH". Este grupo terrorista ha atentado en países aliados como son Francia con los atentados del 13 de noviembre de 2015 y Bélgica el 22 de marzo de 2016. Hay que destacar que en numerosos documentos y vídeos que el DAESH publica, amenazan con atentar en nuestro país, por tanto España está dentro de sus objetivos. En el último año, en España se ha producido la detención de 75 personas en 36 operaciones contra el terrorismo yihadista.

El imparable desarrollo de las tecnologías de la información y la comunicación y las nuevas oportunidades para cometer delitos mediante las mismas, representan una nueva amenaza para la Seguridad Nacional. Internet es un lugar accesible, fácil de usar y eficaz, del que cada vez dependemos en mayor medida para llevar a cabo un sinfín de actuaciones de nuestra vida cotidiana. Estas características hacen precisamente de la red, un lugar propicio para que para que los delincuentes salgan indemnes dadas las dificultades para rastrearlos a través de la red y localizarlos. Las principales modalidades de ataques a través del ciberespacio son las conocidas como: El ciberterrorismo, el ciberdelito, el ciberespionaje y el hacktivismo. Algunos ejemplos de delitos cometidos a través del ciberespacio son la captación y reclutamiento para una organización terrorista y la inutilización de medios informáticos de las instituciones públicas, el robo de datos personales mediante phising y la intrusión de troyanos en los sistemas, que representan todo un reto para las Fuerzas y Cuerpos de Seguridad.

"El crimen organizado se caracteriza por su naturaleza transnacional, opacidad, flexibilidad, capacidad de adaptación y de recuperación, así como su movilidad"[7]. Estas bandas se caracterizan por la comisión de diferentes tipologías de delitos como pueden ser el blanqueo de capitales, la piratería, el tráfico de drogas, armas, seres humanos y órganos, robos y fraudes entre otros. En España en particular, tiene especial incidencia el tráfico de drogas ya que nuestra situación geográfica, nos sitúa como ruta de acceso al resto de Europa.

Las nuevas tecnologías han supuesto también la creación de una nueva metodología de espionaje[8], que se suma a los métodos tradicionales y que genera una gran

---

[6] Como es sabido, los aviones fueron estrellados contra las Torres Gemelas, el Pentágono y un tercero, cuyo objetivo era el Capitolio en Washington, en campo abierto.

[7] CONSEJO DE MINISTROS. Estrategia de Seguridad Nacional, un proyecto compartido [pdf]. Disponible en: «http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf»

[8] NAVARRO BONILLA, D., "Espionaje" En DE LA CORTE IBÁÑEZ, L. y BLANCO NAVARRO, J.M. (Coords), *Seguridad nacional, amenazas y respuestas*, op. cit., pág. 222. define el espionaje como "toda acción perpetrada conscientemente para penetrar en un espacio informacional protegido o descuidado a fin de conseguir un incremento de conocimiento por medios encubiertos, insospechados o desconocidos por su legítimo productor o propietario. El espionaje busca de manera prioritaria la obtención de información no pública, protegida bajo diferentes niveles de clasificación y de accesibilidad

vulnerabilidad de los archivos confidenciales almacenados en los dispositivos electrónicos y en la web. De ahí que sea preciso extremar la protección de los sistemas de almacenamiento españoles, frente a cualquier agresión externa que persiga la extracción de información. Que un grupo terrorista o terceros países consigan información sobre los movimientos de nuestras tropas en el extranjero o de archivos de la otan, puede poner en riesgo las vidas de miles de soldados y sus misiones y, por ende, la seguridad nacional de España.

La inestabilidad económica y financiera de la última década ha supuesto un agravamiento de las amenazas contra la seguridad nacional, debido a la falta de recursos públicos para hacerles frente y a "la conflictividad política y social que genera"[9]. En situaciones de crisis económicas proliferan los conflictos exteriores, las nuevas formas de delincuencia y, en definitiva, la vulnerabilidad de los países que se encuentran en esa situación.

La mayoría de los conflictos exteriores tienen como trasfondo la voluntad de controlar recursos energéticos escasos como los yacimientos de petróleo y de gas natural. España por su localización carece de estos recursos, dependiendo del exterior para el abastecimiento necesario. Es por ello que España tiene que garantizarse el suministro de energía para conseguir el normal funcionamiento del país.

Otra cuestión que genera gran preocupación es la proliferación de armas de destrucción masiva, entre las que se incluyen armas nucleares, químicas y biológicas. En los últimos tiempos, estados problemáticos y grupos terroristas han intentado hacerse con este tipo de tecnología, que si se llegara a materializar, supondría un gravísimo riesgo para toda la comunidad internacional.

Las principales potencias han suscrito el Tratado de No Proliferación Nuclear (En adelante TNP)[10] al que pretenden que se adhieran el máximo número de países, mediante la imposición de sanciones de tipo económico a los que rechazan hacerlo. En la actualidad, India, Pakistán, Israel y Corea del Norte continúan sin adherirse al TNP, circunstancia especialmente preocupante en el caso de Corea del Norte, ya que en el pasado año, este país ha amenazado en numerosas ocasiones con usar sus armas nucleares, habiendo hecho público haber realizado pruebas con la bomba H[11], no confirmadas por la comunidad internacional.

Por su parte, el objetivo de la Organización para la prohibición de las Armas Químicas (OPAQ)[12] es, como su propio nombre indica, la erradicación de este tipo de armas altamente peligrosas, ya que pueden causar daño por el mero contacto con la sustancia, ya sea mediante inhalación, contacto con la piel o la combinación de ambas. Además, al tratarse de gases no es posible saber cuando se es atacado con armas

---

muy limitada cuyo contenido es sensible y de alto valor para el conocimiento de capacidades e intenciones de un adversario, rival, enemigo o incluso aliado".

[9] CONSEJO DE MINISTROS. Estrategia de Seguridad Nacional, un proyecto compartido [pdf]. Disponible en: «http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf»

[10] Estados Unidos, Rusia, República Popular de China, Gran Bretaña y Francia son los únicos que pueden poseer armas nucleares, por haber realizado ensayos nucleares antes de 1967)

[11] La bomba H también conocida como bomba de hidrógeno, bomba de fusión o bomba termonuclear es más potente que la bomba nuclear usada hasta ahora por fisión nuclear.

[12] Organización de de la que forman parte todos los países excepto Israel, Birmania, Angola, Egipto, Corea del Norte y Sudán del Sur.

químicas[13], disminuyendo la capacidad de reacción y aumentando la mortalidad. Los ataques no reivindicados en la Guerra Civil de Siria con gas mostaza y las sospechas de que el DAESH posee este tipo de armas[14] dejan bien patente la amenaza que este tipo de armas representan en la actualidad. Igualmente el 3 de marzo del presente año, Marruecos confirmó que la célula terrorista yihadista desmantelada en Febrero poseía sustancias biológicas/tóxicas para realizar un ataque biológico en el país[15].

Dada su ubicación al sur de Europa, con Ceuta y Melilla en el continente africano y la cercanía de la península al mismo, España constituye una de las principales rutas migratorias irregulares. Los inmigrantes huyen de conflictos bélicos, de regímenes autoritarios, de la pobreza y la desigualdad a países más seguros y con más oportunidades para desarrollarse. Si no se da una respuesta al fenómeno de la inmigración, éste puede convertirse, como de hecho ocurre ya, en un campo abonado para delitos como la trata de personas, tráfico de drogas y tráfico de órganos, entre otros. A ello ha de unirse otro problema de recientemente aparición que es la radicalización de inmigrantes por parte de grupos islamistas: su difícil situación económica y social hace de los inmigrantes personas especialmente vulnerables a la propaganda yihadista y, consecuentemente, presas fáciles del reclutamiento por estos grupos terroristas.

La seguridad en el mar constituye otro importante foco de preocupación para la seguridad nacional. El espacio marítimo se caracteriza por ser una zona vulnerable debido tanto a las dificultades que conlleva controlar tanto espacio y como al hecho de estar menos regulado por el Derecho. El mar es una importante fuente de materias primas, alimenticia, de recursos energéticos y patrimonio, además de ser un medio de transporte esencial, con numerosas rutas comerciales. entre los riesgos para la seguridad nacional relacionados con el medio marítimo cabe destacar su utilización por organizaciones criminales para realizar actividades ilícitas, como el tráfico de drogas desde marruecos a las costas gaditanas y, más concretamente, a la Línea de la Concepción y Algeciras, la inmigración ilegal y la piratería. La situación de la inmigración irregular se ha agravado con la crisis de los refugiados sirios, que afecta a nuestro país, en la medida en que la travesía se realiza por el mediterráneo, y, en general, a toda la unión europea. En 2008 fue asaltado el buque español *Playa de Bakio* y en 2009 el *Alakrana* en las aguas de Somalia, lugar crítico junto a Guinea donde mayor incidencia está teniendo la piratería. Además de un importante caladero pesquero se trata de una importante ruta comercial entre Europa, el sureste asiático y el Golfo Pérsico donde hay, al menos, 30 pesqueros españoles en actividad, de ahí la implicación española en el mantenimiento de la seguridad en la zona.

La seguridad nacional puede igualmente verse amenazada por catástrofes esto es, situaciones cuya causa puede ser natural o provocada por el hombre, que originan importantes daños humanos y materiales y que pueden suponer un grave trastorno para el normal funcionamiento de un país. en nuestro país existen numerosos lugares

[13] Parece que la expresión armas de destrucción masiva fue utilizada por primera vez por el Arzobispo anglicano de Canterbury y Primado de Inglaterra, C. Gordon, en unas declaraciones al periódico *The Times* en diciembre de 1937, refiriéndose al bombardeo de Gernika por la aviación nazi durante la Guerra Civil española y al inicio de la Segunda Guerra Chino-Japonesa.

[14] Información publicada en el Diario ABC, edición digital de 9 de marzo de 2016, disponible en: «http://www.abc.es/internacional/abci-eeuu-bombardea-naves-arsenal-quimico-mosul-gracias-ayuda-cientifico-daesh-201603091706_noticia.html»

[15] Información publicada por la agencia de noticias Europa Press el 4 de marzo de 2016, disponible en: «http://www.europapress.es/internacional/noticia-marruecos-dice-varios-terroristas-detenidos-preparaban-ataque-biologico-20160304033253.html»

susceptibles de sufrir una catástrofe natural: seísmos al sur de la península, dada la presencia de la falla entre la placa africana y euroasiática, erupciones volcánicas en las islas canarias, grandes incendios o inundaciones provocadas por la gota fría en la zona este del país; el cambio climático ha venido a aumentar el riesgo de fenómenos naturales extremos y con ello la necesidad de establecer unos mecanismos capaces de reaccionar suficientemente rápido para evitar el máximo de daños posibles. Finalmente, epidemias como la gripe aviar, el ébola y el zika forman parte del conjunto de vulnerabilidades que pueden amenazar la seguridad de nuestro país y requieren asimismo una decidida acción del Estado.

2.3. Necesidad de un sistema de seguridad nacional.

La reciente Ley 36/2015, de Seguridad Nacional, tiene como principal objetivo crear un sistema de seguridad nacional homologable con los países de nuestro entorno, principalmente con los de la Unión Europea, que, siguiendo las directrices de esta última en la materia, permita proporcionar una respuesta completa frente a cualquier tipo de amenaza contra la seguridad nacional de manera efectiva e integral.

Como hemos tenido ocasión de poner de manifiesto, globalización y aceleración son las principales características de nuestra sociedad actual. Vivimos en un mundo globalizado, en el que los riesgos y amenazas a la seguridad son también globales, por lo que es necesario poder afrontarlos en estrecha colaboración con los países de nuestro entorno para así garantizar la seguridad con éxito. Vivimos igualmente en una sociedad acelerada, en la que se producen muchos cambios en muy poco tiempo, lo que dificulta que los poderes públicos puedan dar una respuesta eficaz a los problemas que surgen en el marco de la seguridad.

En el ámbito de la seguridad nacional resulta esencial contar con una normativa que, de acuerdo con el principio de optimización, establezca mecanismos y procedimientos que proporcionen a los poderes públicos la capacidad de responder con eficacia a todo tipo de vulnerabilidades tanto presentes como futuras, evitando así caer en la improvisación, que supondría una respuesta ineficaz e, incluso, incorrecta, ya sea por exceso o por defecto en el uso de los correspondientes instrumentos. Es más, no sólo ha de desterrarse la improvisación, sino que ha de fomentarse la anticipación y, consiguiente, prevención, para lo que es necesario la mejora de los sistemas de información, pues la obtención de información y su posterior análisis permite tener una visión aproximada de posibles riesgos y amenazas a la seguridad nacional y prevenir, cuando sea posible, su materialización.

