Protección de Infraestructuras Críticas 2011

S2 GRUPO

Sobre S2 Grupo

S2 Grupo, fundada en 1999, es la primera empresa de la Comunidad Valenciana especializada en servicios globales de seguridad digital. La compañía prevé cerrar 2011 con una facturación de 3,85 millones de euros, lo que refleja un crecimiento del 21% respecto al ejercicio anterior, motivado por un aumento de la cartera de clientes y de la actividad de innovación. La inversión en I+D+i es uno de los ejes vertebradores de la compañía que en 2011 ha destinado 1,2 millones de euros a diferentes proyectos nacionales y europeos, lo que supone un 30% de su facturación.

Datos de contacto

S2 Grupo
Ramiro de Maeztu 7, 46022 Valencia
T 963110300 # **F** 963106086

Orense 85, Ed. Lexington. 28020 Madrid.
T 915678488 # **F** 915714244

Autores

Han colaborado en el presente informe

Antonio Villalón

José Miguel Holguín

Nelo Belda

José Vila

Diseño y maquetación

Manuel Benet

Fecha de publicación

Diciembre 2011

Este informe puede descargarse de la página web de S2 Grupo, **http://www.s2grupo.es**, del blog de seguridad Security Art Work, **http://www.securityartwork.es**, o solicitándolo por correo electrónico a **admin@securityartwork.es.**

La protección de infraestructuras críticas es tan antigua como la propia humanidad; aunque sin denominarlo formalmente PIC, gobiernos y ejércitos de todo el mundo han tratado de defender a toda costa los elementos que consideraban más importantes en cada ocasión, desde los sistemas de abastecimiento de agua o alimento hasta las vías de comunicación o ubicaciones físicas más importantes para el grupo (entendiendo grupo por tribu, imperio, reino, gobierno…).

En pleno siglo XXI la preocupación histórica por la seguridad y la defensa de estas infraestructuras sigue tan vigente como en el antiguo imperio romano. A los componentes de seguridad “clásicos”, como la protección mediante personas frente a ataques físicos del enemigo, se han añadido estos años componentes de seguridad menos habituales, fruto de la convergencia de la seguridad de la que tanto se ha venido a hablar durante la primera década del siglo.

Dicho de otra forma, si hace dos mil años la única manera de atacar una infraestructura crítica era mediante el uso de ejércitos a pie o caballo, o si hace cincuenta años la única forma de hacerlo era mediante ejércitos con tanques, barcos y aviación, hoy en día a estas tres armas se une un punto de vista adicional: el de la ciberguerra. O el del ciberterrorismo. O simplemente, el del cibervandalismo. Acciones clásicas con el prefijo “ciber”, que viene a decir que se desarrollan a través de redes de computadores.

Sin un despliegue de miles de hombres y sin un nivel de riesgo considerable para el atacante, estas acciones pueden llegar a sustituir a —o al menos, convivir con— las anteriores, constituyendo un nuevo escenario de seguridad y defensa que preocupa a todos los estados del mundo: el de la ciberseguridad y ciberdefensa, en especial en lo relativo a protección de infraestructuras críticas, que como decíamos al principio es quizás el aspecto que más nos debe preocupar a todos.

Debemos ser conscientes de que la separación entre el ámbito “real” y el “virtual” está cada vez más difuminada, en lo que se ha venido a llamar **convergencia** de la seguridad; este concepto, que aunque data de 1997 recibió su mayor impulso tras los atentados del 11-S en Nueva York, se basa en una idea muy sencilla: la amenaza contra una nación se materializará de la forma que más sencilla le sea, sin importar si su ámbito es físico o lógico, y por tanto la gestión de la seguridad nacional debe realizarse desde un punto de vista holístico, capaz de garantizar tanto la protección física como la virtual de las infraestructuras críticas.

Antecedentes

Si como hemos dicho la preocupación por las infraestructuras críticas ha estado presente a lo largo de toda la historia de la humanidad, no es hasta finales del siglo pasado cuando se empieza a hablar de forma explícita de la protección de tales infraestructuras.

En la *Presidential Decision Directive* (PDD) 39, "*U.S. Policy on Counterterrorism*", de 21 de junio de 1995, ya se menciona la protección frente a ataques terroristas contra los EEUU que se produzcan dentro y fuera del territorio estadounidense. La directiva hace énfasis en las armas de destrucción masiva, las armas nucleares y químicas, y la piratería aérea [1].

> ***"They may try to attack our economy and critical infrastructure using advanced computer technology."*** [2]

Ese año aún no se entra a tratar temas de ciberprotección; no es hasta tres años más tarde, en la PDD 62, "*Combating Terrorism*", y la PDD 63 "*Protecting America's Critical Infrastructures*", ambas de 22 de mayo de 1998, cuando se hace una mención explícita —y en un mismo documento— a la protección de infraestructuras críticas y a los sistemas informáticos en las que éstas se apoyan. En la PDD 62 se crea la figura del *National Coordinator for Security, Infrastructure Protection and Counterterrorism*, y las tareas presentes en la PDD 63 servirán de base para lo que se conocerá más tarde como el **ciclo de vida de la PIC** [2][3][4].

Tres años más tarde, el 11 de septiembre de 2001, se produce el atentado contra las Torres Gemelas, que sin duda marca un antes y un después para todos los que trabajamos en seguridad. Un ataque desconocido hasta el momento con todos los ingredientes necesarios para sorprender, impactar y dañar desde múltiples puntos de vista al enemigo. Un ataque que puso de manifiesto que la gran potencia mundial que es EE.UU. tenía fisuras de seguridad muy graves y que grupúsculos terroristas podían aprovecharlas —podríamos decir incluso que fácilmente— para dañar de forma irreparable al país. Un ataque que nos obligó a todos a plantearnos qué estábamos haciendo mal, a todos los niveles, para que algo así pudiera haber llegado a suceder. Como supimos más tarde, nos encontrábamos ante un punto de inflexión en la seguridad y defensa cuyas consecuencias siguen, a día de hoy —y han pasado más de diez años, lo que en seguridad es mucho tiempo— vigentes y visibles a lo largo y ancho del mundo civilizado.

Evidentemente, todos estos movimientos tienen una causa justificada: el incremento del riesgo asociado a ataques "tecnológicos" contra infraestructuras críticas. Repasando la cronología de los principales ciberataques contra en este sentido —al menos de los públicamente conocidos—, podemos comprobar que van a la par que las iniciativas de protección. De hecho, no es hasta la segunda mitad de los años 90 cuando el

problema empieza a considerarse realmente serio; hasta entonces, quizás lo más destacable es la introducción (junio de 1982, en plena guerra fría) de un troyano para sabotear las tuberías de gas natural de la antigua URSS. A finales de los 90 comienzan a aparecer problemas de seguridad en entornos SCADA, hasta entonces sistemas aislados de la red pero que tras el *boom* de Internet empiezan a conectarse a ésta manteniendo la mentalidad —desde el punto de vista de seguridad— del sistema aislado que hasta ese momento habían sido.

En el año 2000 un ex-empleado de una planta de aguas residuales australiana la ataca de forma inalámbrica; un buen ejemplo del "*insider threat*" como ciberataque —de los primeros en el ámbito civil— a una infraestructura crítica. Tres años más tarde, y como ejemplo adicional de problemas derivados de la conexión a Internet de sistemas que están diseñados para trabajar de forma aislada, el gusano Slammer provoca el apagado de la central nuclear de Davis-Besse. En la segunda mitad de la década las publicaciones que describen vulnerabilidades en entornos SCADA se comienzan a distribuir libremente en Internet, incluyendo (2007) el famoso vídeo "*Aurora vulnerability*" en el que se sabotea un generador… A partir de aquí la palabra "ciberataque" aparece con mucha frecuencia junto a "infraestructura crítica": en enero de 2008 la CIA informa que un ciberataque ha causado la pérdida de electricidad en varias ciudades en una localización desconocida fuera de USA, en junio de 2010 salta a los medios generalistas el descubrimiento de Stuxnet… hasta septiembre de 2011, cuando el que ha saltado a los medios generalistas ha sido Duqu, ambos considerados *malware* muy avanzado capaz de poner en jaque —real, ya no hablamos de hipótesis o estudios teóricos— infraestructuras críticas y, por tanto, vidas humanas.

Situación Internacional

El panorama estadounidense

Como hemos indicado, los atentados del 11S contra las Torres Gemelas neoyorquinas constituyeron un antes y un después en el enfoque de seguridad y defensa del mundo occidental. Pero la preocupación por la seguridad nacional del gobierno estadounidense era previa a estos atentados, y tuvo como reflejo una directiva presidencial por parte del presidente Bill Clinton el 20 de mayo de 1998 por la que instaba a todas las entidades privadas que formaban parte de la infraestructura crítica de la nación a compartir información sobre amenazas, vulnerabilidades, incidentes y soluciones y respuestas dentro de estos sectores críticos: la famosa **PDD 63** (*Presidential Decision Directive 63*); en esta misma directiva se definen los **ISAC**, centros modelo en la protección de infraestructuras críticas mediante la colaboración y el intercambio de información de los que hablaremos en este mismo informe.