Sólo sobre la base de unos mecanismos y procedimientos legalmente preestablecidos, que permitan un mejor análisis de cada situación, podrá darse una respuesta óptima a las amenazas a la seguridad nacional; en este sentido, la promulgación de la LSN debe valorarse positivamente, en cuanto supone el establecimiento por primera vez en nuestro país de un marco regulador en materia de seguridad nacional.

La LSN hace especial hincapié en la necesidad de mejorar la cooperación y coordinación entre las diferentes Administraciones Públicas implicadas en la seguridad nacional, para lo que deben armonizarse los objetivos, los recursos y las políticas en materia de seguridad, sin olvidar la participación ciudadana y la colaboración privada.

Por otro lado, se incide también en la necesidad de que el Estado español, en cumplimiento de sus compromisos internacionales, contribuya junto a sus socios y aliados al mantenimiento y garantía de la seguridad internacional mediante el

intercambio de información, tecnología, técnicas e instrumentos como es el caso de la Oficina Europea de Policía (EUROPOL)[16] o la Organización Internacional de Policía Criminal (INTERPOL)[17]. Concretamente, en el marco de la UE se ha impulsado la armonización de los procedimientos y protocolos de actuación de los diferentes Estados miembros, de manera que resulten homologables.

Ahora bien, siendo importante, la regulación normativa no es suficiente para garantizar la seguridad nacional, resultando fundamental dotar a los poderes públicos de recursos humanos y materiales adecuados para ello, extremo que no obvia la Ley de Seguridad Nacional, que dedica su Título IV (artículos 27 a 29) a regular la contribución de recursos a la seguridad nacional, si bien remite a una futura ley el desarrollo de esta cuestión (Disposición final tercera)[18].

3. INFRAESTRUCTURAS CRÍTICAS.

3.1 Concepto.

La garantía de la seguridad nacional requiere la protección de una serie de infraestructuras que resultan fundamentales para el mantenimiento de servicios esenciales de la comunidad, cuya interrupción tendría graves consecuencias para territorios concretos o para el país en general. Son las llamadas Infraestructuras Críticas (en adelante, IC).

La Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[19], define las infraestructuras críticas como: "el elemento, sistema o parte de éste situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones" (artículo 2.a)[20].

Dentro de la categoría genérica de infraestructuras críticas la Directiva singulariza las que denomina infraestructuras críticas europeas (en adelante ICE), considerando como tales a "la infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros. La magnitud de la incidencia se valorará en función de criterios horizontales, como los efectos de las dependencias intersectoriales en otros tipos de infraestructuras" (artículo 2.b).

La OTAN también ofrece una definición de infraestructuras críticas en su documento *Critical Infrastructure Protection against Terrorist Attacks*, publicado en noviembre de

---

[16] EUROPOL es un órgano europeo que se encarga de coordinar las diferentes policías de los países pertenecientes a la misma para luchar contra la delincuencia dentro de Europa.

[17] INTERPOL es la mayor organización policial del mundo a la que pertenecen 190 países entre los que se incluye España.

[18] Disposición final tercera. Mandato legislativo.

"El Gobierno, en el plazo de un año desde la entrada en vigor de esta ley, deberá remitir al Congreso de los Diputados un proyecto de ley reguladora de la preparación y disposición de la contribución de recursos a la Seguridad Nacional".

[19] Diario Oficial de la Unión Europea, nº L 345, de 23 de diciembre de 2008, pp 75-82.

[20] Definición que hacen suya CORREA HENAO G.J. y YUSTA LOYO J.M., "Seguridad Energética y Protección de Infraestructuras Críticas", *Lampsakos*. Jul-dic. 2013, núm. 10, pág 94.

2014 como aquellas instalaciones, servicios y sistemas de información que son tan vitales para las naciones que su incapacidad o destrucción tendría un impacto debilitador en la seguridad nacional, la economía nacional, la salud pública y la seguridad y las funciones efectivas de un gobierno[21].

En nuestro país, la Ley 8/2011, de 28 de abril, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas (en adelante, LPIC), las define como "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" (artículo 2.d).

Como podemos comprobar, todas las definiciones aportan puntos de vista similares, haciendo referencia al carácter esencial de los servicios proporcionados por las infraestructuras críticas y las graves consecuencias que supondrían la interrupción del funcionamiento de las mismas para los países. Como comprobaremos a continuación, está justificada la importancia dada a las infraestructuras críticas por las leyes y los autores.

En las sociedades occidentales avanzadas la mayoría de las actividades humanas dependen del suministro eléctrico y de agua, de las telecomunicaciones y del transporte. Una interrupción de estos servicios, ya sea por causas naturales (una catástrofe natural que afecte al suministro eléctrico) o provocada por el hombre (un ataque terrorista a una central nuclear) puede tener graves consecuencias. El problema se agrava cuando una infraestructura es dependiente de otra, con lo que la caída de una supondría la paralización de los servicios de ambas, por lo que la protección de las mismas adquiere mayor importancia.

3.2. Marco normativo.

La LPIC es la primera Ley en regular con carácter general e integral las infraestructuras críticas en nuestro país. Anteriormente la protección de las mismas no se materializaba en una única Ley, sino que se encontraba dispersa en diversas leyes como la Ley 16/1987, de 30 de julio, de Ordenación de los Transportes Terrestres; la Ley 21/2003, de 7 de julio, de Seguridad Aérea o la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, ya derogada por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

A raíz de los atentados de Madrid en 2004, en el Consejo Europeo de junio de ese mismo año se constató la necesidad de establecer estrategias para proteger las infraestructuras críticas de forma global, dando lugar a una Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, donde se realizan una serie de propuestas para mejorar la prevención, preparación y respuesta de la UE frente a atentados terroristas[22]. En diciembre de 2004 se puso en marcha la *Critical Infraestructures Warning*

[21] CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM. Critical Infrastructure Protection against Terrorist Attacks [pdf]: "Critical Infrastucture are those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functions of a government". Disponible en: http://www.coedat.nato.int/publication/course_reports/12-CIP.pdf

[22] Comunicación de la Comisión al Consejo y al Parlamento Europeo del 20 de octubre 2010 - Protección de las infraestructuras críticas en la lucha contra el terrorismo [COM (2004) 702 final - no publicada en el Diario Oficial], disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al33259.

Information Network (CIWIN), que es una red de información sobre alertas en infraestructuras críticas y se aprobó por el Consejo el Programa Europeo de Protección de Infraestructuras Críticas (en adelante, PEPIC). Finalmente en el año 2008 se aprobó la antes citada Directiva 2008/114/CE del Consejo, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, que obligaba a los Estados miembros de la UE a adoptar una serie de medidas para la protección de las IC, a fin de que todos ellos cuenten con leyes homologables en la materia.

La LPIC se adopta en España en transposición de dicha Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008[23]. En consonancia con lo exigido por la Comisión Europea la Ley establece las medidas y los procedimientos de protección de las IC, regula los instrumentos, los órganos que se integran en el Sistema de Protección de Infraestructuras Críticas (en adelante SPIC) y sus competencias de los mismos; concretamente se prevé la adopción de planes de seguridad del operador, el nombramiento de responsables de enlace para la seguridad, el desarrollo de métodos comunes de identificación y clasificación de los riesgos y amenazas, así como la designación de los puntos de contacto para la Protección de las Infraestructuras Críticas Europeas (en adelante PICE).

La LPIC ha sido desarrollada por el Real Decreto 704/2011, de 20 de Mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.

En cuanto al objetivo y valoración de esta regulación hacemos nuestras las palabras de Mª José Caro, para quien:

> "El fin primordial de la Ley y del reglamento es el establecimiento de una serie de medidas en materia de protección de infraestructuras críticas que proporcionen un soporte adecuado sobre el que se asiente una eficaz coordinación de las administraciones públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad global. Estos servicios se asientan en 12 sectores estratégicos, subdivididos a su vez en subsectores, ámbitos y segmentos: Administración, Alimentación, Energía, Espacio, Sistema Financiero y Tributario (por ejemplo, banca, valores e inversiones), Agua (embalses, almacenamiento, tratamiento y redes), Industria Nuclear, Industria Química, Instalaciones de Investigación, Salud, Tecnologías de la Información y las Comunicaciones y Transporte (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico)"[24].

Especial relevancia están adquiriendo los aspectos relacionados con la ciberseguridad. El avance en las tecnologías de la información y la comunicación y la dependencia de ellas, hacen de la red un caldo de cultivo de nuevas y muy variadas amenazas a la seguridad nacional y las infraestructuras críticas, como lo corroboran los siguientes datos:

---

[23] Aunque con retraso en cuanto al plazo de transposición, pues la Directiva 2008/114/CE establecía como fecha límite el 12 de enero de 2011 y la LPIC no vio la luz hasta el 29 de abril de ese año.

[24] CARO BEJARANO, M.J., La protección de las infraestructuras críticas [PDF]. Disponible en: «http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf»

- Según el Centro Criptológico Nacional, en junio de 2010 las autoridades de numerosos países se hacen eco de la existencia de un virus informático tipo gusano Stuxnet que se había propagado y uno de sus objetivos pudo haber sido una central nuclear de Irán[25].
- En abril de 2016 se descubrió un *malware* que afectaba a la central nuclear de Gundremmingen en Baviera, Alemania. Estos ataques son cada vez más comunes y un fallo en los sistemas de seguridad de los mismos podría ser catastrófico[26].
- Francisco Martínez, Secretario de Estado de Seguridad destacó que "durante 2015, el CNPIC, a través del Centro de Respuesta a Incidentes de Seguridad TIC de Seguridad e Industria (CERTSI), resolvió alrededor de 50.000 incidentes de ciberseguridad, de los que, 134 estaban dirigidos contra infraestructuras críticas. Además, se prevé que a lo largo de 2016 los ciberataques asciendan a 100.000, de los cuales, 300 serían contra infraestructuras críticas"[27].

3.3 Sistema de protección de infraestructuras críticas.

De acuerdo con lo dispuesto en el Título II de la LPIC y en el Real Decreto 704/2011, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, el Sistema de Protección de Infraestructuras Críticas "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" (artículo 5 de la LPIC). Estas instituciones, órganos y empresas son los agentes que componen el sistema: la Secretaría de Estado de Seguridad del Ministerio del Interior; el Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, CNPIC); los Ministerios y organismos integrados en el Sistema; las Comunidades Autónomas, las Ciudades Autónomas y las Delegaciones de Gobierno de las mismas; las Corporaciones Locales; la Comisión Nacional para la protección de las Infraestructuras Críticas; el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas y los operadores críticos que pueden ser tanto del sector público como privado.

3.3.1 Agentes.

Los agentes que participan en el sistema de protección realizan las funciones que se detallan a continuación.

A. La Secretaría de Estado de Seguridad del Ministerio del Interior es el órgano que encabeza el Sistema de Protección siendo el órgano superior responsable del mismo. Este órgano es el encargado de diseñar además de dirigir la Estrategia Nacional de Protección de Infraestructuras Críticas, aprobar el Plan Nacional de Protección de las Infraestructuras Críticas, los Planes de Seguridad de los Operadores, los Planes de Protección Específicos, los Planes de Apoyo Operativo, aprobar la declaración de una zona como crítica. Por otro lado mediante el análisis de los mecanismos de prevención y de respuesta, en los diferentes ámbitos de responsabilidad. Este órgano es el encargado de dictar las

[25] Información publicada en la web del Centro Criptológico Nacional el día 27 de septiembre de 2010, disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/1222-el-gusano-stuxnet-que-afecta-a-sistemas-scada-causa-revuelo-internacional.html

[26] Información publicada en el diario El País edición digital del día 27 de abril de 2016, disponible en: http://internacional.elpais.com/internacional/2016/04/27/actualidad/1461751859_118617.html

[27] Información publicada en la web del Ministerio del Interior el día 8 de marzo de 2016, disponible en: http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/5721143

instrucciones para el personal y los operadores de las IC, también se encarga de la supervisión, la coordinación y la colaboración con los demás órganos que forman parte del Plan. En las situaciones de crisis, este órgano puede adquirir más funciones que se acordarán por la Comisión Delegada del Gobierno.

B. El CNPIC depende de la Secretaría de Estado de Seguridad del Ministerio del Interior. Este órgano es el que materializa las actuaciones llevadas a cabo por el Secretario de Estado de Seguridad. Tiene como función principal el impulso y la coordinación de los mecanismos que tienen que llevar a cabo los agentes del sistema como son: los Planes Estratégicos Sectoriales (Son responsabilidad del Estado), los Planes de Seguridad de los Operadores, los Planes de Protección Específicos (Son responsabilidad de los titulares de las infraestructuras) y los Planes de Apoyo Operativo (Son responsabilidad de las Fuerzas y Cuerpos de Seguridad)[28].

   El CNPIC es asimismo el órgano encargado del mantenimiento, de la custodia y la actualización del Catálogo Nacional de infraestructuras críticas y de determinar la criticidad de las mismas atendiendo a tres criterios definidos en la Directiva 2008/114/CE: "el número de víctimas, valorado en función del número potencial de víctimas mortales o de heridos; el impacto económico, valorado en función de la magnitud de las pérdidas económicas o el deterioro de productos o servicios, incluido el posible impacto medioambiental; el impacto público, valorado en función de la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida de servicios
   esenciales".

   Otra de sus funciones es la valoración y el análisis de las amenazas y riesgos de las infraestructuras, mediante "la recogida, análisis, integración y valoración de la información procedente de instituciones públicas, servicios policiales, sectores estratégicos, y de la cooperación internacional"[29].

   Cabe destacar que mediante el uso de la herramienta informática HERMES se mantienen en contacto permanente el CNPIC y los operadores críticos para poder llevar a cabo las medidas de seguridad pertinentes mediante la retroalimentación de conocimientos entre este centro, las FCSE y los operadores críticos.

C. Las funciones principales de los Ministerios y organismos integrados en el SPIC son la participación y colaboración en los Grupos de Trabajo Interdepartamentales para la elaboración de los Planes Estratégicos Sectoriales; en los Grupos de Trabajo Sectoriales; con la Secretaría de Estado de Seguridad para la elaboración de las normas sectoriales y la designación de los operadores críticos; en grupos de trabajo y reuniones a nivel internacional y en el proceso de clasificación de una infraestructura como crítica. Además proporciona asesoría técnica a la Secretaría de Estado de Seguridad, a la hora de catalogar las infraestructuras en función de criterios como la criticidad.

D. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades Autónomas de Ceuta y Melilla tienen encomendadas la mayoría de funciones relacionadas con las Fuerzas y Cuerpos de Seguridad del Estado en el

---

[28] CARO BEJARANO, M.J., La protección de las infraestructuras críticas [PDF]. Disponible en «http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf»

[29] Sobre las funciones del Centro Nacional de Protección de Infraestructuras Críticas ver CORREA HENAO G.J. y YUSTA LOYO J.M.,"Seguridad Energética y Protección de Infraestructuras Críticas", op. cit., págs. 101 y ss.

SPIC. Estas funciones consisten en la intervención mediante las FCSE en la implantación de los Planes de Apoyo Operativo, además de coordinar las mismas en caso de que haya una alerta de seguridad en el que se active el Plan Nacional de Protección de Infraestructuras Críticas (en adelante, PNPIC). Otras funciones consisten en la colaboración con los demás agentes que participan en SPIC y cumplir con una función que deben cumplir todos como es la custodia de la información de las IC que es materia clasificada. Por último, estos órganos tienen capacidad para proponer que se incluya en el Catálogo las infraestructuras que cumplan con los criterios de criticidad.

E. Las Comunidades Autónomas y las Ciudades Autónomas de Ceuta y Melilla cumplen funciones muy similares a las atribuidas las Delegaciones del Gobierno, si bien sus labores son desempeñadas a nivel autonómico y sus potestades se ejercen sobre los Cuerpos policiales de las CCAA, en el caso de contar con ellos[30] o las correspondientes Unidades adscritas del Cuerpo Nacional de Policía.

F. La Comisión Nacional para la Protección de las IC (en adelante Comisión) es uno de los agentes más importantes que componen el SPIC. La función más característica es el control que ejerce sobre los demás agentes verificando que se llevan a cabo todas las medidas necesarias para la protección de las IC. Otras funciones importantes son la aprobación de los Planes Estratégicos Sectoriales, la designación de los operadores críticos y la aprobación de la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico y el establecimiento de los objetivos que deben cumplir y de sus marcos de actuación. Esta comisión se tiene que reunir una vez al año obligatoriamente, aunque se podrán realizar reuniones extraordinarias si es necesario. Esta comisión está compuesta[31]:

a) En representación del Ministerio del Interior:

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

- El Director General de Protección Civil y Emergencias.

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

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

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

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

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

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

[30] En la actualidad, País Vasco, Cataluña y Navarra y más recientemente Canarias.

[31] Artículo 11.2 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

G. El Grupo de Trabajo Interdepartamental para la protección de las IC es un agente del sistema cuya función principal es la creación de los Planes Estratégicos Sectoriales con la colaboración de los agentes a los que afecte el mismo, también realizarán los estudios y trabajos que les encargue la Comisión. En relación a los operadores críticos, pueden proponer la designación de los mismos a la Comisión según los diferentes sectores estratégicos[32]. Igualmente pueden proponer la creación, modificación o supresión de los grupos de trabajos sectoriales o de carácter técnico y su supervisión. Este Grupo debe reunirse dos veces al año, sin perjuicio de poder celebrar una reunión extraordinaria cuando sea necesario.

El Grupo de Trabajo Interdepartamental estará compuesto por[33]:

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

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

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

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

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

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

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

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

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

H. Los Operadores Críticos son agentes que forman parte del Sistema, designados por la Comisión Nacional para la Protección de las IC. Se encargan principalmente de la elaboración de los Planes de Seguridad del Operador y de los Planes de protección específicos, prestando asistencia técnica a la Secretaría de Estado de Seguridad a la hora de valorar las IC. Asimismo les corresponde la designación tanto de un Responsable de Seguridad y Enlace que "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" (art 34.2 del RD 704/2011) como de un Delegado de Seguridad que constituye "el enlace operativo y el canal

[32] Estos sectores son: La Administración, el espacio, la industria nuclear, la industria química, las instalaciones de investigación, el agua, la energía, la salud, las tecnologías de la información y las comunicaciones (TIC), el transporte, la alimentación y por último, el sistema financiero y tributario.

[33] Artículo 12.2 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

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" (art 35 del RD 704/2011). Por último, los Operadores Críticos son los encargados de facilitar que las autoridades lleven a cabo inspecciones para comprobar que cumplen con la normativa sectorial.

3.3.2 Instrumentos.

El SPIC se vale de cinco instrumentos para proteger las IC: El Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales, los Planes de Seguridad del Operador, los Planes de Protección Específicos y los Planes de Apoyo Operativo. El uso de estos Planes tanto en sus respectivos ámbitos como en la acción conjunta permite prevenir y dar una respuesta eficaz en caso de que exista una amenaza para las IC.

A. El Plan Nacional de Protección de infraestructuras críticas establece las directrices en cuanto a las medidas preventivas a llevar a cabo por los organismos públicos y privados que participan en el Sistema. Además en el Plan se articulan una serie de niveles de seguridad, que dependerán de la evaluación de los riesgos y amenazas, cada nivel de seguridad lleva aparejada la implantación de medidas acordes con el nivel correspondiente. Especial mención ha de hacerse a la necesidad de coordinación con el Plan de Prevención y Protección Antiterrorista, en el que los niveles de seguridad se establecerán en función del nivel de alerta en infraestructuras críticas (NAIC). La intervención se realizará por las Fuerzas y Cuerpos de Seguridad, los agentes responsables de las infraestructuras y las Fuerzas Armadas en los niveles más altos de seguridad.
B. El fin de los Planes Estratégicos Sectoriales es establecer, mediante un análisis de los riesgos y amenazas, las medidas a adoptar para el funcionamiento y mantenimiento de las infraestructuras críticas, así como para determinar sus vulnerabilidades y los efectos que se derivarían en caso de que dejasen de funcionar. Estos Planes se realizan por sectores a nivel nacional y tiene que reflejar los siguientes requisitos (artículo 19.4 del Real Decreto 704/2011):

    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.

C. Los objetivos de los Planes de Seguridad del Operador son recoger los criterios que determinaran las medidas de seguridad que se deban aplicar en caso de amenaza, las cuales han de ser analizadas con anterioridad, a fin de garantizar de garantizar la continuidad de los servicios. Estas políticas generales de actuación son definidas mediante estos documentos estratégicos.

D. Los Planes de Protección Específicos incluyen tanto medidas permanentes de protección de las IC como medidas temporales que se activarán en caso de una amenaza concreta mediante el PNPIC.
E. Los Planes de apoyo operativos contienen "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" (artículo 30.3 del RD 704/2011). En síntesis, se trata de medidas que llevan a cabo las Administraciones Públicas, tanto a nivel nacional, autonómico y local de apoyo a los operadores críticos con el objetivo de mejorar la protección de las IC.

2.4 Especial mención a las herramientas HERMES y CERT.

El Catálogo Nacional de Infraestructuras Críticas recoge la información de las IC nacionales proporcionada principalmente por los operadores críticos y también por los demás agentes del Sistema, información actualizada constantemente y sistematizada informáticamente. De acuerdo con el Real Decreto 704/2011, en el Catálogo deben "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" (artículo 4.1 del RD 704/2011). El Catálogo es calificado como secreto, ya que la información que contiene es sensible y por lo tanto, su secreto es necesario para garantizar la seguridad de las IC.

Para proteger las IC de una manera eficaz, es preciso que se produzca una comunicación fluida entre los agentes implicados en el sistema. Para ello se creó el proyecto HERMES para la creación de un sistema de información que lleva el mismo nombre. Con este sistema se pretendía gestionar de una manera eficiente el Catálogo y la información que contenía. Pero para poder cumplir con los principios de colaboración y coordinación a la hora de compartir la información, fue necesaria la creación de dos plataformas diferenciadas, cada una con un grado distinto de clasificación como secreto: la Plataforma de Intercambio de Información sobre infraestructuras (en adelante PI3) y ARGOS.

Según Fernando Sánchez Gómez, Director del CNPIC, la plataforma PI3 está "destinada a proveer un mecanismo de información directo y eficiente entre todos los agentes del Sistema PIC, mediante el establecimiento de herramientas colaborativas como, por ejemplo, una destinada al desarrollo de documentos tipo Wiki, foros de discusión, gestor documental, etc. La plataforma permitirá gestionar información clasificada como 'difusión limitada'"[34].

[34] Entrevista a Fernando Sánchez Gómez, Revista SEGURITECNIA [en línea]. Disponible en: «http://www.seguritecnia.es/seguridad-aplicada/infraestructuras-criticas/el-espiritu-de-la-normativa-pic-se-basa-en-la-confianza-mutua-y-en-la-confidencialidad-de-la-informacion-que-se-comparte»

Por su parte, ARGOS[35] es un sistema de alerta temprana que recoge y analiza la información, con el objetivo de detectar cualquier amenaza que permitirá responder a la misma de una manera más rápida y eficaz.

El Centro Criptológico Nacional (en adelante CCN) que depende del Centro Nacional de Inteligencia (en adelante CNI) también proporciona asistencia a las IC con la creación del CCN-CERT que es "un órgano gubernamental con capacidad de respuestas a incidentes de seguridad de la información"[36]. El *Computer Emergency Response Team* (CERT), lo define Marcos Gómez Hidalgo, subdirector de Operaciones de INCIBE como:

> "Un equipo humano y tecnológico que aglutina capacidades de detección, alerta temprana, análisis e investigación, respuesta a incidentes, mitigación de daños y riesgos, capacitación, etc., pero sobre todo que sabe coordinarse con todos los agentes o entidades competentes, con atribuciones y con responsabilidades, incluyendo a los afectados de un incidente o problema de Ciberseguridad"[37].

Además este centro estudia la seguridad global de las redes y sistemas del España, siendo su función principal la prevención de ataques a través de la red y la ejecución de las medidas necesarias en respuesta a los mismos.