Tras el 11S, algo que se intuía y que posteriormente se constataría de manera oficial, es la dispersión de las agencias y organismos que podrían haber evitado el atentado, actores que no compartían ni correcta ni completamente la información antiterrorista de la que disponían.

Apenas un mes después de los atentados, el 8 de octubre de 2001, el gobierno estadounidense constituye la *Office of Homeland Security* con el fin de aunar los esfuerzos en materia de seguridad dentro del propio territorio y menos de una semana más tarde, el 26 de octubre de ese mismo año, se firma el *USA Patriot Act*. Ambas acciones constituyen el embrión de lo que iba a ser la nueva protección nacional no sólo en los EE.UU., sino en todo el mundo occidental.

Un año después, el 25 de noviembre de 2002, dentro del marco del *Homeland Security Act*, se crea el *Department of Homeland Security* con el fin de aglutinar las diferentes agencias ocupadas de la seguridad dentro del propio territorio; recordemos lo indicado con anterioridad: uno de los problemas raíz del 11S fue, sin duda, la dispersión de agencias y organismos encargados de velar por la seguridad nacional. Actualmente, las siguientes agencias relacionadas con la protección de infraestructuras críticas están incluidas dentro del Departamento: *Infrastructure Protection and Security Directorate*, *Transportation Security*

Administration, *US-CERT*, *Office of Cybersecurity and Communications* y *Office of Infrastructure Protection*.

Posteriormente, ya en diciembre de 2003, el gobierno estadounidense publicó la **HSPD 7** (*Homeland Security Presidential Directive 7*), "*Critical Infrastructure Identification, Prioritization, and Protection*", que actualiza la anterior PDD 63 (que recordemos data de 1998, previa a los atentados) con respecto al *USA Patriot Act*, y establece una política nacional para las agencias y departamentos federales cuyo objetivo es (como el propio nombre indica) la identificación, priorización y protección de las infraestructuras críticas.

El panorama europeo

En especial a raíz de los atentados del 11M, la Comisión Europea (CE) quiso mejorar la seguridad en diferentes tipos de infraestructuras de la UE que considera "críticas", para lo que presentó un programa de acciones que van desde la elaboración de normas al apoyo a los estados miembros para identificarlas. Franco Frattini, recordó en un comunicado que "*la seguridad y la economía de la UE, así como el bienestar de los ciudadanos están ligados a ciertas infraestructuras y servicios*". Frattini afirmó que "*la*

interrupción de las mismas podría provocar la pérdida de vidas humanas y de bienes materiales, así como la merma de la confianza de los ciudadanos en la UE".

De esta forma, y en la línea de actuación contra los ataques terroristas, se han desarrollado sucesivas directivas al respecto que se han ido publicando en los últimos años. La primera de estas directivas es la **COM/2004/0698**, "*Prevención, preparación y respuesta a los ataques terroristas*", en la que se definen una serie de objetivos primarios para encauzar el tratamiento de los actos terroristas y prevenirlos, así como para proteger infraestructuras críticas y dificultar la financiación del terrorismo. En este sentido se indica que los esfuerzos deben ser integradores e inclusivos, involucrando a parlamentos, agentes económicos, organizaciones civiles, y todos los ciudadanos europeos. También se debe promocionar un "diálogo de seguridad" entre los sectores público y privado, para aumentar la efectividad en este ámbito. En todos estos aspectos, la Unión Europea tratará de proveer, adaptar y unificar los canales de comunicación entre entidades, para que se consiga un intercambio de información eficaz. Dado el carácter global del terrorismo, se destaca también que la Unión Europea debe fomentar, dentro de su política de asuntos exteriores, una colaboración en el ámbito antiterrorista con entidades y organizaciones del resto del mundo. Así mismo, en esta directiva se indica que se debe proteger y asegurar con especial recelo el uso de elementos que pueden ser potencialmente utilizados como armas terroristas. Dentro de este grupo se incluyen armas de fuego, explosivos, material para la fabricación de bombas, así como cualquier tecnología que contribuya a perpetrar actos terroristas.

Por su parte, la directiva **COM/2004/0701**, titulada "*Lucha contra el terrorismo: preparación y gestión de las consecuencias*", se centra en enumerar los elementos clave en la gestión de una situación de emergencia provocada por un ataque terrorista. En primer lugar, se extiende el funcionamiento del Centro de Control e Información (MIC), para coordinar también las solicitudes y el despliegue de las ayudas entre el país que ha sufrido el ataque terrorista y el resto de países de la Unión. Al igual que en la anterior, se sigue haciendo hincapié en que se deben aumentar, agilizar y estrechar los lazos de colaboración entre agencias de los estados miembros. En este aspecto se enumeran agencias de protección civil y seguridad sanitaria, fomentando en todos los casos la colaboración mutua e interoperabilidad.

Además, se destaca la importancia que tiene la correcta formación de expertos que puedan facilitar la coordinación y resolución de estos problemas, así como el estudio e investigación en todos los campos, para aportar nuevas medidas y estrategias en la lucha antiterrorista. Aquí se considera esencial la realización de cursos de formación y ejercicios de simulación a nivel europeo, así como la investigación en temas de seguridad sanitaria. Para facilitar la gestión de emergencias, en esta directiva se establece también la creación y puesta a disposición de la Unión de una base de datos de activos y capacidades militares, y otra en el ámbito civil, para la protección de la población contra los efectos de cualquier tipo de ataque terrorista. También se indica que la Comisión creará un sistema europeo general seguro de alerta rápida (ARGUS) para conectar todos los sistemas de emergencia especializados que requieren una actuación a nivel europeo, como punto de encuentro y gestión centralizado; el principal eslabón ausente de los actuales sistemas de respuesta rápida (RAS) gestionados a nivel de la UE es un sistema de alerta referente al orden público y a la seguridad en lo relativo tanto a la preparación como a la respuesta a crisis que implican a los servicios represivos.

La directiva **COM/2004/0702**, titulada "*Protección de las infraestructuras críticas en la lucha contra el terrorismo*" se centra, por fin, en las infraestructuras críticas. En ella se define en primer lugar la amenaza que supone un ataque terrorista para ciertas infraestructuras de los miembros de la Unión. Posteriormente se define lo que se considera como infraestructura crítica y las métricas que se utilizarán para definir la criticidad exacta de estas infraestructuras. Para llevar un control de seguridad adecuado, se contempla la creación de un procedimiento para hacer un inventario y clasificación de infraestructuras críticas, así como para alcanzar un punto de vista común que permita mejorar las medidas de protección de las infraestructuras más importantes. Algunas de ellas no pueden ser controladas al 100% (por ejemplo, las redes eléctricas), por lo que se deben definir puntos de máximo riesgo, sobre los que se centrará la protección. En esta directiva se indica también que se ha avanzado notablemente en la mejora y protección de las infraestructuras críticas "tradicionales", legislándose tanto a nivel nacional como europeo medidas de protección al respecto; en el campo de la seguridad de las comunicaciones, más novedoso y poco protegido hasta el momento, se crea ENISA (Agencia Europea de Seguridad de las Redes y de

la Información), un organismo europeo para la seguridad de la información: la Unión Europea considera las redes de comunicaciones y los sistemas informáticos esenciales para el desarrollo de la economía y la sociedad, por lo que la seguridad de las comunicaciones y los sistemas de información es considerada de especial interés y parte de la infraestructura crítica de servicio a los ciudadanos. Por todo ello, las actividades de la agencia ENISA están dirigidas a ser un centro de excelencia en el campo de la seguridad de la información

En la directiva se propone además la creación del Programa Europeo de Protección de las Infraestructuras Críticas (PEPIC, EPCIP en sus siglas en inglés), que ayudará a las empresas y administraciones públicas de los estados miembros a armonizar y coordinar esfuerzos en temas de seguridad de infraestructuras críticas. Para ello, seguirá con la identificación de infraestructuras críticas, sus vulnerabilidades e interdependencias, y presentará soluciones de protección y preparación ante cualquier tipo de peligro. Se hace especial hincapié en esta directiva, una vez más, en el intercambio de información: se anuncia la creación de la Red de Información sobre Alertas en Infraestructuras Críticas (CIWIN), que agrupa a todos los especialistas en PIC de los estados miembros y fomenta el intercambio de información tanto sobre amenazas comunes como sobre medidas de atenuación de riesgos, permitiendo asesorar a los estados miembros a la hora de valorar qué infraestructuras pueden considerar críticas; sobre esta cuestión, un experto comunitario subrayó en rueda de prensa que son "los estados los que deben sugerir qué infraestructuras son críticas en sus territorios".