4. SISTEMAS DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE OTROS PAÍSES.

Conocer en qué estado se encuentra en otros países el desarrollo en materia de protección de las infraestructuras críticas, puede proporcionarnos, mediante el análisis comparativo, una imagen de cuál es la situación de las mismas en España. Concretamente, expondremos los sistemas de protección de IC de Australia, Japón, Estados Unidos, Canadá, Reino Unido, Francia y Bélgica, todos ellos países occidentales desarrollados. La elección se justifica en algunos casos por tratarse de países pioneros en este campo, como es el caso de Estados Unidos, primer país en hacer mención explícita a la protección de las IC con la *Presidential Decision Directive nª 63 "Protecting America's Critical Infrastructures"*, de 22 de mayo de 1998. En el caso de los Estados europeos, además de la importancia de conocer la labor desarrollada por éstos tras la Directiva 114/2008/CE, su elección no ha sido fruto de la casualidad: Francia, Reino Unido y Bélgica son los países europeos que junto con España, más han sufrido las consecuencias de atentados terroristas.

[35] ARGOS es un proyecto que creó un sistema de alerta temprana del mismo nombre para instalaciones que se financió con fondos europeos.

[36] CORREA HENAO G.J. y YUSTA LOYO J.M.,"Seguridad Energética y Protección de Infraestructuras Críticas", op. cit., pág. 99.

[37] Información recogida en la web de INCIBE del día 26 de noviembre de 2014, disponible en: https://www.incibe.es/pressRoom/Prensa/Actualidad_INCIBE/Jornada_IICC_Amenaza_Ciberterrorista

4.1 Australia.

En Australia los órganos encargados de la protección de las IC son el *Critical Infrastructure Advisory Council* (en adelante CIAC) perteneciente al *Attorney General´s Department* del Gobierno de Australia. El CIAC es un órgano consultivo del gobierno cuya misión es el liderazgo de la protección de las IC, que además de estar presidido por el *Attorney General´s Department*, realiza labores de secretaría y asesoría en materias de recuperación de las IC. Es el encargado de revisar el trabajo de los *Sector Groups*, de los *Expert Advisory Groups* y de las *Comunities of Interest*. El CIAC australiano asemeja sus funciones al CNPIC español, aunque nuestro centro posea mayor cantidad de las mismas. Este sistema se vale de las siguientes herramientas para llevar a cabo sus objetivos:

- *Trusted Information Sharing Network* (en adelante TISN) Es uno de los instrumentos utilizados por Australia para la comunicación e intercambio de información entre los propietarios y los operadores con el Gobierno. Este se conforma como un espacio seguro en el que además de comunicarse, cooperan para hacer frente a los problemas de seguridad que pueden surgir en las IC. Es el instrumento homólogo al sistema HERMES en España. Por otro lado, Australia también cuenta con un CERT como ocurre en la mayoría de países estudiados a continuación.
- *Critical Infrastructure Resilience* (en adelante CIR). Es un sitio web cuya función es el asesoramiento en materias de recuperación y de acciones a realizar en caso de ataque a las IC. El objetivo es que los operadores principalmente y los propietarios de una IC sepan gestionar mejor los riesgos y amenazas, proporcionando continuidad a los servicios que realizan y así evitar la interrupción de la actividad, que podría tener graves consecuencias para la sociedad.
- *National Terrorism Threat Advisory System*[38]. Mediante esta herramienta se informa de la probabilidad de actos terroristas, para realizar las labores de protección y prevención de la nación. A fecha de 02/06/2016 el nivel se sitúa en "probable"[39] de la siguiente escala de cinco niveles: "Not expected", "possible", "probable", "expected" y "certain".

La *Australian Security Intelligence Organisation* (en adelante ASIO) colabora estrechamente con el Gobierno, con la Policía Federal Australiana (AFP), con los operadores y propietarios de las IC, en la prevención y respuesta a los ataques terroristas que se puedan producir sobre una IC.

Los sectores de las IC australianas son los siguientes:

- Banking and Finance
- Central Government / Government Services
- (Tele-)Communication / Information and Communication Technologies (ICT)

[38] Página web de la *National Terrorism Threat Advisory System*: https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/National-Terrorism-Threat-Advisory-System.aspx

[39] En la página web de la *National Terrorism Threat Advisory System* se advierte de "Credible intelligence, assessed by our security agencies indicates that individuals or groups have developed both the intent and capability to conduct a terrorist attack in Australia. The public should continue to exercise caution and report any suspicious incidents to the National Security Hotline by calling 1800 1234 00".

- Emergency / Rescue Services
- Energy / Electricity
- Health Services
- Food
- Transportation / Logistics / Distribution
- Water (Supply)

Como podemos comprobar, la *National Guidelines For Protecting Critical Infrastructure From Terrorism* dedica sus líneas casi exclusivamente a ataques físicos, dejando de lado posibles ataques a sus sistemas informáticos. Es el plan bastante más policial de los que vamos a estudiar, en el que se le da mucha importancia a los servicios de inteligencia australianos y la realización de investigaciones preventivas. Los objetivos principales son: mantener la seguridad, salvar vidas, prevenir el daño, proteger las propiedades, reducir las pérdidas, investigar el incidente y recuperarse del mismo. También se hace referencia a la necesidad de mejorar la administración de la información pública con los medios de comunicación, algo innovador en un plan de este tipo, ya que otras estrategias de otros países no hacen mención a esta temática.

4.2 Japón.

El sistema de protección de las IC en Japón se conforma mediante *The Second National Strategy on Information Security*[40], *Second Action Plan on Information Security Measures for Critical Information Infrastructure*[41] y *The Basic Policy of Critical Information Infrastructure Protection*[42].

El sistema japonés es un sistema complejo, bastante desarrollado y que atiende a todo tipo de riesgos y amenazas, en el que una vez más vuelve a destacar la colaboración público-privada. El sistema japonés hace hincapié "en la prevención de ataques cibernéticos a sus infraestructuras de interés nacional como principal amenaza"[43]. El *Cabinet Secretariat* es el órgano de mayor rango encargado de la protección de las IC bajo el que se encuentran el *Information Security Policy Council* (ISPC) y el *National Information Security Center* (NISC) cuya función principal es el desarrollo de la política de protección de las IC. Por otro lado, cobra vital importancia la colaboración internacional, en este caso con Estados Unidos, Europa, la región Asia-Pacífico y la Asociación de Naciones del Sudeste Asiático (ASEAN). Los sectores de vital importancia para Japón son los siguientes:

- Information communication.
- Finance.
- Aviation.
- Railway.
- Electric power.
- Gas.

---

[40] The Second National Strategy on Information Security. February 3, 2009, National Information Security Policy Council. http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf

[41] Second Action Plan on Information Security Measures for Critical Information Infrastructure. February 3, 2009, The Information Security Policy Council. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf

[42] The Basic Policy of Critical Information Infrastructure Protection (3rd Edition). May 19, 2014, Information Security Policy Council. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

[43] MIRANZO,M.; DEL RÍO,C., "La protección de infraestructuras críticas" *UNISCI Discussion Papers*. May. 2014, núm. 35, p.349.

- Government and administrative services.
- Medical.
- Water service.
- Logistics

Otros centros, órganos y organizaciones que participan en el sistema son:

- *National Incident Response Team* (NIRT). Su misión principal es analizar las amenazas, la realización de estrategias técnicas para prevenir incidentes y ayudar a otras organizaciones gubernamentales en materia de seguridad de la información proporcionando conocimiento en la materia.
- *Japan Computer Emergency Response Team Coordination Center* (JPCERT/cc). Es un CERT japonés cuyo objetivo es proporcionar productos y servicios en materia de seguridad a las agencias gubernamentales y a las asociaciones de industria y comercio.
- *Telecom Information Sharing and Analysis Center (*Telecom-ISAC). Es un centro cuyo objetivo consiste en intercambiar información entre el gobierno y los agentes participantes, del sector de las telecomunicaciones, en el sistema de protección de las IC, además del almacenamiento y análisis de la información.
- *Cyber Force*. Se encarga de vigilar internet con el objetivo de proteger la seguridad de la red y en caso de tener constancia de un ataque "ciberterrorista" informar a los operadores críticos del mismo para que puedan reaccionar al mismo.
- *Portal Site of National Police Agency*. Este sitio web se encarga de proporcionar información sobre la seguridad en las redes al gobierno para prevenir emergencias a gran escala en la red.
- *Capability for Engineering of Protection, Technical Operation, Analysis and Response* (CEPTOAR). Se encarga de intercambiar y analizar la seguridad de la información y las comunicaciones entre las entidades privadas y públicas[44].

La siguientes figuras reflejan el funcionamiento de los centros y órganos anteriores a la hora de compartir información en condiciones de normalidad. En situaciones de crisis, la única diferencia destacable es que los ministros encargados de gestionar la crisis y los ministros encargados de la prevención de desastres se comunican con el *Cabinet secretariat* en vez de con el NISC, que será el encargado de dirigir las acciones pertinentes en respuesta a la amenaza.

[44] Andress,J. ; Winterfeld, S., *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2ª ed., Syngress-Elsevier, Waltham, 2013, p. 94.

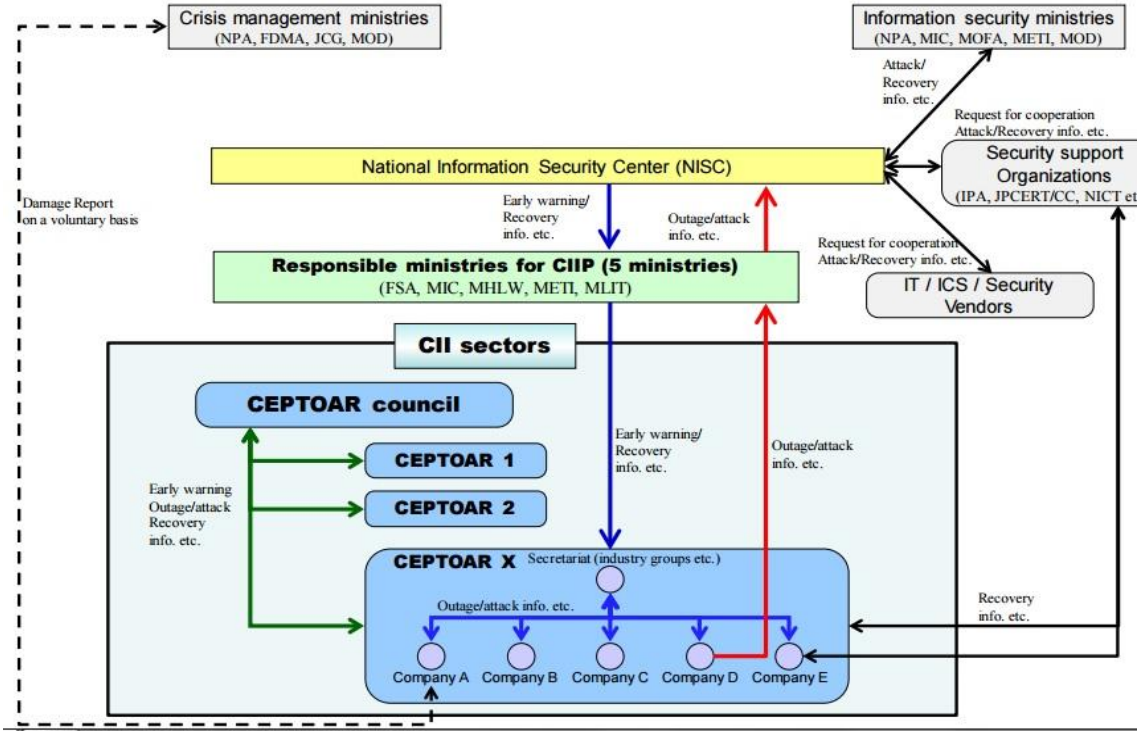

Figura 1. Fuente: ***The Basic Policy of Critical Information Infrastructure Protection*.**

Un aspecto a destacar es el análisis de los resultados obtenidos con los planes anteriores y el reconocimiento de los aspectos que hay que mejorar y que se deben implantar en los siguientes planes como queda reflejado en el documento *The Basic Policy of Critical Information Infrastructure Protection*. Por lo tanto, la evaluación de su sistema les permite perfeccionar su capacidad de protección de las IC. Recientemente el gobierno japonés ha desvelado que pretende crear una nueva agencia para la protección de las IC, que comenzará a funcionar en 2017, antes de los Juegos Olímpicos de Tokio 2020. Esta agencia llamada *Industrial Cybersecurity Promotion Agency* (ICPA) contratará a "white hat hackers" para la realización de sus actividades y también funcionará sobre la base de la colaboración público-privada[45].