Ya en 2005 la Unión Europea publica la directiva **COM/2005/0576**, denominada el "*Libro Verde Sobre un programa europeo para la protección de infraestructuras críticas"*. Este documento propone opciones para PEPIC con el objeto de asegurar unos niveles adecuados y equivalentes de seguridad en infraestructuras críticas para los distintos estados miembros, según las repercusiones, y siguiendo el principio de proporcionalidad de costes. Propone la definición de unos principios básicos como pueden ser los de subsidiariedad o cooperación y establece un marco común de protección para garantizar unos niveles adecuados con medidas horizontales en todos los agentes del Sistema. Como medidas más concretas, establece la necesidad de identificar las *Infraestructuras Críticas Europeas* (ICE) -

sin descuidar las *Infraestructuras Críticas Nacionales* (ICN) y la creación de un *Organismo de Coordinación Nacional del PIC* (OCNP), como organismo de supervisión único del PEPIC en los Estados. Asimismo, enumera las responsabilidades de los diferentes agentes del ICN o ICE haciendo especial hincapié en el PSO, llegando a incluir una propuesta de modelo. Por último, describe varias medidas de apoyo al PEPIC como pueden ser la creación de una *Red de información sobre alertas en infraestructuras críticas* (CIWIN), la definición de metodologías comunes de niveles de alerta entre los Estados miembros y otros temas, como la financiación o el control.

Posteriormente se publica **COM/2006/786**, "*Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas"*. A raíz del *Libro Verde sobre un Programa europeo para la protección de IC*, el *Consejo de Justicia e Interior* concluyó que la Comisión elaborara una propuesta de PEPIC, definiendo su objetivo como la mejora de la protección de las ICE mediante la creación de este marco de la UE donde establece un enfoque global de las amenazas, definiendo los principios fundamentales del PEPIC. El marco que propone consta de un procedimiento para identificar ICE, medidas para facilitar la aplicación del PEPIC, apoyo a los Estados miembros en sus ICN o medidas financieras complementarias, entre otros. También define la designación de un grupo de contacto de PIC comunitario que coordinará a los puntos de contacto nacionales. Como medidas para facilitar la aplicación del PEPIC, se establece un *plan de acción* organizado en tres líneas de actividad, la creación de la *Red de información sobre alertas en infraestructuras críticas* (CIWIN), creación de *grupos de expertos* con funciones y objetivos concretos, procedimientos para compartir información que ayude a protegerse de amenazas y vulnerabilidades. Asimismo, anima a la creación de programas nacionales de PIC con la propuesta de un contenido mínimo de éstos para garantizar que se siguen marcos similares para reducir costes y esfuerzos. Por último, se cita el *programa comunitario de prevención, preparación y gestión de las consecuencias del terrorismo y de otros riesgos relacionados con la seguridad* para el periodo 2007-2013, como medidas financieras que apoyen la adopción de estos planes y el desarrollo de instrumentos, estrategias y medidas, entre otros, en la protección de infraestructuras críticas.

Para finalizar el repaso al panorama europeo en la protección de

infraestructuras críticas, es necesario hablar, por supuesto, de la directiva **2008/114/CE**, aprobada en diciembre de 2008, que tiene por objeto establecer un procedimiento de identificación y designación de infraestructuras críticas europeas (en lo sucesivo, ICE) y un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras, con el fin de contribuir a la protección de la población. Esta directiva requiere a los estados miembros —entre los que obviamente se encuentra España— la adopción de medidas necesarias para dar cumplimiento a la misma de forma previa al 12 de enero de 2011 y proponiendo una revisión para el 12 de enero de 2012.

Aunque la directiva define conceptualmente las Infraestructuras Críticas, su desarrollo se centra en las Infraestructuras Críticas Europeas, es decir aquellas infraestructuras críticas cuya perturbación o destrucción afectaría a dos o más estados miembros.

De la lectura de esta directiva se desprenden dos conceptos principales: **colaboración** e **intercambio de información** entre diferentes actores, nacionales o europeos, con el fin de lograr los objetivos expuestos en la misma. El análisis de la introducción a la directiva determina lo siguiente:

> La responsabilidad principal y última de proteger las ICE corresponde a los Estados miembros y a los propietarios u operadores de dichas infraestructuras.
>
> Las ICE deben identificarse y designarse por un procedimiento común, y la evaluación de necesidades de seguridad de las mismas debe ejecutarse también con un planteamiento común de mínimos.
>
> Se fomenta la plena participación del sector privado en la PIC.
>
> En las ICE deben existir planes de seguridad del operador que incluyan la identificación de elementos relevantes, un análisis de riesgos y un documento de selección de controles (especificando identificación, selección y prioridad de salvaguardas).
>
> Cada ICE debe nombrar un responsable de enlace para la seguridad.
>
> Debe existir una comunicación fluida entre los propietarios y operadores de ICE, los Estados miembros y la Comisión Europea .
>
> Puede desarrollarse métodos comunes de identificación y clasificación de riesgos.
>
> Especialmente los Estados miembros deben facilitar a los propietarios u operadores de ICE códigos de mejores prácticas y métodos de protección de IC.

Deben designarse puntos de contacto para la PIC (puntos de contacto PICE) en cada Estado miembro.

El intercambio de información debe ser coherente y seguro, con las medidas de protección de la información adecuadas en cada caso y siempre en un entorno de confianza y seguridad.

En relación al análisis del desarrollo de la directiva, se determinan los siguientes aspectos destacables:

Identificación de ICE. Cada Estado debe identificar conforme al procedimiento establecido las ICE correspondientes a su territorio.

Designación de ICE**.** Cada Estado debe informar al resto que pueda verse afectado por una ICE potencial de la identidad de ésta y de los motivos de su designación, estableciendo conversaciones bilaterales o multilaterales con dichos países. También es necesaria la notificación anual a la Comisión y la notificación al propietario u operador.

Planes de seguridad del operador**.** Cada Estado velará para que las ICE dispongan de un Plan de Seguridad del Operador o equivalente, garantizando su aplicación en el plazo de un año tras la designación como ICE.

Responsables de enlace para la seguridad**.** Cada Estado velará para que las ICE dispongan de un responsable de enlace para la seguridad o cargo equivalente, garantizando que se dispone de esta figura en caso de que no exista previamente. También aplicará los mecanismos de comunicación adecuados entre la autoridad competente y el responsable de enlace para la seguridad.

Informes**.** Cada Estado llevará a cabo una evaluación de amenazas relativa a los subsectores de las ICE en el plazo de un año desde la designación como ICE, presentando cada dos años a la Comisión datos generales resumidos sobre riesgos en cada sector.

Puntos de contacto para la PICE**.** Cada Estado miembro designará un punto de contacto PICE.

Aplicación**.** Los Estados miembros adoptarán las medidas necesarias para cumplir lo establecido en la directiva antes del 12 de enero de 2011.

Esta directiva es la base de la **Ley de Protección de Infraestructuras Críticas** española, que analizaremos en el siguiente capítulo.

Centros para la Seguridad Nacional

La defensa de las infraestructuras de interés nacional ha hecho que los gobiernos fomenten la creación de centros de seguridad para la defensa de infraestructuras críticas. Aunque como se ha indicado previamente el concepto es anterior, los desastres naturales y ataques terroristas sucedidos en la primera década del siglo XXI han impulsado la creación de este tipo de organizaciones, que "tuteladas" por los gobiernos pretenden la asociación de las empresas privadas por sectores, para compartir la información necesaria para la defensa de estas infraestructuras críticas para la seguridad nacional.
Como hemos indicado previamente, en 1998, en la directiva **PDD 63**, se define ISAC como *Information Sharing and Analysis Center*. Así, un ISAC es una organización de confianza, específica de un sector, que posee capacidades de operación seguras 24/7, que establece información de inteligencia sobre incidencias, amenazas y vulnerabilidades. Basándose en análisis experto especializado del sector, el ISAC recoge, analiza y distribuye alertas e informes sobre incidentes a todos sus miembros y ayuda al gobierno a entender los impactos en el sector. Provee a los miembros de la capacidad e intercambio de información sobre amenazas informáticas, físicas y de todo tipo de amenazas para proteger las infraestructuras críticas; esto incluye

soporte analítico al gobierno y a otros ISACs al respecto a detalles técnicos durante incidencias existentes o potenciales causadas de manera intencionada o por desastres naturales. Entre los sectores que se definen como infraestructura crítica y actualmente cuentan con un ISAC propio (coordinado con el resto de centros por el *ISAC Council*) encontramos el sector eléctrico, el transporte público, las telecomunicaciones o el sector energético, por citar sólo unos ejemplos.

También en el Reino Unido se han establecido centros de seguridad focalizados en la protección de infraestructuras críticas; destacan por encima del resto de actores el Centro para la Protección de la Infraestructura Nacional (**CPNI**, *Center for the Protection of National Infrastructure*), que está formado por el Centro de Coordinación de Seguridad de la Infraestructura Nacional (NISCC, *National Infrastructure Security Co-ordination 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*), que surgen de la necesidad expresada anteriormente de proteger las infraestructuras nacionales mediante la compartición de información sensible, en este caso del gobierno británico.

Por su parte, y también en el ámbito anglosajón, el gobierno australiano creó en abril de 2003 TISN, un foro en el que los responsables, gestores, operadores... de la infraestructura crítica nacional australiana colaboran conjuntamente (y también con el gobierno de la nación) compartiendo información que pueda afectar a la seguridad de esta infraestructura crítica; se compone de diversos grupos denominados IAGGs (*Infrastructure Assurance Advisory Groups*) provenientes de diferentes sectores de negocio, coordinados por el CIAC (*Critical Infrastructure Advisory Council*) australiano.