4.3 Estados Unidos.

El *National Infrastructure Protection Plan 2013 (NIPP): Partening for Critical Infrastructure Security and Resilience* se desarrolló con la colaboración entre los sectores públicos y privados, siendo los participantes en el sistema de protección los propietarios y operadores de las IC, las agencias gubernamentales a nivel territorial, estatal y local, las agencias no gubernamentales, las agencias específicas de cada sector y otros agentes y departamentos Federales. El *Department of Homeland Security* bajo mando del Secretario de este Departamento, es el órgano encargado de guiar, promover y coordinar los esfuerzos de todos los integrantes de la comunidad de infraestructuras críticas para promover la seguridad y la resiliencia de las mismas.

El Plan estadounidense es bastante complejo y consta de numerosos agentes que participan y realizan una actividad específica en la protección de las IC. Algunos de

[45] Enlace de la noticia: http://www.tripwire.com/state-of-security/latest-security-news/japan-to-form-new-cybersecurity-agency-to-protect-its-critical-infrastructure/

ellos se agrupan por sectores, agencias de coordinación entre diferentes sectores y a nivel estatal, local y territorial[46]. *Sector Coordinating Structures* es el título bajo el que se agrupan aquellos agentes mencionados anteriormente referidos a un solo sector y *Cross-Sector Coordinating Structures* es la agrupación de aquellos que se refieren a la coordinación entre sectores diferentes. La siguiente figura refleja algunos de los elementos que componen la comunidad de IC:

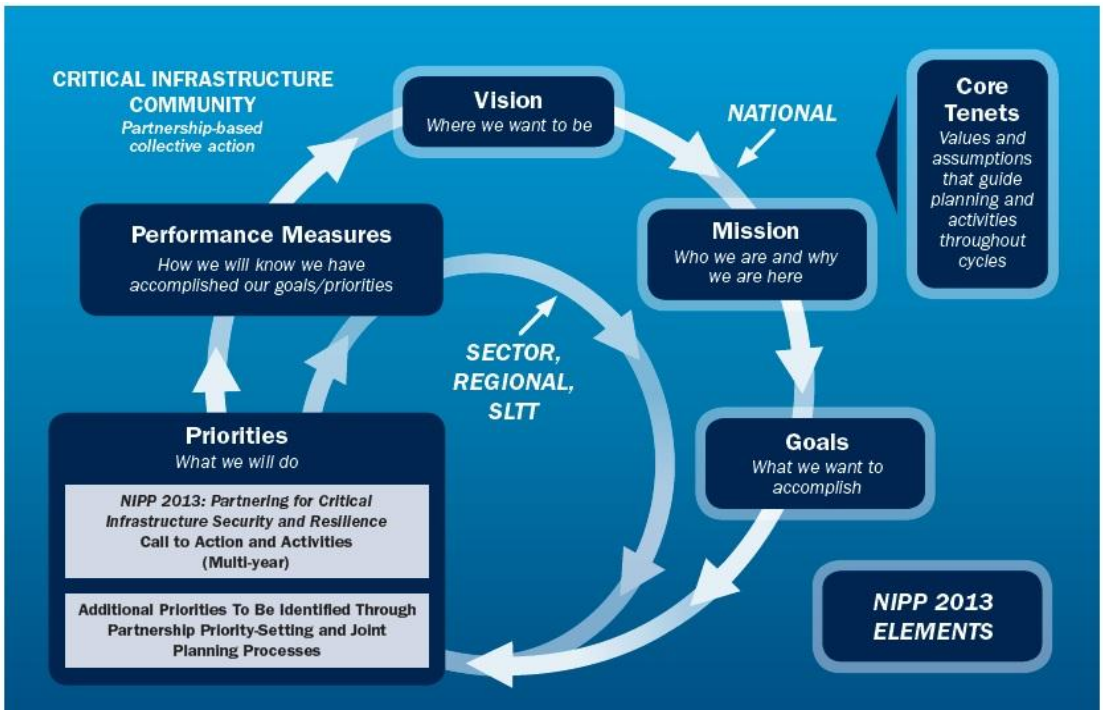

Figura 2. Fuente: ***NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*.**

Otros centros, agencias y organismos que participan de forma activa en este sistema, aportando diferentes funciones a la misma, son

a) *Information Sharing and Analysis Centers* (ISACs). Existe un centro para cada sector cuyo objetivo consiste en proporcionar análisis sectoriales profundos de amenazas y riesgos que ponen en peligro sus IC y coordinar las acciones llevados a cabo por el sector durante los incidentes, intercambiando además información con otros agentes de este sistema.

b) *Critical Infrastructure Patnership Advisory Council* (CIPAC). Los objetivos principales de este órgano son: la planificación, la coordinación y el intercambio de información entre sectores; el asesoramiento en materia de actividades operativas y de recuperación de las IC; proporcionar asesoramiento al Gobierno Federal en la creación y aplicación de políticas relacionadas con las IC.

c) *National Infrastructure Coordinating Center* (NICC). Es uno de los dos centros nacionales de IC del *Department of Homeland Security* junto con el *National Cybersecurity and Communications Integration Center* (NCCIC), que mencionaremos a continuación. Este centro tiene como objetivo proporcionar información previamente obtenida de las IC, para que los órganos encargados de tomar decisiones lo hagan eficazmente sobre cualquier tipo y nivel de amenaza.

[46] Murray, A. y Grubesic, Tony., "Critical infrastructure protection: The vulnerability conundrum" *Telematics and Informatics*. Feb 2012, núm 29, pp. 56-65.

d) *National Cybersecurity and Communications Integration Center* (NCCIC). Es el otro centro nacional de IC del *Department of Homeland Security* y tiene objetivos similares al NICC, con la diferencia de que sus actividades se centran sobre la parte lógica de las infraestructuras. Junto con el NICC tratan de reducir los tiempos de respuesta a la hora de tomar decisiones gracias a la información que aportan.
e) *National Operations Center* (NOC). Este órgano proporciona información y un marco de actuación común para el Gobierno Federal y los Gobiernos locales, estatales y territoriales, en caso de un incidente.
f) *National Cyber Investigative Joint Task Force* (NCIJTF). El FBI es el responsable de esta agencia y su función principal es desarrollar y compartir información sobre amenazas a través de la red y coordinar e integrar las actividades operacionales para hacer frente a los riesgos y amenazas, inclusive las que puedan afectar a las IC.

Estados Unidos, a pesar de usar instrumentos personalizados para cada órgano, también posee un CERT como ocurre en la gran mayoría de países. Uno de esos instrumentos es el *Protected Critical Infrastructure Information Program* (PCII) que establece los requisitos y pasos a seguir para el acceso y protección de la información de las IC. Por otro lado la comunicación entre las infraestructuras críticas es administradas por los ISACs, en las que cada uno de ellos administra la información relacionadas con las IC de su sector, a diferencia del caso español, en el que con la herramienta HERMES se realiza una comunicación global entre los agentes encargados de la protección de las IC. La siguiente figura muestra el esquema que sigue el plan estadounidense a la hora de compartir información dentro del marco de gestión del riesgo de las IC.

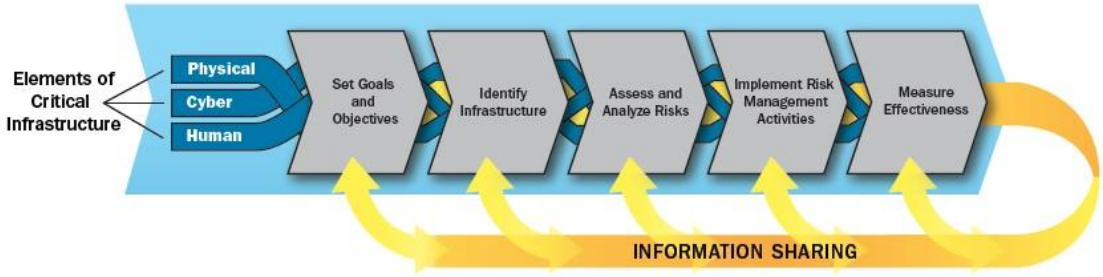

Figura 3. Fuente: ***NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*.**

La comunidad en caso de incidente utiliza los sistemas establecidos en el *National Prevention Framework*, *National Response Framework*, *National Disaster Recovery Framework* y el *National Cyber-Incident Response Plan* cuyo objetivo principal es la prevención, la protección, la reducción de daños, la reacción y recuperación.

Como señalan Correa y Yusta, en el marco de gestión de riesgos, el NIPP cabe diferenciar seis etapas bien delimitadas: "establecimiento de objetivos de seguridad; identificación de activos, sistemas, redes y funciones; evaluación del riesgo; priorización de acciones; ejecución de programas de protección; y medición de la efectividad", al tiempo que se proporciona un marco de retroalimentación y de mejora continua, flexible y adaptable a las situaciones de riesgo de cada sector[47]. La diferenciación de estas etapas permite llegar al último estadío que no es otro que la

[47] CORREA HENAO G.J. Y YUSTA LOYO J.M.,"Seguridad Energética y Protección de Infraestructuras Críticas", op. cit., pág. 96.

medición de la efectividad del sistema, algo por desgracia no demasiado común en los planes y políticas españolas.

El sistema estadounidense para proteger las IC es completo pero bastante complejo. El plan recoge todo tipo de posibilidades que pueden dañar sus IC como pueden ser catástrofes naturales a ataques perpetrados por el hombre. Abarca desde la protección de ataques físicos hasta la de ataques lógicos, además de hacer referencia a las amenazas de carácter internacional que puede afectarlas, a diferencia del sistema australiano que se centra casi en exclusiva a ataques terroristas y en sus estructuras físicas, dejando de lado la posibilidad de ataques a través de la red.

Los sectores a los que hace referencia el plan de Estados Unidos son los siguientes:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

4.4 Canadá.

El sistema canadiense de protección de las IC se desarrolla en la *National Strategy for Critical Infrastructure* y el *Action Plan for Critical Infrastructure* que establecen una colaboración a nivel federal, provincial, territorial y de los sectores de las IC para el fortalecer la capacidad de recuperación de las mismas. El primero establece los principios básicos del funcionamiento de este sistema y el segundo profundiza en ellos desarrollando las actividades y mecanismos de los participantes en el mismo. La protección de las IC se enmarca dentro del *Department of Public Safety and Emergency Preparedness*, más conocido como *Public Safety Canada*.

Este sistema establece 10 sectores en los que se clasificarán las IC, como podemos observar en la siguiente tabla:

Sector	Sector-specific federal department/agency
Energy and utilities	Natural Resources Canada
Information and communication technology	Industry Canada
Finance	Finance Canada
Health	Public Health Agency of Canada
Food	Agriculture and Agri-Food Canada
Water	Environment Canada
Transportation	Transport Canada
Safety	Public Safety Canada
Government	Public Safety Canada
Manufacturing	Industry Canada Department of National Defence

Tabla 1. Fuente: *Action Plan for Critical Infrastructure* 2014. Sectors and sector-specific federal department/agency.

La Estrategia Nacional para la Infraestructura Crítica de Canadá tiene como objetivo mejorar la resiliencia de las IC y definir las competencias de los Gobiernos provinciales, territoriales y federales y del sector privado[48]. Para lograr la coordinación de las actividades a diferentes niveles de gobierno y sectores se crea el *National Cross Sector Forum* y el *Federal-Provincial-Territorial Critical Infrastructure (FPT-CI) Working Group*:

• *National Cross Sector Forum.* Está formado por 10 representantes de cada uno de los diez sectores de IC. Se reune anualmente y es presidida por el Viceministro de Seguridad Pública Canadá y un representante provincial o territorial.

• *FPT-CI Working Group.* Es el foro permanente en el que colaboran los Gobiernos, provinciales, territoriales y Federal en materia de IC. Las reuniones están copresididas por un representante del *Public Safety Canada* y un representante provincial o territorial.

Por su parte, el *National Risk Profile of Critical Infrastructure* proporciona información sobre los riesgos y amenazas para las IC, identificando dependencias e interdependencias entre las IC y sus sectores. El análisis de dicha información permite alcanzar una comprensión de las tendencias de los riesgos y amenazas. Estas actividades permiten llevar a cabo de una manera eficaz las actividades de gestión de riesgos de las IC.