Protección de Infraestructuras Críticas en España

El día 11 de marzo de 2004 se producen en Madrid unos atentados muy similares a los sufridos en EE.UU. el 11 de septiembre de 2001; la amenaza terrorista salía del territorio norteamericano y golpeaba de pleno —y no sería la última vez— a Europa. España, acostumbrada a lidiar contra el terrorismo independentista, parecía haber evaluado incorrectamente la amenaza islamista. Y por supuesto, tuvo que tomar las medidas oportunas para evitar que algo similar a lo que acababa de suceder pudiera volverse a producir.

Así, el 28 de mayo de 2004 —poco más de dos meses después de los fatídicos atentados del 11M— nace el Centro Nacional de Coordinación Antiterrorista (CNCA), un centro de coordinación y análisis —no operativo— que ejerce funciones de inteligencia, información y coordinación buscando el tratamiento integrado de la información estratégica relativa al terrorismo, tanto en su proyección nacional como internacional. El CNCA es equivalente al JTAC (*Joint Terrorism Analysis Centre*) británico o al NCTC (*National Counter-Terrorism Centre*) estadounidense.

El CNCA es un órgano de recepción, proceso y valoración de la información estratégica disponible sobre todos los tipos de terrorismo que constituyen una amenaza para España; no tiene una focalización específica en la protección de infraestructuras críticas, sin consideración oficial y específica hasta 2007, cuando se diseña y desarrolla el Plan Nacional de PIC (PNPIC) y se crea el Centro Nacional para la Protección de Infraestructuras Críticas, CNPIC. Desde ese momento hasta este año 2011 no ha habido mucho movimiento en la materia a nivel nacional, a pesar de que Europa aprobó hace tres años la directiva 2008/114/CE —analizada a continuación— que marcaba un plazo de dos años para su adopción por parte de los países miembros; en este 2011 en España se ha publicado la Ley de Protección de Infraestructuras Críticas, el Reglamento que la desarrolla y también la Estrategia Española de Seguridad, todos ellos —en especial los dos primeros— puntos clave para la protección de infraestructuras críticas en España. Analizamos a continuación estas normativas de forma resumida, lo que nos proporciona una idea de los movimientos nacionales a alto nivel para protección de las infraestructuras críticas.

Ley de Protección de Infraestructuras Críticas

Cuatro año después de la aprobación de la directiva 2008/114/CE, y con los plazos de la misma ya expirados, durante 2011 en España se ha creado legislación específica sobre la protección de infraestructuras críticas: el 28 de abril se publica la Ley 8/2011, el 20 de mayo el Real Decreto 704/2011 que desarrolla la anterior y, finalmente, el 24 de junio la Estrategia Española de Seguridad.

La Ley de Protección de Infraestructuras Críticas (LPIC) recoge las medidas necesarias establecidas por el Gobierno de España para dar cumplimiento a lo establecido en la Directiva 2008/114/CE; su objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (físicos o lógicos) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras, que aglutine a las AAPP y entidades privadas afectadas.

De su análisis se desprenden los elementos descritos en las páginas siguientes.

Agentes del sistema

Son agentes del sistema los siguientes:

Secretaría de Estado de Seguridad (Ministerio del Interior), con competencias a determinar en el Reglamento de desarrollo y responsable del Sistema de Protección de las Infraestructuras Críticas Nacionales.

CNPIC, responsable del impulso, la coordinación y supervisión de las actividades encomendadas a la Secretaría de Estado de Seguridad en relación con la PIC y responsable también de la gestión del Catálogo.

Ministerios y organismos (anexo de la Ley), ***encargados de impulsar las políticas de seguridad sobre los sectores estratégicos de su competencia*** y de velar por su aplicación, desempeñando las funciones a determinar por el Reglamento de Desarrollo de la Ley.

Delegaciones del Gobierno en las CCAA, con funciones a determinar en el Reglamento de Desarrollo con respecto a infraestructuras críticas localizada en su demarcación.

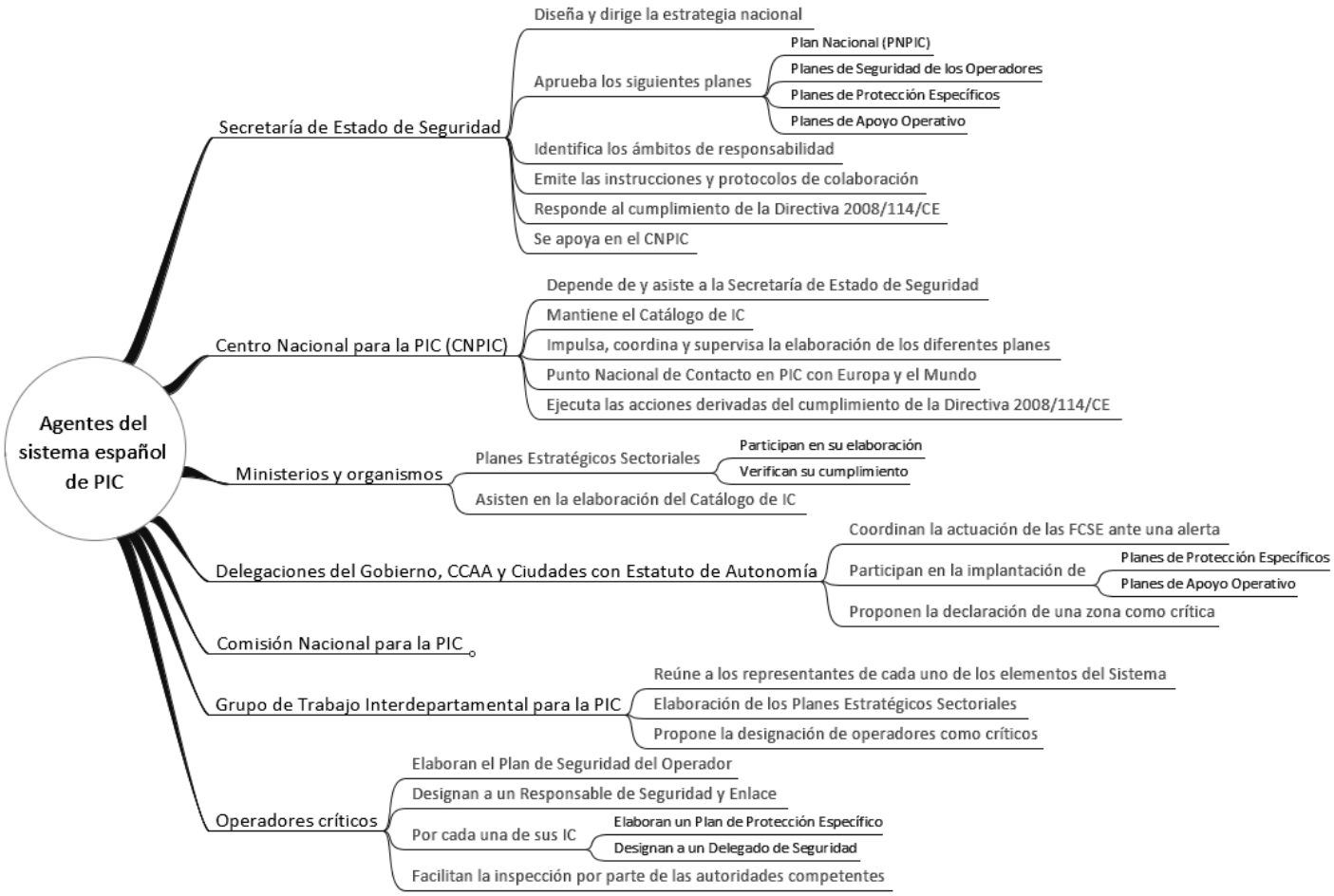
CCAA y ciudades con Estatuto de Autonomía con competencias en materia de protección de personas y bienes, con funciones a determinar en el Reglamento de Desarrollo.

Comisión Nacional para la PIC, con competencia para aprobar los Planes Estratégicos Sectoriales y designar a los operadores críticos y funciones y composición a determinar en el Reglamento de Desarrollo.

Grupo de Trabajo Interdepartamental para la PIC, con funciones y composición a determinar en el Reglamento de Desarrollo y con responsabilidad de elaboración de los diferentes Planes Estratégicos Sectoriales y propuesta a la Comisión de operadores críticos.

Operadores críticos, con obligación de colaborar con las autoridades competentes del Sistema en los términos indicados en la Ley.

En la figura siguiente se representan los agentes del sistema, involucrados en la PIC en España, de forma gráfica:



Como vemos en el diagrama anterior, son muchos los actores involucrados en la protección de infraestructuras críticas a nivel nacional. Por tanto, debe ser un objetivo principal del CNPIC, como órgano responsable de dicha protección, el facilitar el flujo de información entre actores a diferentes niveles.

Instrumentos y comunicación

La LPIC especifica la relación y responsabilidad de desarrollo o aprobación de los siguientes planes de actuación: Plan Nacional de PIC (Ministerio del Interior).

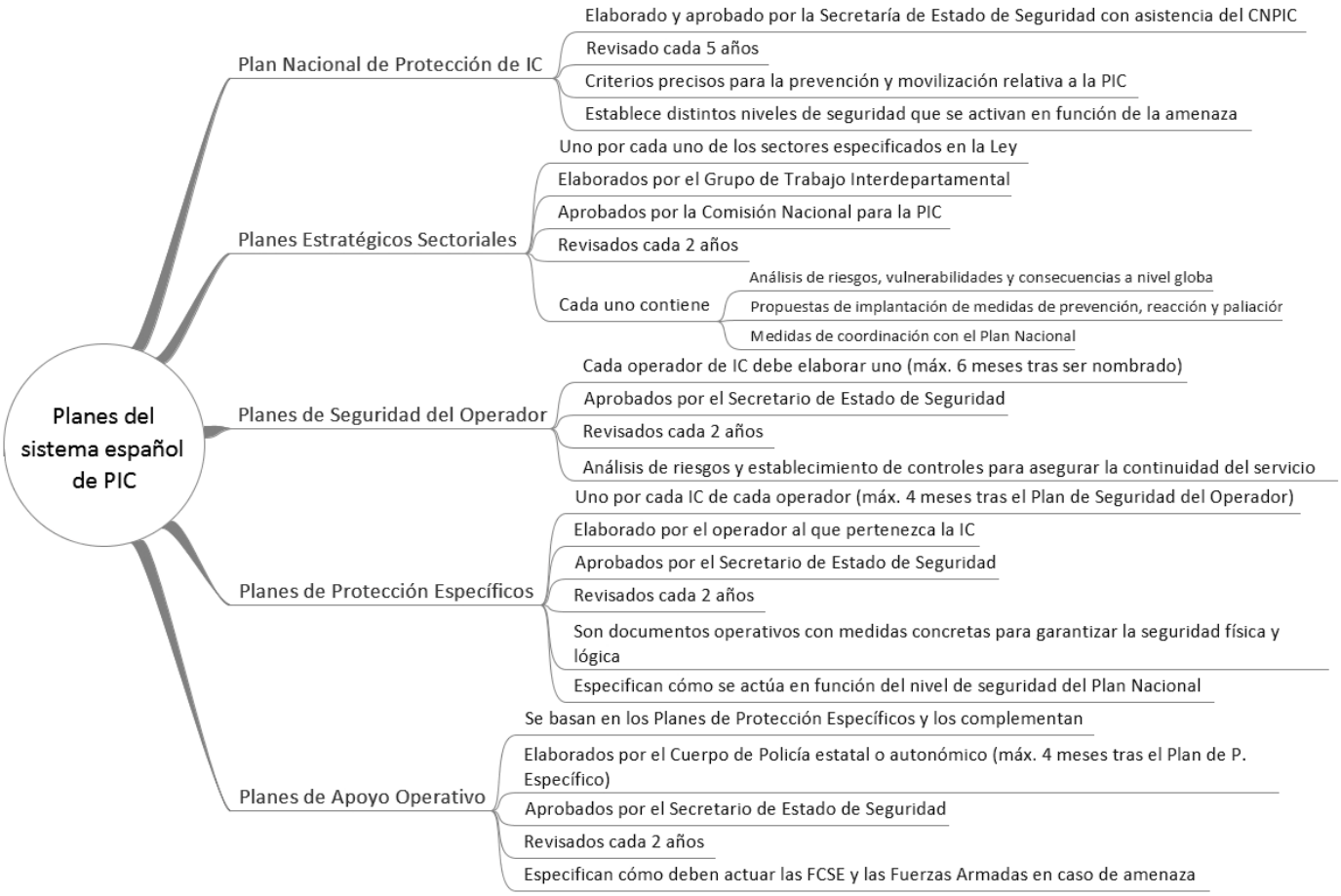
Planes Estratégicos Sectoriales (Grupo de Trabajo, aprobación por la Comisión).

Planes de Seguridad del Operador (Operadores Críticos).

Planes de Protección Específicos (Operadores Críticos).

Planes de Apoyo Operativo (FFCCSE).

Gráficamente, el mapa de dichos planes es el expuesto a continuación:



Responsabilidades

La LPIC marca la necesidad de garantizar la seguridad de la información por parte de las AAPP y los operadores críticos, siendo responsabilidad de la Secretaría de Estado de Seguridad arbitrar los sistemas de gestión que permitan el mantenimiento e intercambio de la información relativa a PIC. Adicionalmente, se define la figura del Responsable de Seguridad y Enlace, con la habilitación de Director de Seguridad expedida por el Ministerio del Interior, así como del Delegado de Seguridad de la ICE.

Reglamento de Protección de Infraestructuras Críticas

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el **Reglamento de Protección de las Infraestructuras Críticas**, desarrolla, concreta y amplía los aspectos contemplados en la LPIC con la articulación de un sistema compuesto por órganos y entidades tanto de las Administraciones Públicas como del sector privado y el diseño de todo un planeamiento orientado a prevenir y proteger dichas infraestructuras críticas. El texto contempla la elaboración de diferentes **planes** que deben ser desarrollados tanto por las Administraciones Públicas —en el caso del Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales y los Planes de Apoyo Operativo— como por las

empresas, organizaciones o instituciones clasificadas como operadores críticos, para la elaboración de los Planes de Seguridad del Operador y los Planes de Protección Específicos.

El Reglamento consta de 36 artículos y está estructurado en cuatro Títulos. El Título I contiene las cuestiones generales relativas a su objetivo y ámbito de aplicación. El Título II está plenamente dedicado al Sistema de Protección de Infraestructuras Críticas, concretando la composición, competencias y funcionamiento de todos los órganos creados por la Ley. El Título III se encarga de la regulación de los instrumentos de planificación y, por último, el Título IV está dedicado a la seguridad de las comunicaciones y a las figuras del Responsable de Seguridad y Enlace y del Delegado de Seguridad de la infraestructura crítica.

Del análisis de este Reglamento se desprenden los siguientes aspectos principales:

Título I

En este Título se define el **objeto** del Reglamento como el **establecimiento de medidas para la protección de las infraestructuras críticas** y la **regulación de las obligaciones** que deben asumir tanto el Estado como los operadores de aquellas infraestructuras que se determinen como críticas. El **ámbito** se establece para las **infraestructuras críticas en territorio nacional**, a excepción de las dependientes del Ministerio de Defensa y de las FFCCSS. También se referencia el **Catálogo Nacional de Infraestructuras Estratégicas**, registro de carácter administrativo que contiene información de todas las infraestructuras estratégicas, incluyendo tanto las críticas como las críticas europeas, y cuya finalidad es valorar y gestionar los datos que se dispone de ellas para diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza. Según se indica en el Reglamento, el **Catálogo** contendrá todos los datos necesarios (relativos a la descripción de las infraestructuras, su ubicación, titularidad y administración, servicios que prestan, medios de contacto, nivel de seguridad) aportados por el **Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)** y los operadores, así como el resto de sujetos responsables y tendrá la clasificación de SECRETO; su gestión y mantenimiento corresponde al Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.

Título II

En este Título se enumeran y definen los **agentes** del Sistema de Protección de Infraestructuras Críticas; se establecen las funciones para la **Secretaría de Estado de Seguridad**, órgano superior responsable del Sistema de Protección de las IICC

nacionales, entre las que destacan el **diseño y dirección de la estrategia nacional** de protección de IICC, la aprobación del **Plan Nacional de Protección de las IICC** declarando los niveles de seguridad, en coordinación con el Plan de Prevención y Protección Antiterrorista, los Planes de Seguridad de los Operadores, los Planes de Protección Específicos y los Planes de Apoyo Operativo, así como la aprobación de declaración de **zona crítica** o la identificación de los ámbitos de responsabilidad en la protección de IICC; dentro también de este Título, se define y establece el Centro Nacional para la Protección de las Infraestructuras Críticas (**CNPIC**), dependiente de la Secretaría de Estado de Seguridad, cuyas funciones principales son las de asistir al Secretario de Estado de Seguridad en materia de protección de IICC actuando como **contacto y coordinador entre los agentes del Sistema**, mantener el Plan Nacional de Protección de las IICC, determinar la criticidad de las IICC y mantener el Catálogo. Respecto a los instrumentos de planificación, el CNPIC **dirige y coordina los análisis de riesgos** realizados por los organismos especializados en los Planes Estratégicos Sectoriales, establece los **mínimos** de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo, y evalúa los Planes de Seguridad del Operador y los propone al Secretario de Estado de Seguridad para su aprobación. Otras funciones asignadas son la **propuesta** de declaración de **zona crítica** al Secretario de Estado de Seguridad, la **recopilación y valoración de la información sobre infraestructuras estratégicas** para su remisión al **Centro Nacional de Coordinación Antiterrorista** del Ministerio del Interior, la participación en la realización de **ejercicios y simulacros** y el establecimiento del **Punto Nacional de Contacto** con organismos internacionales en el ámbito de la protección de IICC.

Las principales competencias de los **Ministerios** y organismos integrados en el Sistema de Protección de IICC son la participación en los Planes Estratégicos Sectoriales a través del **Grupo de Trabajo Interdepartamental** y la verificación de su cumplimiento, la colaboración en la **designación de los operadores críticos** y el **asesoramiento técnico** en la catalogación de las infraestructuras y su clasificación como crítica; todo ello, dentro de su sector de competencia correspondiente. Se establecen adicionalmente facultades para las **Delegaciones del Gobierno** en las Comunidades Autónomas y Ciudades Autónomas, como la coordinación de las FFCCSE ante una alerta de seguridad o el velar por la aplicación y cumplimiento del Plan Nacional de Protección o de los Planes Sectoriales, entre otras. Las competencias para las **Comunidades Autónomas y las Ciudades Autónomas** con competencias para la protección de persona y bienes y para el mantenimiento del orden público son

similares a las de las Delegaciones del Gobierno; para aquellas que no tengan competencias, se les reconoce la participación en el Sistema y en los órganos colegiados.

Las funciones de la **Comisión Nacional para la Protección de las Infraestructuras Críticas** pasan por preservar, garantizar y promover una cultura de seguridad de las IICC en las Administraciones Públicas, promover la aplicación efectiva de las medidas de protección e impulsar acciones de cooperación interministerial. Esta Comisión estará presidida por el Secretario de Estado de Seguridad y tendrá representación de los organismos implicados con rango Director General, así como un representante por Comunidad Autónoma con competencias de seguridad. Se reunirá una vez al año y será asistida por el **Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas**, grupo entre cuyas funciones está elaborar los diferentes Planes Estratégicos Sectoriales, proponer a la Comisión la designación de operadores críticos y la creación de grupos de trabajo sectoriales.

Los últimos agentes del sistema reconocidos en el Reglamento son los **Operadores Críticos**, aquellos en los que al menos una de las infraestructuras gestionadas por él reúna la consideración de crítica; deberán prestar colaboración técnica en la valoración de las infraestructuras, colaborar con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en el análisis de riesgos, así como elaborar el Plan de Seguridad del Operador, un Plan de Protección Específico y **designar a un Responsable de Seguridad y Enlace y un Delegado de Seguridad**, entre otras funciones.

Título III

Este Título recoge los **instrumentos de planificación**; define el **Plan Nacional de Protección de las Infraestructuras Críticas** como el instrumento de programación dirigido a mantener seguras las infraestructuras españolas que proporcionan servicios esenciales. Este Plan establece criterios y directrices para asegurar la protección del sistema de infraestructuras estratégicas y prevé distintos niveles de seguridad e intervención policial, en coordinación con el **Plan de Prevención y Protección Antiterrorista**. Se definen además los **Planes Estratégicos Sectoriales** indicando que se trata de instrumentos de estudio y planificación que permitirán conocer los servicios esenciales, el funcionamiento general de éstos, sus vulnerabilidades, las potenciales consecuencias de su inactividad y las medidas necesarias para su mantenimiento. El Grupo de Trabajo, con la participación de los operadores afectados, elaborará un Plan Estratégico por cada sector o subsector de actividad que estará basado en un análisis general de riesgos cuyo

contenido mínimo será un análisis de riesgos, vulnerabilidades y consecuencias a nivel global y una serie de propuestas de implantación de medidas para los diferentes escenarios, medidas de coordinación con el Plan Nacional PIC.

Los **Planes de Seguridad del Operador** vienen recogidos en el Capítulo III de este Título y tienen como finalidad definir las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión. Estos planes deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios y recoger los criterios de aplicación de las diferentes medidas. Dentro del Capítulo IV se desarrollan los **Planes de Protección Específicos** como los documentos operativos donde se definen **medidas concretas para garantizar la seguridad integral de sus infraestructuras críticas**. Deberán contemplar la adopción tanto de medidas permanentes de protección como de medidas de seguridad temporales y graduadas. En un plazo de dos meses tras su recepción, la Secretaría de Estado de Seguridad notificará al interesado su resolución de la aprobación, proponiendo un calendario de implantación gradual. Las Delegaciones del Gobierno mantendrán un registro de los Planes que afecten a su demarcación y el CNPIC mantendrá un registro central de todos ellos. La revisión de estos planes se realizará cada dos años y deberá ser aprobada por la Delegación del Gobierno, quien velará también por la correcta ejecución de los Planes de Protección Específicos. Ésta tendrá facultades de inspección y podrán requerir del responsable de las IICC la situación actualizada de la implantación de las medidas propuestas. Estos Planes se efectuarán sin perjuicio del obligado cumplimiento de lo exigido para instalaciones nucleares y radiactivas, portuarias, aeroportuarias, aeródromos e instalaciones de navegación aérea.

Finalmente, en este mismo Título III, el **Capítulo V** recoge los **Planes de Apoyo Operativo** donde se deben plasmar las medidas concretas para la mejor protección de las IICC; su realización será supervisada por la Delegación del Gobierno y para la elaboración de estos planes se dispone de cuatro meses tras la aprobación del respectivo Plan de Protección Específico, debiendo contemplar las medidas planificadas de vigilancia, prevención, protección y reacción, cuando se produzca la activación del Plan Nacional de Protección de las IICC. El contenido mínimo será establecido por el CNPIC, así como el modelo en el que fundamentar la estructura y desarrollo de éstos.

Título IV

El último Título del Reglamento versa sobre las **comunicaciones entre los operadores críticos y las Administraciones públicas**, donde se designa al CNPIC como responsable de administrar los sistemas de información y comunicaciones diseñadas para la protección de las IICC, y cuya seguridad será acreditada y certificada por el Centro Criptológico Nacional; cada infraestructura crítica deberá contar con un Responsable de Seguridad y Enlace y en caso de ser necesario, con un Delegado de Seguridad. El nombramiento y comunicación de ambos se hará en el plazo de tres meses al CNPIC y a la Delegación del Gobierno, respectivamente.

Estrategia Española de Seguridad

Durante este año 2011 se ha publicado el documento que tiene por título "*Estrategia Española de Seguridad, una responsabilidad de todos".* Esta estrategia expone la necesidad de una estrategia de seguridad para España, sitúa el estado de la seguridad de España en el mundo y analiza los potenciadores del riesgo para la seguridad del país, así como los principales riesgos y amenazas. Propone además un modelo institucional integrado, que requiere una serie de cambios orgánicos para ofrecer una respuesta a las necesidades de seguridad del país.

La Estrategia Española de Seguridad (EES) realiza especial hincapié en la necesidad de tratar los aspectos cambiantes en los que nos vemos envueltos en la actualidad. Uno de los factores más importantes que hace necesaria una estrategia de seguridad es la globalización, que requiere un estudio y diseño acorde a este fenómeno. Ante esto, las respuestas ofrecidas deben ser necesariamente nacionales, europeas, regionales y globales. Sólo un enfoque integral, que conciba la seguridad de manera amplia e interdisciplinar, a nivel nacional, europeo e internacional, puede responder a los complejos retos a los que nos enfrentamos.

La política de seguridad estará basada en seis conceptos básicos, **enfoque integral** de las diversas dimensiones de la seguridad, **coordinación** entre las administraciones públicas y con la sociedad, **eficiencia en el uso de los recursos**, **anticipación y prevención** de las amenazas y riesgos, **resistencia y recuperación** de sistemas e instrumentos y, por último, **interdependencia responsable** con nuestros socios y aliados.

Dentro de la EES se analizan los fenómenos globales que propician la propagación o transformación de los riesgos y amenazas que nos afectan; entre los fenómenos se encuentran disfunciones de la globalización, desequilibrios demográficos, pobreza y desigualdad, cambio climático, peligros tecnológicos e ideologías radicales y no democráticas, todos éstos considerados como potenciadores de los riesgos y amenazas. Destacar cómo se considera en la era en la que vivimos como uno de los potenciadores de las amenazas los peligros tecnológicos, hecho viene a destacar la importancia que los mismos poseen en nuestra seguridad nacional. Algunos de estos fenómenos pueden no afectarnos de manera directa, pero sí de manera indirecta, por lo que es necesario contemplarlos ya que en menor o mayor medida afectan a la seguridad del país.

El análisis de los riesgos y las amenazas que se realiza en la estrategia analiza en primera instancia los ámbitos en los que tienen lugar. Los ámbitos contemplados van desde el terrestre, marítimo, aéreo, espacial o ciberespacio al informativo. Se destacan como principales amenazas los conflictos armados, el terrorismo, crimen organizado, inseguridad económica y financiera, vulnerabilidad energética, proliferación de armas de destrucción masiva, ciberamenazas, flujos migratorios no controlados, emergencias y catástrofes en infraestructuras, suministros y servicios críticos. La EES destaca que es necesaria una coordinación entre en la administración pública y el sector privado en materia de infraestructuras críticas, dado que parte de la infraestructuras críticas están manos de este sector privado, lo que hace necesaria una comunicación, coordinación constante y eficaz.

También destaca entre las infraestructuras, suministros y servicios críticos para el país la energía, las redes de comunicación y las finanzas, ya tratados en otros apartados, el transporte, el agua, la salud o la alimentación.

Para reforzar la resistencia y capacidad de recuperación de estos activos fundamentales, la EES considera indispensable seguir avanzando en aspectos como la consolidación de los instrumentos para la protección de las instalaciones, la mejora del marco regulador de los sectores críticos, el establecimiento de medidas que aumenten su fortaleza, incrementen su resistencia y refuercen sus capacidades de adaptación ante condiciones adversas y el diálogo y cooperación permanente entre las administraciones públicas y los operadores de infraestructuras y servicios.

Tal y como se recoge en este mismo informe, España ha creado un Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) y aprobado un Catálogo nacional de infraestructuras Estratégicas, así como un primer plan para protegerlas. Del análisis realizado en la EES, destaca por encima de las demás la necesidad de impulsar cambios orgánicos al máximo nivel del Estado que garanticen la articulación de esta nueva concepción integrada de la seguridad, su gestión y su seguimiento.

Análisis

La preocupación por la protección de las infraestructuras críticas es cada vez más patente, no sólo desde el punto de vista gubernamental sino también desde el punto de vista particular de las personas y empresas que trabajamos en el ámbito de la seguridad; sin referirnos a complejas estadísticas —que las hay— acerca de la protección de estas infraestructuras, algo tan sencillo como consultar los datos de búsquedas (por ejemplo en Google) de términos relativos a estos temas ("*SCADA Security*", "*Critical Infrastructure Protection*", etc.) nos arroja unos resultados claros: la protección de infraestructuras críticas preocupa mucho, y esta tendencia sigue al alza. Y con razón, debemos añadir, porque es la seguridad de estas infraestructuras es completamente necesaria, pero dista mucho de ser sencilla, y nos jugamos mucho para que algo pueda salir mal.

Sin duda uno de los mayores problemas asociados a la protección de las infraestructuras críticas es la **complejidad** de lo que se viene a llamar el ecosistema; existen muchos agentes involucrados en dicha protección (desde los propios operadores hasta FFCCSE, pasando por el Gobierno de la nación), y por tanto la coordinación y la comunicación entre ellos debe ser ágil y segura para garantizar la seguridad de estas infraestructuras. Además, el 80% de operadores de infraestructuras críticas pertenecen al sector privado, siendo muchos de ellos compañías multinacionales… ¿El Estado necesita intervenir a las empresas privadas? ¿Cómo se consigue el equilibrio? ¿Hace falta un marco sancionador?

Dentro de la complejidad a la que hacemos referencia, no únicamente nos encontramos ante sistemas en cuya protección se involucra a un gran número de actores sino que, además, nos encontramos con los problemas de **dependencia** en IICC: infraestructuras críticas pueden ser independientes, pero más habitual es que sean dependientes o interdependientes. Esto implica que una infraestructura depende en buena parte de otra —nacional o europea— para su funcionamiento correcto, con lo que un fallo en cascada o un error en un punto único de fallo puede suponer un enorme problema; en especial, si a esta dependencia añadimos que en ocasiones no se conocen del todo bien las interdependencias entre infraestructuras… Para corregir esta situación, desde Europa se está subvencionando activamente a proyectos de I+D+i para modelizar y/o simular estas interdependencias; adicionalmente, los planes para la protección de infraestructuras críticas (en concreto, la confección de catálogos de IC) pueden y deben ayudar a identificar no sólo las infraestructuras, sino también su grado de redundancia y sus interdependencias.

La seguridad de las infraestructuras críticas debe garantizarse desde **cualquier punto de vista**; la seguridad

es un concepto global, y el medio natural, un atacante —cuyo objetivo, no lo olvidemos, es dañar a sus víctimas— o un accidente simplemente elegirá el camino más fácil para materializarse: cualquiera de las visiones de la seguridad. La protección física es, bajo nuestro punto de vista, aceptable en la mayor parte de ocasiones, pero no así la seguridad lógica de las infraestructuras críticas. La exposición a Internet de los sistemas SCADA, entornos tecnológicos que controlan la operación de muchas de estas infraestructuras, así como el que habitualmente se trate de sistemas no diseñados con la seguridad como premisa básica, hacen que un posible ataque remoto a estos sistemas sea un riesgo más que considerable para los operadores.

¿Cómo se comparan en términos de probabilidad e impacto los ciberataques contra una infraestructura crítica con los ataques tradicionales (por ejemplo, un bombardeo) contra esa misma infraestructura? 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. En otras palabras, puede resultar más fácil sobornar —o extorsionar— a alguien con capacidad de acceso a la plataforma tecnológica de la infraestructura crítica para que haga algo por nosotros desde el punto de vista lógico que lanzar un ataque "al uso" contra esa misma infraestructura. Por tanto, podemos deducir —y así parecen haberlo hecho los gobiernos de todo el mundo— que la probabilidad de un ciberataque contra infraestructuras críticas es más que significativa, por lo que hay que tomar medidas para reducir el riesgo asociado a estas amenazas.

Queremos creer —y algunos estudios así lo indican— que las infraestructuras críticas no son tan frágiles como pudiera parecer. Estas infraestructuras suelen estar preparadas (redundancia, etc.) contra fallos rutinarios o accidentes más o menos relevantes —el punto de vista de la *safety* más que de la *security*—. No obstante, ¿hasta qué punto esa preparación sirve para combatir los ataques intencionados? ¿Sirven los protocolos de actuación diseñados para hacer frente a estas situaciones frente al ataque intencionado, lógico o físico? Si un ciberterrorista ataca una central eléctrica y la anula, ¿se puede comparar el impacto con el de un fallo rutinario? Quizás más de lo que se supone… De hecho, cuando se trata de ciberterrorismo, la gente no está dispuesta a asumir ningún fallo de suministro; sin embargo, si se trata de un fallo casual, se es más indulgente. ¿La pérdida es la misma? ¿Es peor la pérdida de una vida por terrorismo que por un fallo no intencionado? El ciberterrorismo claramente sirve para facilitar un ataque terrorista, pero por sí

mismo no hay ningún caso documentado en el que un ciberataque haya tenido como consecuencia pérdidas de vidas. Además, los efectos de una bomba tienen un mayor efecto aterrorizador, que es lo que busca principalmente un terrorista…Quizás debamos prestar más atención a la lucha contra el ciberespionaje que contra el ciberterrorismo, dado que el robo de información en este caso es sin duda más sencillo que un ataque terrorista contra una infraestructura crítica; por supuesto, robo de información que un tercero puede utilizar para cualquier fin, desde económico hasta político… Es más, ¿hasta qué punto es más probable la infección accidental por un virus de un sistema que corre un SCADA que el ataque intencionado?

Líneas de Trabajo

El elevado número de actores involucrados en la seguridad de las infraestructuras críticas no debe ser un obstáculo para protegerlas; así, es necesario potenciar la colaboración y el intercambio de información entre los actores participantes en la PIC nacional a diferentes niveles, desde el estratégico al operativo, y también con diferentes ámbitos de colaboración:

Actores del ámbito público. El intercambio de información entre entidades del ámbito público (FFCCSE, FAS, CNPIC…) debe ser garantizado al más alto nivel; la implicación de múltiples actores debe ser liderada en la práctica de forma única y coordinada, evitando que los ámbitos de competencia de cada uno de ellos se conviertan en un obstáculo para la capacidad de respuesta nacional.

Actores del ámbito privado. Dado el elevado porcentaje de IICC operadas por el sector privado, la participación de este en cualquier iniciativa de seguridad es clave para garantizar el éxito de la misma y si a este hecho añadimos la interdependencia entre infraestructuras, la relevancia del sector privado es aún mayor. En este caso los obstáculos a superar vienen marcados por el recelo a la colaboración que en ocasiones puede producirse entre organizaciones que en casos son incluso competencia, y en este sentido las empresas deben abandonar la idea de seguridad como diferencia o negocio y adoptar la estrategia de "*responsibility to provide*".

Colaboración público-privada. La coordinación entre el ámbito público y privado para la protección de infraestructuras críticas debe ser también exhaustiva, constituyendo lo que se viene a denominar PPP (*Public-Private Partnerships*) y garantizando que los esfuerzos son comunes y van siempre en la misma dirección.

El marco de esta colaboración debe extenderse a todos los ámbitos de la seguridad de una infraestructura crítica; en el marco de la seguridad privada la colaboración y el intercambio de información con la seguridad pública es algo habitual, e incluso lo es —cada vez más— entre empresas o Departamentos de Seguridad que en muchos casos son competencia directa. Cuando hablamos de protección lógica el panorama es completamente diferente: si bien la colaboración público privada es común (por poner un ejemplo, las empresas no vemos a las FFCCSE como nuestra competencia), no lo es tanto la colaboración entre empresas o actores exclusivamente del sector privado, y esto claramente perjudica al global de la seguridad nacional. Existen iniciativas —el Consejo Nacional Consultivo sobre Ciberseguridad, CNCCS, puede ser una de ellas—

demasiado tímidas y dispersas por el momento, por lo que deben reforzarse para conseguir que sean operativas y por tanto permitan incrementar la seguridad de nuestras infraestructuras críticas.

Estas iniciativas de colaboración e intercambio de información no deben verse jamás en ámbitos reducidos de la seguridad (física, lógica…) sino que deben realizarse desde el punto de vista de la SEGURIDAD con mayúsculas, sin importar el apellido o especialización concreta que queramos aplicar después; como hemos comentado previamente, el riesgo es global y la protección, si queremos que sea efectiva, debe serlo también, ya que en caso contrario estamos construyendo un muro sin cimientos y con bastantes agujeros en el mismo. Y desde todos estos puntos de vista de la seguridad con mayúsculas, debemos trabajar con la adaptabilidad como premisa; estamos enfrentándonos a situaciones nuevas, con amenazas desconocidas hasta hace poco tiempo —a las que probablemente se unan nuevas amenazas desconocidas ahora mismo— y que modifican los esquemas de seguridad y defensa tradicionales de forma radical. Si no somos capaces de adaptarnos rápidamente a estas nuevas situaciones y hacer que las infraestructuras críticas tengan un elevado grado de resiliencia y puedan recuperarse ante problemas de diversa índole, conocidos y, por qué no, desconocidos, fracasaremos en su protección.

Es muy complejo, como hemos dicho, hacer que todo el ecosistema de actores implicados en la seguridad de IICC trabaje en la misma dirección; esta visión no puede ser liderada por grupos u organizaciones concretas, ni en el ámbito público ni en el privado, sino que debe hacerse al más alto nivel del Estado y con el apoyo explícito de éste, algo que recoge muy bien la Ley de Protección de Infraestructuras Críticas que hemos analizado previamente. Un enfoque piramidal, en el que desde la cima —la estrategia— hasta la base —la operativa— se definan y articulen los mecanismos de protección al nivel correspondiente. Cualquier iniciativa que no venga liderada y apoyada desde el propio Estado y con el más alto nivel estará condenada al fracaso. Como también lo estará cualquier iniciativa que, como antes hemos dicho, focalice su atención en unas amenazas concretas y descuide otras en función de en qué ámbito se puede materializar cada una de ellas.

Para finalizar este análisis, es necesario destacar la importancia del nivel operativo, el que día a día hace frente a las amenazas, a la hora de

hablar de protección de infraestructuras críticas. La organización, el apoyo al más alto nivel, el intercambio de información… servirá de muy poco si operativamente no somos capaces de proteger adecuadamente cada infraestructura. En este ámbito, desde el punto de vista técnico consideramos necesario reforzar la seguridad en entornos de control industrial asociados a las infraestructuras críticas, sistemas que o bien se diseñaron para trabajar en entornos aislados, sin considerar amenazas provenientes de la otra punta del mundo, o bien están a cargo de equipos que no tienen la idea de la interconexión de sistemas en la cabeza. En opinión de este equipo, a la hora de hablar de la seguridad lógica de estos entornos, nos encontramos ahora en la misma situación que teníamos hace quince años con cualquier sistema operativo de propósito general: entornos no diseñados con la seguridad como premisa, abiertos por completo a Internet y accesibles a golpe de ratón y teclado desde cualquier punto del mundo. No hay que ser ningún experto en seguridad para utilizar analizadores o buscadores basados en cabeceras de protocolos (típicamente, HTTP) y determinar, por ejemplo, que existen numerosos sistemas SCADA, cámaras IP de videovigilancia o sistemas de control de acceso encargados de proteger infraestructuras críticas —incluidas españolas—, accesibles por completo desde Internet mediante un simple usuario y contraseña o con vulnerabilidades críticas —fallos en su diseño o implementación— que pueden permitir a un atacante tomar el control total o parcial de la infraestructura, desde cualquier punto de Internet, sin correr ningún riesgo y con un impacto potencial muy alto. Preocupante, ¿no?

En la protección de infraestructuras críticas actual desde el punto de vista lógico debemos aplicar, a muy corto plazo, medidas drásticas que incrementen la seguridad tecnológica de las infraestructuras, en especial la de los sistemas de control industrial, en dos grandes líneas: control de acceso y robustez de aplicaciones; algo similar a las medidas que en su momento se tomaron para proteger los sistemas generalistas, expuestos a Internet por completo. Confiamos en que a corto plazo se apliquen medidas de seguridad, teniendo en cuenta que aquí la situación puede ser más grave que en otros entornos: de muchos de esos sistemas dependen infraestructuras críticas (insistimos: vidas humanas en la mayor parte de ocasiones). ¿En cuántos años seremos capaces de tenerlos correctamente protegidos? La respuesta debe ser rápida, al menos más de lo que pueda ser el ataque…

Conclusiones

La protección de infraestructuras críticas es una preocupación para los gobiernos de todo el mundo; en este siglo nos enfrentamos a nuevos paradigmas de seguridad que implican amenazas y modelos desconocidos hasta el momento —y más que habrá, previsiblemente— que nos obligan y nos seguirán obligando a replantearnos todos los esquemas de protección que teníamos hasta la fecha.

Se ha trabajado intensivamente en la protección de infraestructuras críticas pero todavía queda mucho trabajo por hacer a nivel nacional; todas las iniciativas, lideradas al más alto nivel, deben ir orientadas a la protección integral y a la resiliencia de las infraestructuras, y deben garantizar que el Estado es capaz de adaptarse rápidamente a nuevas situaciones que quizás hoy no podamos ni imaginar. Y estas iniciativas deben contar con la colaboración del sector público y del privado, este último involucrado de lleno en la PIC.

Desde el apoyo, implicación y liderazgo del alto nivel estatal, los mecanismos de seguridad y defensa de las infraestructuras críticas deben ser plasmados correctamente en todos los escalafones necesarios para la protección hasta llegar al operativo puro y duro, que deberá reforzar la seguridad del día a día prestando especial atención a los aspectos de seguridad tecnológica, cada vez más relevantes en la PIC.

A modo de resumen, planteamos algunas líneas de trabajo para el corto y medio plazo que este equipo considera necesario destacar y que han sido desarrolladas a lo largo del presente informe:

Potenciar la colaboración y el intercambio de información entre los actores participantes en la PIC a diferentes niveles.

Promover la participación activa del sector privado y la colaboración público-privada.

Impulsar los cambios orgánicos necesarios al máximo nivel del Estado para garantizar la gestión correcta de los nuevos paradigmas de la seguridad y la defensa.

Garantizar la adaptabilidad de la protección a nuevas situaciones que sean radicalmente opuestas a las conocidas, permitiendo la resiliencia de las infraestructuras críticas.

Abordar la protección de infraestructuras críticas desde el punto de vista físico y desde el punto de vista lógico, con una gestión integrada.

Mejorar la seguridad lógica de las infraestructuras críticas haciendo especial hincapié en la protección adecuada de los sistemas de control.

Referencias

[1] Presidential Decision Directive, PDD-39. "*U.S. Policy on Counterterrorism*". Junio, 1995. http://www.fas.org/irp/offdocs/pdd39.htm

[2] Presidential Decision Directive, PDD-62. "*Combating Terrorism*". Mayo, 1998.

http://www.fas.org/irp/offdocs/pdd-62.htm

[3] Presidential Decision Directive, PDD-63. "*Protecting America's Critical Infrastructures*". Mayo, 1998.

http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

[4] "*The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive-63*" (whitepaper). Mayo, 1998.

http://www.fas.org/irp/offdocs/paper598.htm

[5] Homeland Security Presidential Directive HSPD-7. "*Critical Infrastructure Identification, Prioritization, and Protection*". Diciembre, 2003.

http://www.fas.org/irp/offdocs/nspd/hspd-7.html

[6] "*Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*"

James A. Lewis. *Center for Strategic and International Studies*. Diciembre 2002.

[7] "*Security Economics and Critical National Infrastructure*". Ross Anderson, Shailendra Fuloria. Computer Laboratory, Cambridge University. 2009

[8] "*Cyber War Will Not Take Place*". Thomas Rid. King's College London. Octubre 2011.

[9] "*La protección de las infraestructuras críticas*". María José Caro Bejarano. Instituto Español de Estudios Estratégicos. Julio, 2011.

[10] "Protecting critical infrastructure in the EU". CEPS Task Force Report. Centre for European Policy Studies. 2010.

[11] *Ley 8/2011*. Boletín Oficial del Estado, núm. 102, sec. I, pág. 43370. Abril de 2011.

[12] *R.D. 704/2011*. Boletín Oficial del Estado, núm. 121, sec. I, pág. 50808. Mayo de 2011.

[13] *Entrevista a Fernando Sánchez Gómez, director del CNPIC*. Seguritecnia. Septiembre, 2011.

[14] "*En el punto de mira. Las infraestructuras críticas en la era de la ciberguerra*". Informe McAfee. Septiembre, 2009.

[15] "*Amenazas en la oscuridad. Las infraestructuras críticas se enfrentan a ciberataques*". Informe McAfee, Noviembre, 2010.

[16] "*Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*". Cap. 6: "Estrategias Nacionales de Ciberseguridad. Ciberterrorismo". Cuaderno de Estrategia 149. Instituto Español de Estudios Estratégicos. Instituto Universitario "General Gutiérrez Mellado". Ministerio de Defensa.

[17] *Estrategia Española de Seguridad: una responsabilidad de todos*. Gobierno de España, 2011.

Contacto

Antonio Villalón Huerta

Director de Seguridad

S2 Grupo

avillalon@s2grupo.es

www.s2grupo.es

www.securityartwork.es