Este sistema tiene previsto que se comparta información multidireccional entre propietarios, operadores, gobiernos y organizaciones de seguridad e inteligencia como son *Royal Canadian Mounted Police* (RCMP), *Canadian Security Intelligence Service* (CSIS), *Canada Border Services Agency* (CBSA), *Canadian Cyber Incident Response Centre* (CCIRC) que ayudan, proporcionando información sobre los riesgos y amenazas, a la realización de actividades de gestión de riesgos.

A diferencia del sistema de comunicación utilizado entre los agentes que participan en nuestro sistema (HERMES), Canadá utiliza *Canadian Critical Infrastructure*

[48] QUIGLEY, K., "Man plans, God laughs": Canada's national strategy for protecting critical infrastructure", *Canadian Public Administration.* Mar 2013, Núm 56, pp 142-164.

Gateway. Consiste en una plataforma de trabajo de información no clasificada en el que los participantes en el sistema de protección pueden colaborar e intercambiar información con el objetivo de mejorar la capacidad de recuperación y hacer más seguras las IC canadienses asemejándose a las funciones de nuestra plataforma PI3 de HERMES. Por otro lado, el intercambio y la divulgación de información protegida o clasificada se rigen por las leyes y políticas federales, provinciales y territoriales.

El *Regional Resilience Assessment Program* (RRAP) es un programa mediante el cual se realizan actividades de formación y evaluaciones de las IC, que podrán ser llevadas a cabo "in situ", con el objetivo de analizar la capacidad de recuperación y la interdependencias entre ellas mismas. En estas evaluaciones se implican todos los agentes participantes en el sistema canadiense.

El sistema canadiense no está excesivamente detallado, siendo un sistema más sencillo que el estadounidense y el español. La estrategia hace referencia a la protección de ataques físicos y de ciberataques, que no se centra exclusivamente en el terrorismo, sino que también menciona incidentes ocasionados por fenómenos naturales como ocurre con nuestro sistema. Es importante resaltar que el sistema canadiense está provisto de herramientas para evaluar el progreso realizado en la capacidad de resiliencia y protección de sus IC, al igual que en Estados Unidos y Japón cosa que, insistimos, no ocurre en España.

4.5 Especial mención al acuerdo entre EE.UU y Canadá.

Canada-United States Action Plan for Critical Infrastructure (en adelante *Canada-U.S. Action Plan*) es un Plan que pretende fortalecer la protección y la capacidad de resiliencia de las infraestructuras críticas mediante la colaboración entre Canadá y Estados Unidos. El citado Plan es fruto del *Agreement Between the Government of Canada and the Government of the United States on Emergency Management Cooperation*, acuerdo formalizado entre Estado Unidos y Cánada en diciembre de 2008, por el que ambos Estados se comprometieron a colaborar en situaciones de emergencia que involucrasen a los dos países.

El Plan prevé el intercambio y protección de información entre ambos países, además de la colaboración entre los diferentes sectores de ambos, la colaboración en la identificación de IC y sectores de riesgo y la intervención conjunta mediante los planes de gestión de riesgos.

Los objetivos del *Canada-U.S. Action Plan* serían básicamente:

- La naturaleza interconectada de las infraestructuras críticas exige un enfoque coordinado entre Canadá- EE.UU.
- Los enfoques regionales para la colaboración a través de la frontera debe ser guiada por un marco global para la infraestructura crítica entre Canadá-EE.UU.
- La fuerte colaboración del sector privado a través de la frontera debe ser respaldado por un enfoque integrado entre Canadá-EE.UU.
- La descoordinación aumenta la probabilidad de la duplicación de costes y esfuerzos que pueden ser evitados a través del desarrollo de la colaboración y el intercambio de mejores prácticas.

- La comunicación entre las partes implicadas en las infraestructuras críticas (tanto nacional como transfronteriza) necesitan ser coordinadas de forma precisa y oportuna[49].

4.6 Programa Europeo de Protección de Infraestructuras Críticas (PEPIC).

El Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) tiene como objetivo la mejora de la protección de las IC en la UE frente a las amenazas a las mismas, especialmente contra el terrorismo. Su punto de partida es la identificación y designación de las Infraestructuras Críticas Europeas (en adelante ICE), tal y como ordena la Directiva 2008/114/CE. Su ejecución requiere la adopción de "medidas diseñadas para facilitar la aplicación del PEPIC, lo que incluye un Plan de acción del PEPIC, la Red de información sobre alertas en infraestructuras críticas (CIWIN), el uso de grupos de expertos en PIC a nivel de la UE, los procedimientos para compartir la información sobre PIC y la identificación y análisis de interdependencias". Por lo tanto, se deben llevar a cabo planes de intervención en caso de incidente que afecte a alguna ICE y además se le debe prestar apoyo a las IC de los Estados miembros. Este programa sitúa su plan de acción entorno a 3 líneas de actividad que son las siguientes:

- Línea de actividad 1: se ocupará de los aspectos estratégicos del PEPIC y del desarrollo de medidas aplicables horizontalmente a todas las acciones de protección de IC.
- Línea de actividad 2: se ocupará de las infraestructuras críticas europeas y se ejecutará a nivel sectorial.
- Línea de actividad 3: se ocupará de apoyar a los Estados miembros en sus actividades relacionadas con infraestructuras críticas nacionales.

Los Estados miembros usan para el intercambio de información de sus ICE y de alertas rápidas, la Red de Información sobre Alertas en Infraestructuras Críticas (CIWIN), complementando los sistemas y plataformas que tengan los países establecidos para sus IC. El Sistema Europeo de Alerta Rápida (ARGUS por sus siglas en inglés) permite la conexión de todos los sistemas de emergencia en Europa mandando la información a los mismos para que lleven a cabo las medidas pertinentes en caso de amenaza[50].

Los Planes de Intervención se realizan en caso de incidente, su finalidad es reducir los daños e impedir la destrucción de la IC, intentando evitar que interrumpan sus servicios, tanto en el país en el que se produce el incidente como en los Estados miembros a los que proporcione servicios o se interconecten con las correspondientes IC. En su ejecución intervienen todos los agentes implicados en la protección de las ICE tanto nacionales como comunitarios.

---

[49] Original: -The interconnected nature of critical infrastructure requires a coordinated Canada-U.S. approach; Regional approaches to cross-border collaboration need to be guided by an overarching Canada-U.S. framework for critical infrastructure; Strong private sector collaboration across the border needs to be supported with an integrated Canada-U.S. approach; Uncoordinated efforts increase the likelihood of wasteful duplication of efforts that can be managed through collaborative development and sharing of best practices; and Communications with critical infrastructure stakeholders (both domestic and crossborder) need to be coordinated, accurate and timely.

[50] Descripción del sistema en la web: http://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/argus_en.htm

El PEPIC marcó las pautas que debían seguir los Estados miembros en sus desarrollos legislativos sobre las IC, explicando la similitud entre los sistemas de protección de las IC de la mayoría de los Estados miembros de la UE.

4.7 Reino Unido.

En Reino Unido la protección de las infraestructuras críticas se ha concretado en la *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards* de marzo de 2010; otros documentos que describen su sistema de protección de IC son: *el United Kingdom National Security Strategy* (NSS), la *Strategic Defence and Security Review* (SDSR) y la *UK's Cyber Security Strategy*, cada uno de ellos preve, en su respectivo ámbito, la creación de un marco sobre la protección de las IC. El terrorismo y la ciberseguridad son los asuntos más relevantes a la hora de protegerse, además vuelve a ponerse de manifiesto la importancia de la colaboración público-privada y la agrupación por sectores para una mejor protección. Igualmente se hace hincapié en la prevención y en la capacidad de resiliencia de las IC. La estrategia de UK agrupa las IC en los siguientes sectores:

National Infrastructure Sector	Sub Sector	Whitehall Sector Sponsor Dept	Lead in Scotland	Lead in Wales	Lead in Northern Ireland
Communications	-Telecommunications	BIS	BIS	BIS	NIO
	-Postal Services	BIS	BIS	BIS	
	-Broadcast	DCMS	DCMS	DCMS	
Emergency Services	-Ambulance	DH	SE	WAG	NIO
	-Fire & Rescue	DCLG	SE	WAG	NIO
	-Marine	DfT	DfT	DfT	NIO
	-Police	HO	SE	HO & WAG	NIO
Energy	-Electricity	DECC	DECC	DECC	NIO
	-Gas				
	-Fuel				
Finance	-Payment, Clearing & Settlement Systems	HMT	HMT	HMT	NIO
	-Markets & Exchanges	HMT	HMT	HMT	NIO
	-Public Finances	HMT	HMT	HMT	NIO
Food	-Production	DEFRA & FSA	SE	WAG & FSA	NIO
	-Processing				
	-Import				
	-Distribution				
	-Retail				
Government	-Central government[2]	CO			NIO
	-Devolved Administrations/Functions;		SE	WAG	NIO
	-Regional & Local government;	CLG	SE	WAG	NIO
	-Parliament	Palace of Westminster Authorities[3]	Scottish Parliamentary		
Health	-Health & Social Care	DH	SE	WAG	NIO
Transport	-Aviation	DfT	DfT	DfT	DfT/NIO
	-Maritime	DfT	DfT	DfT	DfT/NIO
	-Land	DfT,	SE(road)	WAG(road)	NIO (road+ rail)
Water	-Potable Water Supply	DEFRA	SE	WAG	NIO
	-Waste Water Services				
	-Dams				

Key
BIS: Department for Business, Innovation and Skills, **CLG:** Department for Communities and Local Government, **CO:** Cabinet Office, **DCMS:** Department for Culture, Media and Sport, **DECC:** Department of Energy and Climate Change, **Defra:** Department for Environment, Food and Rural Affairs, **DfT:** Department for Transport, **DH:** Department of Health, **FSA:** Food Standards Agency, **HO:** Home Office, **HMT:** Her Majesty's Treasury, **NIO:** Northern Ireland Office, **SE:** Scottish Executive, **WAG:** Welsh Assembly Government.

Tabla 2. Fuente: ***Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*** **de marzo de 2010.**

La *UK Government's counter terrorism strategy* (CONTEST) también hace referencia a las IC y dividide su estrategia en cuatro aspectos: Prevent, Pursue, Protect and Prepare[51]. El CPNI es el centro encargado de la protección de las IC en Reino Unido y es el equivalente al CNPIC español que "está formado por el Centro de Coordinación de Seguridad de la Infraestructura Nacional (NISCC, National Infrastructure Security Coordination Centre) y el NSAC (National Security Advice Centre), dependiente este a su vez del MI5 británico, y los centros WARP (Warning, Advice and Reporting Point)"[52].

La *Office of Cyber Security & Information Assurance* (OCSIA) es un órgano cuya misión es asumir la dirección y coordinar el programa de ciberseguridad en Reino Unido con el objetivo de mejorar la seguridad en la red y la seguridad de la información, además proporciona asesoramiento al *Cabinet Office ministers* y al *National Security Council*. Este órgano trabaja con el *Communications-Electronics Security Department* (CESG) que pertenece al *Government Communications Headquarters* y es la autoridad nacional para el aseguramiento de la información que además, proporciona asesoramiento sobre cómo proteger la información y sistemas de información contra las amenazas actuales. Otros órganos importantes en la protección de las IC son el *National Cyber Security Centre*, creado este mismo año y del que está aún por ver qué competencias adquiere, y el *Cyber Security Operations Centre* (CSOC). Este conglomerado de estrategias y de órganos componen el sistema de protección de las IC de Reino Unido, que como ocurre en la mayoría de los países también posee un CERT.

4.8 Francia.

En relación a la protección de las IC, Francia cuenta con la *Stratégie Nationale pour la sécurité du numérique* y el *Livre blanc sur la défense et la sécurité nationale*. La principal regulación de la protección de las IC se realiza en la *Instruction générale interministérielle relative la sécurité des activités d'importance vitale Nº6600/SGDSN/PSE/PSN du 7 janvier 2014*[53], que sustiuye la tradicional denominación de infraestructura crítica por la de *points d'importance vitale* (PIV) o *activités d'importance vitale*[54]. Esta *Instruction générale* crea el *Dispositif de sécurité des activités d'importance vitale* (SAIV) que es descrito como:

"el cuadro legislativo y reglamentario que permite asociar a los operadores de vital importancia (OIV), públicos o privados, al sistema nacional de protección contra el terrorismo, el sabotaje y los actos de mala fe y analizar los riesgos y aplicar las medidas de su nivel en coherencia con las decisiones de los poderes públicos"[55].

Además, la *Instruction générale interministérielle* crea tres planes de protección:

- *Plans de sécurité d'opérateur* (PSO).

---

[51] Traducción: Prevenir, buscar (información), proteger y preparar.

[52] Protección de Infraestructuras Críticas 2011, S2 Grupo. http://s2grupo.es/wp-content/uploads/2016/01/Informe_PIC2011_S2Grupo.pdf

[53] Instruction générale interministérielle relative la sécurité des activités d'importance vitale, 07/01/2014 (6600/SGDSN/PSE/PSN). *Disponible en*: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf

[54] Traducción de esos términos: Puntos de vital importancia o actividades de vital importancia

[55] Original: "*Il constitue le cadre législatif et réglementaire permettant d'associer les opérateurs d'importance vitale* (OIV)*, publics ou privés, au système national de protection contre le terrorisme, le sabotage et les actes de malveillance et d'analyser les risques et d'appliquer les mesures de leur niveau en cohérence avec les décisions des pouvoirs publics".*

- *Plans particuliers de protection des points d'importance vitale* (PPP).
- *Plans de protection externe* (PPE).

Los planes anteriores son equivalentes a los Planes de Seguridad del Operador, los Planes de Protección Específicos y a los Planes de Apoyo Operativo españoles respectivamente.

El órgano responsable del sistema de protección de las IC en Francia es la *Secrétariat General de la Défense Nationale* (SGDSN) y el principal objetivo del sistema es protegerse especialmente de los ataques terroristas sobre infraestructuras físicas, aunque también adquiere importancia la protección de ataques a través de la red.

El SAIV se coordina con otros planes como son el *Plan Vigipirate* y los planes complementarios del anterior llamado *Plans Pirate.* El *Plan Vigipirate* es un dispositivo de vigilancia, prevención y de protección en la lucha contra el terrorismo. Este dispositivo contiene planes específicos de intervención que requieren de medios especializados y que permiten una reacción rápida en caso de amenaza. Por su parte, los *Plans Pirate* son una serie de planes de intervención que se adaptan a un tipo de riesgo particular. Estos planes contemplan la utilización de medios específicos tales como armas biológicas, químicas y nucleares, en lugares igualmente específicos como pueden ser medios de transporte colectivos como aviones o el metro. Para cada caso existen unos mecanismos y respuestas específicos de reacción. La siguiente figura proporciona una visión esquemática de los planes y medidas antiterroristas de Francia:

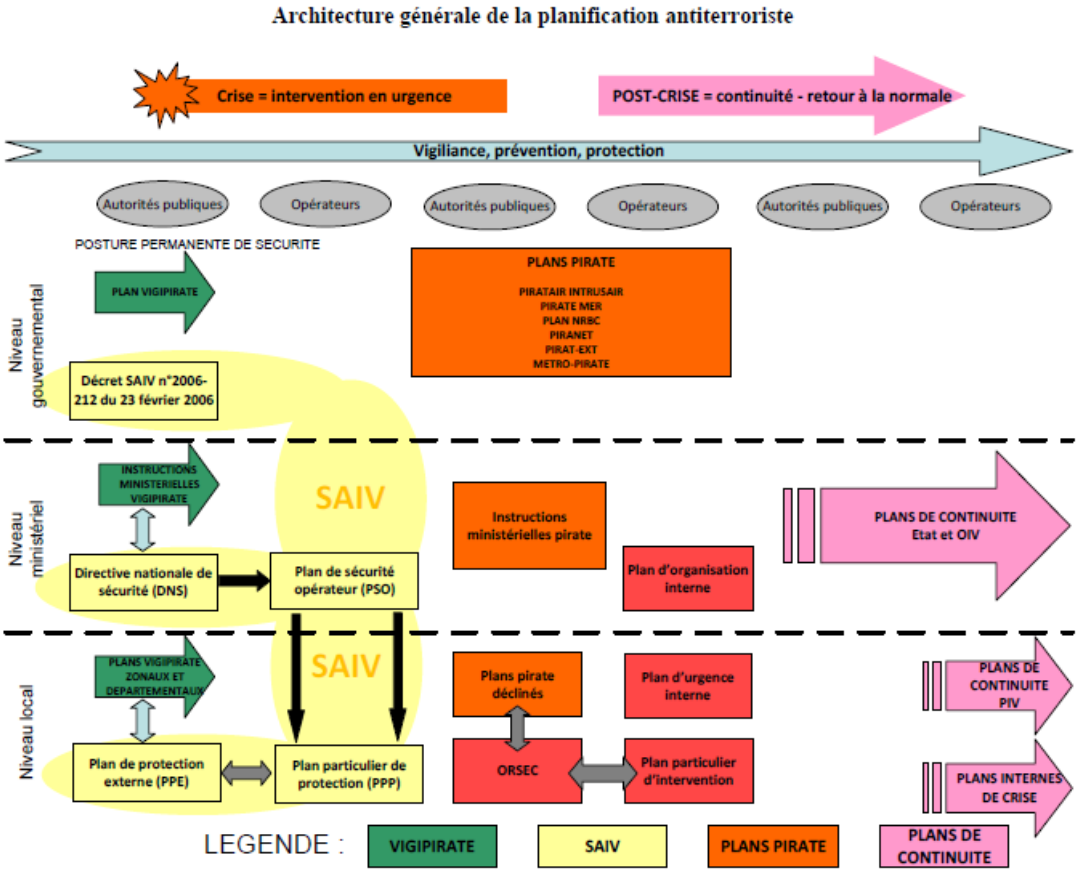

Figura 4. Fuente*: L'instruction générale interministérielle n° 6600/SGDSN/PSE/PSN relative à la sécurité des activités d'importance vitale (SAIV) du 7 janvier 2014.*

La *Instruction générale interministérielle* define los sectores de las IC:

- Activités civiles de l'Etat (ACE).
- Activités judiciaires.
- Activités militaires de l'Etat (AME).
- Alimentation.
- Communications électroniques, audiovisuel et information.
- Energie.
- Espace et recherche.
- Finances.
- Gestion de l'eau.
- Industrie.
- Santé.
- Transports.

Por último señañar que en Francia se han creado reglamentariamente órganos implicados en la protección de IC como es el *Conseil de politique nucléaire*[56] o la *Agence nationale de la sécurité des systèmes d'information*[57], impleméntadose una regulación más exhaustiva mediante circulares e instrucciones como la *Circulaire relative à la doctrine nationale d'emploi des moyens de secours et de soins face à une action terroriste mettant en oeuvre des matières radioactives, 18/02/2011 (800/SGDSN/PSE/PPS)* u otras relativas a la protección de información clasificada[58].

El sistema francés es muy similar al nuestro, ambos coinciden en aspectos básicos como los planes de protección que equivalen a los españoles, como hemos señalado anteriormente, o la coordinación de la protección de las IC con los diferentes planes de prevención antiterroristas y además, ambos se sustentan sobre la base la colaboración público-privada e interministerial.

4.9 Bélgica.

El sistema de protección de IC belga se configura principalmente en la *Loi 01/07/2011 - Sécurité et protection des infrastructures critiques*[59]*, buena parte de cuyo* articulado coincide con los mandatos de la Directiva 114/2008/CE. La citada Ley ha sido posteriormente desarollada reglamentariamente a través de las siguientes normas:

- Subsector del transporte aéreo: *AR 02/12/2011 - Les infrastructures critiques dans le sous-secteur du transport aérien*[60].
- Sector de la energía: *AR 11/03/2013 - La sécurité et la protection des infrastructures critiques pour le secteur de l'Energie*[61].

---

[56] Décret n° 2008-378 du 21 avril 2008 instituant un conseil de politique nucléaire (article 2). Documento: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000018685579

[57] Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé "Agence nationale de la sécurité des systèmes d'information". Documento: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000020828212

[58] Instruction interministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), 22/10/2013 (910/SGDSN/ANSSI). Documento: http://circulaire.legifrance.gouv.fr/pdf/2013/11/cir_37647.pdf

[59] LOI 01/07/2011 - Sécurité et protection des infrastructures critiques. Documento: http://centredecrise.be/sites/5052.fedimbo.belgium.be/files/loi_du_1er_juillet_2011_sur_les_ic_0.pdf

[60] AR 02/12/2011 - Les infrastructures critiques dans le sous-secteur du transport aérien. Documento: http://centredecrise.be/sites/5052.fedimbo.belgium.be/files/kb_2_december_2011_betreffende_luchtvervoer.pdf

- Subsector de los puertos: *AR 29/01/2014 - La sécurité et la protection des infrastructures critiques dans le sous-secteur des ports*[62].
- Sector de telecomunicaciones: *AR 27/05/2014 - Arrêté royal portant exécution dans le secteur des communications électroniques de l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques*[63].
- Sector de transporte y subsector de transporte ferroviario: *AR 19/02/2016 - Sécurité et prévention des infrastructures critiques, pour le secteur du transport, sous-secteur du transport ferroviaire*[64].

En cuanto a los centros y órganos que participan directa o indirectamente en la protección de las IC belgas son los siguientes:

- *Direction générale Centre de Crise du Service public fédéral Intérieur* (DGCC): *Le Centre de Crise* es el agente más importante en la protección de las IC que no tiene centro propio, sino que forma parte de las muchas tareas de las que se encarga este centro. Éste se encarga de la protección de los bienes y personas y de la coordinación nacional en materia de orden público.
- *Organe de Coordination pour l'Analyse de la Menace* (OCAM) que se encarga de analizar las amenazas a nivel nacional.

Los sectores en los que se agrupan las IC son cuatro:

- Énergie.
    - Électricité.
    - Pétrole.
    - Gaz.
- Transport.
    - Transport par route.
    - Transport ferroviaire.
    - Transport aérien.
    - Navigation intérieure.
    - Transport hauturier et transport maritime à courte distance et ports.
- Finances.
- Communication électronique.

Las medidas previstas en la *LOI 01/07/2011* tienen por objeto la prevención de incidentes que puedan dañar o afectar al suministro proporcionado por las IC, sin embargo en materia de planificación de emergencias y gestión de la crisis, la ley remite a otras disposiciones legales y reglamentarias.

---

[61] AR 11/03/2013 - La sécurité et la protection des infrastructures critiques pour le secteur de l'Energie. Documento:http://centredecrise.be/sites/5052.fedimbo.belgium.be/files/kb_11_maart_2013_betreffende_energie.pdf

[62] AR 29/01/2014 - La sécurité et la protection des infrastructures critiques dans le sous-secteur des ports. Documento: http://centredecrise.be/sites/5052.fedimbo.belgium.be/files/kb_29_januari_2014_betreffende_havens.pdf

[63] AR 27/05/2014 - Arrêté royal portant exécution dans le secteur des communications électroniques de l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques. Documento: http://centredecrise.be/sites/5052.fedimbo.belgium.be/files/ar_27_05_2014_-_la_securite_et_la_protection_des_infrastructures_critiques_dans_le_secteur_des_communications_electroniques.pdf

[64] AR 19/02/2016 - Sécurité et prévention des infrastructures critiques, pour le secteur du transport, sous-secteur du transport ferroviaire. Documento: http://centredecrise.be/sites/5052.fedimbo.belgium.be/files/ar_19022016.pdf

5. CONCLUSIONES.

Las infraestructuras críticas pueden ser y son objetivos tanto de ataques físicos como de ataques a través de la red y pueden sufrir las consecuencias de catástrofes naturales. La situación de inestabilidad que estamos viviendo en los últimos tiempos ha provocado una avalancha de riesgos y amenazas que requieren de una protección eficiente. El Sistema de Seguridad Nacional debe proporcionar los recursos, mecanismos y planes necesarios para afrontar con éxito esta problemática.

Nuestro SPIC, al igual que en la mayoría de los países estudiados, es un sistema complejo que requiere la actuación de numerosos agentes y que se sustenta sobre el principio de coordinación y cooperación público-privada[65]. Existen bastantes similitudes entre los países pertenecientes a la UE y esto se debe a las Directiva europea, cuyo objetivo fundamental era que los Estados miembros crearan sistemas de protección para las IC o que se realizaran las modificaciones pertinentes en las ya existentes, para que fueran homogéneas.

El análisis de la normativa española permite afirmar que la misma cumple con lo demandado por la Directiva 114/2008/CE: la Ley 8/2011 describe los agentes e instrumentos que participan en el Sistema de protección de IC y sus actividades, que luego son desarrolladas en el posterior reglamento.

El sistema de protección de IC más complejo de todos los estudiados es el estadounidense. Es el que mayor cantidad de agentes tiene que coordinar, pues cuenta con diversas agencias y órganos implicados en la protección de las IC, llegando incluso a tener dos centros nacionales de protección de las mismas, lo que provoca que existan ciertas duplicidades en las funciones atribuidas a algunos de ellos y, sobre todo, dificulta la coordinación de todos los agentes, a cuyos efectos se prevén órganos descentralizados para la coordinación a nivel local, territorial y federal. El sistema canadiense se asemeja bastante al estadounidense, aunque es menos extenso y más simple en lo que a números de agentes y órganos de coordinación se refiere. Los sistemas español, francés y japonés son más sencillos que el estadounidense, su estructura resulta más simple y, a priori, la información pasa por canales más fluidos, acortando los tiempos de reacción ante las amenazas.

De los países de la UE estudiados, el que menos ha desarrollado normativamente sus sistemas de protección de IC es Bélgica, cuya *Loi 01/07/2011 - Sécurité et protection des infrastructures critiques* resulta bastante esqjuemática e incompleta a la hora de establecer planes e instrumentos de actuación a diferentes niveles. Por ello cabe presumir que la colaboración con Bélgica en este ámbito puede resultar más complicada por no haber llevado a cabo todas las exigencias de la UE en materia de protección de IC. También resulta preocupante que en Bélgica solo se designen cuatro sectores de IC siendo estos la energía, el transporte, economía y comunicaciones electrónicas, número bastante reducido en comparación con el resto de países analizados (Australia, el siguiente de los países s con menor número, cuenta con nueve sectores). Esta incompleta regulación en materia de seguridad y protección de IC, unida a otros factores como los problemas de coordinación entre los diferentes cuerpos policiales existentes en

[65] SÁNCHEZ GÓMEZ, F.J., "Protección de infraestruturas críticas: conceptos básicos" En DE TOMÁS MORALES, S. (Coord), *Retos del derecho ante las nuevas amenazas*, Dykinson, Madrid, 2015.

Bégica y el ser el país con mayor proporción de yihadistas en Europa Occidental[66] pueden explicar en cierto modo la facilidad con la que se perpetraron los ataques en el aeropuerto y en el metro del 22 de marzo de 2016[67] (no debemos olvidar que tanto los aeropuerto como los metros son IC que forman parte del sector del transporte).

Otro aspecto destacable es la necesidad de mantener acuerdos de protección de las IC con otros países, como ocurre en Europa y como ocurre entre EE.UU. y Canadá. Las directivas europeas y el *Canada-United States Action Plan for Critical Infrastructure* son ejemplos palpables de los esfuerzos que están realizando los Estados para coordinarse en materia de protección de IC y de la interdependencia entre las mismas a diferentes lados de las fronteras. La naturaleza interconectada de las IC hace que en muchos casos, la caída del servicio de una de ellas, pueda suponer la caída en cadena de otras, inclusive las que se encuentran fuera de las fronteras del país en el que se encuentren. Conscientes de ello, los Estados han dedicado muchos esfuerzos a crear planes que permitan la protección de éstas a nivel internacional. España necesariamente debe coordinarse con los países de la UE como obliga la Directiva 114/2008/CE por la presencia de ICE en nuestro país, que son infraestructuras críticas cuyo corte del suministro produciría daños en al menos dos países miembros de la UE. Además, se realizan colaboraciones a nivel policial y con los servicios secretos de otros países, que recíprocamente se proporcionan información necesaria para mantener la seguridad. Un rasgo común a todos los sistemas de protección de IC es la colaboración con los servicios de inteligencia de sus respectivos países: estos participan de un modo activo en la protección de las IC, proporcionando información y alertas sobre las amenazas que puedan afectarlas. La alerta temprana permite preparar y actuar de forma más eficaz para prevenir cualquier incidente. Recordemos que de la prevención es la base sobre la que se debe asentarse cualquier sistema de protección de IC eficiente.

Prácticamente todas las estrategias y documentos referentes a las infraestructuras críticas hacen referencia a la protección física y lógica, excepto la *National Guidelines For Protecting Critical Infrastructure From Terrorism* australiana que hace referencia exclusivamente a ataques de tipo físico en atentados terroristas. Hoy en día es mucho más probable y "rentable", si se nos permite la expresión, que se produzca un ataque informático o ciberataque a una IC a que se produzca un ataque tradicional (por ejemplo, un bombardeo o una catástrofe que destruya físicamente edificios o equipamientos, pues como bien se indica en el informe del S2 Grupo sobre las IC:

> "Desde el punto de vista del atacante, el ataque remoto puede parecer más beneficioso: el riesgo asumido por el atacante o atacantes es casi nulo si operan correctamente, ya que será casi imposible localizarlos e identificarlos, y además el ataque remoto puede ser incluso más barato que el físico y tanto o más efectivo que éste"[68].

Muy interesante nos ha parecido la mención expresa en la *National Guidelines For Protecting Critical Infrastructure From Terrorism* a la necesidad de mejorar la relación entre el gobierno australiano y los medios de comunicación en materia de terrorismo. Los ciudadanos han de confíar en su gobierno y sus sistemas en la lucha antiterrorista,

---

[66] Información publicada por la agencia de noticias *BBC* el día 17 de enero de 2015, disponible en: http://www.bbc.com/mundo/noticias/2015/01/150116_internacional_belgica_yihadistas_nc

[67] Información publicada por el diario El Mundo el día 23 de marzo de 2016, disponible en: http://www.elmundo.es/internacional/2016/03/22/56f0f2cf22601d20498b4648.html

[68] S2GRUPO. Protección de Infraestructuras Críticas 2011 [pdf]. Disponible en: «http://s2grupo.es/wp-content/uploads/2016/01/Informe_PIC2011_S2Grupo.pdf»

ya que uno de los objetivos del terrorismo es minar dicha confianza. El derecho a la información es un derecho fundamental que debe ser garantizado en todas las sociedades democráticas y la materia que nos ocupa no puede constituir una excepción absoluta al mismo, la ciudadanía tiene derecho a estar informada, a saber qué hace el Estado en materia de seguridad y cómo lo hace, contribuyéndose así al buen funcionamiento de la democracia. El límite a este derecho debe ser no proporcionar información, datos concretos o información clasificada sobre IC u operaciones que se estén llevando a cabo por las Fuerzas de Seguridad, ya que puede suponer un grave perjuicio a la seguridad nacional. Pero la divulgación y difusión en los medios de comunicación de estadísticas y aspectos muy generales sobre IC puede ayudar a fomentar la cultura de la seguridad. En España es difícil encontrar en los medios de comunicación de masas información sobre las IC, para ello es preciso acudir a revistas especializadas en seguridad, notas de prensa y declaraciones de miembros del Ministerio del Interior. Por tanto, todos los países analizados y España deben mejorar en este aspecto e incluir en sus estrategias y planes una referencia a los medios de comunicación como ocurre en Australia, que reportará beneficios desde el mismo momento en que se lleve a cabo.

Por último, no hay que olvidar la importancia de ir cambiando los sistemas y planes de protección de IC para adecuarlos a los nuevos retos que van surgiendo en el marco de la protección de las mismas y, en definitiva, de la seguridad nacional. Es por ello que los Estados deben ir renovándolos cuando sus medidas se quedan obsoletas o se descubren fallos en los mismos. España en este 2016 prevé la instrucción del nuevo Plan Nacional de Protección de IC, aprobado en febrero por la Secretaría de Estado de Seguridad, en cuya presentación Francisco Martínez, Secretario de Estado de Seguridad, subrayó que el mismo "va a servir para fortalecer el sistema de seguridad nacional de manera alineada con el Plan Nacional de Prevención Antiterrorista", puesto que "contempla la seguridad de forma integral"[69]. Pese a que el texto está clasificado, se conoce que los cambios están orientados a la mejora e inclusión de medidas de ciberseguridad y a la adquisición y concreción de nuevas obligaciones para los operadores críticos. Además en este plan se "homogeneíza las medidas operativas que contiene el Plan de Prevención y Protección Antiterrorista, identificándose con los niveles de alerta consignados en este último"[70].

En definitiva, todos los implicados en la protección de las IC deben colaborar a la hora de mejorar los sistemas. También es necesaria la participación de la comunidad científica especializada en materia de seguridad, pues, como ya hemos señalado, no existe en España demasiada bibliografía sobre las IC, y son muchas las líneas de investigación posibles en relación a las mismas (aun teniendo la dificultad que supone el hecho de que gran parte de la información esté clasificada como secreta: tanto estudios cualitativos como cuantitativos sobre la efectividad de los planes que se llevan a cabo, la eficacia en la reacción en caso de amenaza, la proporcionalidad de las actuaciones realizadas, etc. Estas investigaciones podrían contribuir a la mejora de los sistemas de protección de IC en nuestro país.

---

[69] Información extraída de la web del Ministerio del Interior, disponible en: http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/5721143

[70] Información publicada en la web de la revista especializada Red Seguridad el 7 de marzo de 2016, disponible en: http://www.redseguridad.com/actualidad/info-tic/interior-adapta-el-pnpic-a-la-normativa-con-una-nueva-version

6. BIBLIOGRAFÍA

- ANDRESS, J. y WINTERFELD, S., *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2ª ed., Syngress-Elsevier, Waltham, 2013.

- CARO BEJARANO, M.J., La protección de las infraestructuras críticas [PDF]. Disponible en: «http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf»

- CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM. Critical Infrastructure Protection against Terrorist Attacks [pdf]. Disponible en: http://www.coedat.nato.int/publication/course_reports/12-CIP.pdf

- CONSEJO DE MINISTROS. Estrategia de Seguridad Nacional, un proyecto compartido [pdf]. Disponible en: «http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf»

- CORREA HENAO G.J. y YUSTA LOYO J.M., "Seguridad Energética y Protección de Infraestructuras Críticas", *Lampsakos*. Jul-dic. 2013, núm. 10.

- DE LA CORTE IBÁÑEZ, L.; BLANCO NAVARRO, J.M. (Coords), *Seguridad nacional, amenazas y respuestas*, Lid, Madrid, 2014.

- DE TOMÁS MORALES, S. (Coord), *Retos del derecho ante las nuevas amenazas*, Dykinson, Madrid, 2015.

- GUINEA,M., "La estrategia de seguridad nacional 2013: Una evaluación desde la perspectiva de la pertenencia a la Unión Europea" *UNISCI Discussion Papers*. May. 2014, núm. 35.

- MIRANZO,M.; DEL RÍO,C., "La protección de infraestructuras críticas" *UNISCI Discussion Papers*. May. 2014, núm. 35.

- MURRAY, A.; GRUBESIC, T., "Critical infrastructure protection: The vulnerability conundrum" *Telematics and Informatics*. Feb 2012, núm 29.

- QUIGLEY, K., ""Man plans, God laughs": Canada's national strategy for protecting critical infrastructure", *Canadian Public Administration.* Mar 2013, Núm 56, pp 142-164.

- REVISTA SEGURITECNIA . Entrevista a Fernando Sánchez Gómez [en línea]. Disponible en: «http://www.seguritecnia.es/seguridad-aplicada/infraestructuras-criticas/el-espiritu-de-la-normativa-pic-se-basa-en-la-confianza-mutua-y-en-la-confidencialidad-de-la-informacion-que-se-comparte»

- Second Action Plan on Information Security Measures for Critical Information Infrastructure. February 3, 2009, Information Security Policy Council. Disponible en: «http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf»

- S2GRUPO. Protección de Infraestructuras Críticas 2011 [pdf]. Disponible en: «http://s2grupo.es/wp-content/uploads/2016/01/Informe_PIC2011_S2Grupo.pdf»

- The Basic Policy of Critical Information Infrastructure Protection (3rd Edition). May 19, 2014, Information Security Policy Council. Disponible en: «http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf»

- The Second National Strategy on Information Security. February 3, 2009, National Information Security Policy Council. Disponible en: «http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf»