Capítulo quinto

Cooperación público-privada en la protección de infraestructuras críticas

Fernando Sánchez Gómez

Director del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Es teniente coronel de la Guardia Civil y diplomado de Estado Mayor por el Centro Superior de Estudios de la Defensa Nacional

Justo López Parra

Responsable de Prevención y Respuesta a la Ciberamenaza en Endesa. Es Ingeniero Informático por la Universidad de Castilla La Mancha, certificado CISM y está homologado como director de Seguridad Privada por el Ministerio del Interior

Resumen

Este capítulo se inicia mostrando las nuevas amenazas que han surgido contra el sistema de sectores estratégicos, tratando, asimismo, la colaboración entre las empresas privadas y los organismos públicos para su protección. Como ejemplos de estas amenazas se estudian los ciberataques Blackenergy, que consiguió dejar sin electricidad a una población de 1,5 millones de habitantes, y Stuxnet, primer ciberataque que de forma masiva consiguió la destrucción física de su objetivo.

El contenido de este trabajo está basado en la intensa colaboración que el CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) y Endesa han desarrollado, en el marco de la protección de las infraestructuras críticas, durante los últimos años, aprovechando así la experiencia adquirida en el tratamiento conjunto de las ciberamenazas. Actualmente, las herramientas que el CNPIC, en colaboración con el INCIBE, pone al servicio de las organizaciones que proveen servicios esenciales son: apoyo frente a incidentes, equipo de respuesta a incidentes cibernéticos (CERTSI_), servicios de alerta temprana, planificación y desarrollo de ciberejercicios y acuerdos de colaboración. Al mismo tiempo, la Oficina de Coordinación Cibernética del Ministerio del Interior ejerce la tarea de llevar a cabo la coordinación operativa entre los elementos tecnológicos ya reflejados y las capacidades de investigación y de persecución del delito propias de las Fuerzas y Cuerpos

de Seguridad del Estado, constituidas por las unidades tecnológicas de la Guardia Civil y de la Policía Nacional.

Para finalizar este capítulo, se da cuenta de distintas herramientas previstas para continuar potenciando la colaboración público-privada que tan satisfactorios resultados están dando para mejorar la seguridad de nuestros servicios esenciales.

Palabras clave

Ciberataque, amenaza, stuxnet, blackenergy, normativa, colaboración público-privada, *CERT* (equipo de respuesta a emergencias informáticas), infraestructuras críticas, servicios esenciales, planificación.

Abstract

This chapter begins by describing the latest threats that have emerged against the system of strategic sectors. It is also highlighted the need of seeking cooperation among all actors and building a robust public-private partnership scheme. Some examples of these new threats are *BlackEnergy*, which managed to leave without electricity a population of 1.5 million, and not so recently, Stuxnet, first known cyberattack which achieved a massively physical destruction of its target.

The content of this work is based on the intensive collaboration developed in the last few years between CNPIC (National Centre for the Protection of Critical Infrastructure) and Endesa, taking advantage of the experience already acquired in the joint treatment of cyberthreats.

Currently, the tools that the CNPIC, in collaboration with the INCIBE, makes available to those organizations that provide essential services include: support against incidents, a devoted cyberincidents response team (CERTSI_), early warning services, planning and development ciberexercises, and non diclosure agreements for information sharing. At the same time, the Cyber Coordination Office, of the Ministry of the Interior, is entitled to carry out operational coordination between all these actors and the Law Enforcement Agencies, whose capabilities of investigation and crime pursuit are provided by the technological units of the Civil Guard and the National Police.

Finally, this chapter ends accounting for a number of tools that could be useful to further enhance the public-private partnership.

Keywords

Cyberattack, threat, stuxnet, blackenergy, regulation, public-private partnership, CERT (computer emergency response team), critical infrastructures, essential services, planification.

Introducción

Tras los últimos ciberataques conocidos contra los servicios esenciales de diferentes países de nuestro entorno, con distintos grados de afección sobre los que se conocen como infraestructuras críticas y sus redes de comunicaciones, cabe, en buena lógica, hacerse la pregunta de cómo de resistente y adaptable es la sociedad moderna e hipertecnificada de hoy a, por ejemplo, la dependencia del suministro de energía, agua o medios de pago.

Si una gran ciudad, o una extensa zona de un territorio cualquiera, sufriese un ciberataque, dirigido por otro Estado o por terroristas, que lograse eventualmente una caída del servicio eléctrico, del transporte público o de las telecomunicaciones durante, digamos, veinticuatro horas ¿cómo respondería la población?, ¿cómo responderían los mercados?, ¿cómo responderían nuestros sistemas de emergencia?, ¿cuándo se restituirían los servicios?, es más, ¿a qué otros servicios podría arrastrar un posible «efecto dominó»? y, sobre todo ¿cuáles serían sus consecuencias?

Preguntas como estas podrían repetirse *ad eternum* pero lo que parece claro es que nuestra sociedad, la sociedad postmoderna, no solo no está aún preparada, sino que ni siquiera contempla un posible fallo generalizado de los servicios esenciales sobre los que pivotan nuestra vida económica, política, social y nuestra propia supervivencia como individuos. Esto mismo es lo que ha convertido a los servicios esenciales y a las infraestructuras críticas que los sustentan en un objetivo de primer nivel y es lo que ha provocado que las naciones modernas se hayan puesto manos a la obra para proteger estos activos que suponen la columna vertebral del mismísimo estado del bienestar.

El estudio de los ataques realizados contra infraestructuras estratégicas nos sirve para confirmar que una empresa privada no puede defenderse por sí misma de ataques cada vez más sofisticados y agresivos. La desproporción entre los medios con los que cuenta el atacante y el defensor hace que solo sea cuestión de tiempo el que aquel consiga el objetivo planteado. Por otra parte, el paradigma de la globalización ha hecho posible que, por primera vez en la historia de la humanidad, las grandes amenazas contra los Estados no tengan por qué provenir de otros Estados, sino que han entrado en juego otra serie de actores cuyas capacidades pueden poner en jaque o desestabilizar países enteros. De la misma manera, la participación del sector privado en la seguridad nacional, dados los recursos y la información que maneja, no es ya un factor meramente deseable sino que se ha convertido en una verdadera necesidad.

La colaboración público-privada viene a dar algunas de las claves y también algunas de las herramientas apropiadas para que las empresas privadas y los propios Estados puedan defenderse con mayores garantías contra estas amenazas de nuevo cuño.

En España esta colaboración es ya un hecho, sin perjuicio de que aún queda mucho camino por recorrer. Varios de los sectores estratégicos de nuestro

país, si bien es verdad que en diferentes escenarios de madurez, trabajan de forma coordinada y regular con el Centro Nacional para la Protección de las Infraestructuras Críticas y, a través de este, con el *CERT* de Seguridad e Industria (CERTSI_) en la protección de los sistemas informáticos que dan soporte a las infraestructuras críticas del país. Muestra objetiva de ello es que, tan solo en la primera mitad de 2016, este *CERT* había trabajado ya sobre doscientos sesenta y dos incidentes reportados sobre activos críticos de nuestro país. Más del doble que en todo 2015 (ciento treinta y cuatro). Y más del cuádruple que en todo 2014 (sesenta y tres)[1].

Como indicaba en el párrafo anterior, el trabajo que el CNPIC viene realizando contempla varios escenarios de madurez. Uno de los más satisfactorios, en cuanto a los resultados y en cuanto a la obtención de la sinergia necesaria, viene llevándose a cabo con el sector eléctrico español, de los que ENDESA, que ha tenido a bien colaborar con nosotros en este artículo, es uno de sus mejores representantes. El camino recorrido por el momento en este modelo de colaboración público-privada es un posible caso de éxito que estamos intentando replicar en muchos otros proyectos que ahora estamos iniciando.

Un poco de historia

Con el inicio del siglo XXI aparece una nueva tipología de ciberataques muy sofisticados, llevados a cabo por grupos organizados apoyados por Estados o directamente por esos Estados. El objetivo inicial era robar información estratégica que sirva a los intereses del atacante. Con el tiempo, ese objetivo inicial se amplía a otros más ambiciosos como el bloqueo de servicios públicos o la toma de control de sistemas industriales, que permitan manejar en remoto infraestructuras estratégicas para el funcionamiento del país.

Este tipo de ataques suponen un nuevo tipo de amenaza llamada *APT* (*Advanced Persistent Threat* o Amenaza Persistente Avanzada). Las amenazas persistentes avanzadas[2] suelen manifestarse como un *malware* (*software* malicioso) en el que se invierten millones de dólares, que persigue objetivos muy concretos, tras el que, en un buen número de casos, se pueden encontrar Estados u organizaciones terroristas o criminales y que está especialmente diseñado para mantenerse oculto en el sistema atacado y que aprovechan vulnerabilidades de *software* desconocidas hasta ese momento o usan técnicas de ingeniería social muy concretas con las que infectar al personal de la empresa objetivo.

En este tipo de amenazas, las medidas de seguridad habituales no son efectivas ya que el *malware* se ha diseñado para que las herramientas de segu-

[1] Fuente: CERTSI_. *Informe Situación Ciberseguridad*. Septiembre de 2016.

[2] Fuente: CNPIC. *Ciberdelicuencia, ciberterrorismo, y protección de infraestructuras críticas*. Documento PIC_8_1.pdf

ridad no las detecten y por lo tanto no actúe contra él. Los sistemas de seguridad utilizados actualmente en las empresas como antivirus, *IPS* (Sistemas de Protección de intrusiones) o *firewalls* (cortafuegos), basan la detección de *malware* en el uso de bases de datos de firmas de *malware* conocido. Es decir, de *software* que sabemos que es malicioso. Pero si es la primera vez que se usa este *software* los sistemas de seguridad no lo detectarán. Esto provoca la dificultad para identificar el *malware* y por lo tanto para tratarlo de forma eficaz.

Actualmente, los sistemas informáticos ocupan un lugar central en nuestra vida, dando soporte a multitud de procesos industriales, procesos ligados a nuestra actividad económica y social, como los ligados a la energía, el agua o el transporte. Como activos importantes de un país, dentro de un conflicto internacional, estos sistemas se han convertido en objetivos atacables y, por supuesto, en potenciales objetivos terroristas. El concepto de guerra informática o ciberguerra hace referencia al desplazamiento de un conflicto que toma el ciberespacio y las tecnologías de la información como campo de operaciones. Podemos definir la guerra cibernética como «el conjunto de acciones llevadas a cabo por un Estado para penetrar en los ordenadores o en las redes de otro país con la finalidad de causar prejuicio o alteración».

La ciberguerra ya ha sido empleada en diversos conflictos, tanto en ofensivas militares de un país contra otro como de un grupo terrorista en contra de un gobierno.

Estos son algunos de los ataques más importantes que se han realizado en los últimos años:

- BlackEnergy, Ucrania 2015. Este *malware* de tipo «troyano», programa malicioso que permanece oculto en el equipo infectado y ofrece al atacante acceso remoto al mismo, infectó a varias compañías eléctricas ucranianas y provocó apagones de varias horas en la ciudad ucraniana de Ivano-Frankivsk.
- Stuxnet, Irán 2010. Stuxnet es un el primer gusano (*software* malicioso que se duplica a sí mismo) conocido dedicado a espiar y manipular sistemas industriales. El ataque tuvo como objetivo los sistemas de centrifugado de las plantas de enriquecimiento de uranio de Irán, logrando retrasar el programa nuclear iraní durante al menos dos años.
- Ciberataque a Estonia, 2007. El traslado en Tallin del Soldado de Bronce, monumento a los soviéticos caídos durante la II Guerra Mundial, provocó un ciberataque el 27 abril de 2007 que consiguió bloquear el acceso a sitios web de organizaciones públicas y privadas de Estonia, incluidos el Parlamento, bancos, ministerios y periódicos. En el momento álgido de los ataques, los teléfonos móviles y las tarjetas bancarias dejaron de funcionar.
- Titan Rain, EEUU 2003. «Titan Rain» fue el nombre en clave que se le asignó a una serie de ataques coordinados sobre sistemas de información de Estados Unidos llevados a cabo desde 2003 hasta 2006, con posi-

ble origen en China. Los atacantes lograron acceso a las redes corporativas de empresas que gestionaban información sensible, como Lockheed Martin, Redstone Arsenal y la NASA, entre otros.

En este tipo de ataques debemos tener en cuenta que las medidas de seguridad habituales no son suficientes. La amenaza ha cambiado, el atacante está muy preparado y cuenta con el personal y los recursos adecuados para atacar cualquier sistema. Tradicionalmente, las empresas trabajan en un perímetro de seguridad donde se mantienen seguros sus equipos informáticos, utilizando programas de formación y concienciación para que su personal sepa actuar frente a las nuevas amenazas. Sin embargo, esto no es suficiente, hoy en día es necesaria la existencia en las empresas de equipos de respuesta especializados en la prevención y gestión de este tipo de incidentes. Estos equipos especializados deben trabajar junto a los *CERT* (*Computer Emergency Response Team*) nacionales en el tratamiento de los ataques y en mantener información actualizada de las amenazas y ataques que puedan afectar a su sector. La información obtenida deben transmitirla dentro de sus organizaciones a las distintas áreas afectadas y muy especialmente a aquellas que proporcionan los servicios esenciales a la sociedad, de la forma más ágil posible, estableciéndose una relación de confianza que permita el trabajo conjunto y transparente frente a cualquier amenaza entre el *CERT* y los equipos especializados existentes en las empresas.

Para entender mejor estas amenazas vamos a profundizar en estos casos por su carácter de referente en este tipo de ataques.

BlackEnergy

En 2013 se inició un conflicto entre Ucrania y Rusia provocado por el acercamiento de la primera a la Unión Europea. Como consecuencia de este conflicto, la península de Crimea, con una población mayoritariamente prorusa, se independizó de Ucrania para adherirse a la Federación Rusa.

Enmarcado en este conflicto se produce el ciberataque BlackEnergy, ejecutado el 23 de diciembre de 2015, con el objetivo de sabotear los sistemas de control de infraestructuras públicas ucranianas. En él varias distribuidoras eléctricas fueron comprometidas por el troyano BlackEnergy dejando a los hogares de la región ucraniana de Ivano-Frankvisk (con una población de alrededor de 1,5 millones de habitantes) sin electricidad.

Sin embargo, este no ha sido el único caso de ataque ocurrido a sistemas de control en Ucrania ya que a comienzos de 2016 se produjo un ataque a los sistemas informáticos del aeropuerto de Kiev con la intención de provocar el caos y el desconcierto tras la afección del servicio aéreo. Las noticias coinciden en que el *malware* detectado es similar a BlackEnergy, aunque en este caso se detectó en sus estados iniciales y pudo ser eliminado sin tener con-

secuencias. En noviembre de 2015 también se produjo otro ataque a cadenas de televisión y medios con características similares a los descritos.

BlackEnergy es un troyano, programa malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. El objetivo del programa es, obviamente, poder controlar en remoto el equipo infectado.

La vía de infección utilizada en el caso que nos ocupa fue el envío de correos electrónicos con documentos adjuntos infectados, suplantando al emisor. Estos correos se enviaban a personas seleccionadas de las compañías eléctricas afectadas.

El vector de ataque utilizado para la infección es la explotación de vulnerabilidades de los programas Microsoft Word, Excel y Powerpoint.

El funcionamiento de BlackEnergy[3] puede resumirse en tres funciones:

- Comunicación con el servidor de comando y control que lo dirigirá. Es una de las primeras acciones que intenta realizar BlackEnergy para, a continuación, poder descargarse nuevos componentes y llevarse la información sustraída.
- Escaneos de red que buscan generalmente servicios abiertos relacionados con protocolos del sector de la energía como ICCP o IEC-104 para obtener información de la red.
- Envío de comandos para la ejecución de órdenes que incluyen múltiples aperturas y cierres de interruptores de circuitos, más comúnmente conocidos como *breakers*, en un espacio limitado de tiempo.
- Borrado de archivos de sistema para que el rearranque sea lo más difícil posible.
- Borrado de los eventos/registros de Windows para borrar las evidencias de las actuaciones realizadas.

El objetivo buscado con estas actuaciones es provocar el mayor daño posible y la incapacidad para arrancar de nuevo los sistemas. Precisamente, al ser estos los sistemas que gestionan la infraestructura eléctrica, su inhabilitación tiene como consecuencia provocar primero la caída del sistema eléctrico y después dificultar la restitución del servicio.

Stuxnet

En 2006 Irán retomó su programa nuclear con la puesta en marcha de un grupo de centrifugadoras para el enriquecimiento de uranio en la planta de enriquecimiento de combustible de Natanz. Ante la sospecha de que se pudiera hacer un uso militar del uranio enriquecido, aumentaron las presiones

[3] Fuente: CERTSI. https://www.certsi.es/blog/blackenergy-sistemas-criticos y https://www.certsi.es/blog/protegiendose-blackenergy-detectando-anomalias

de la comunidad internacional, lideradas por la ONU y Estados Unidos, para que Teherán abandonase estas actividades.

Ante esta hipotética amenaza nuclear iraní surgió Stuxnet, con el objetivo de retrasar o paralizar el programa nuclear iraní. El origen del *malware* parece encontrarse en una colaboración entre la National Security Agency de Estados Unidos e Israel.

Stuxnet es un gusano informático, programa malicioso que se duplica a sí mismo y que afecta a equipos con Sistema Operativo Windows que tienen instalado *software* de Siemens para el control de plantas industriales. Con Stuxnet se infectó la planta de combustible de Natanz, consiguiendo que se modificaran periódicamente las condiciones de funcionamiento de las centrifugadoras (necesarias para el enriquecimiento de uranio, que a su vez es el combustible usado para provocar una reacción nuclear) causando un gran estrés a los rotores y provocando roturas en los mismos. Se calcula que en el momento más álgido del ataque fueron afectadas unas mil centrifugadoras.

El primer ataque fue en 2008, consiguiendo dejar fuera de control las primeras centrifugadoras afectadas que al mismo tiempo enviaban parámetros de funcionamiento normal al Centro de Control de Natanz. Esto provocó un importante daño físico a las centrifugadoras pero también una falta de confianza por parte de las autoridades iraníes en sus técnicos y sistemas de control, que acabaron solicitando ayuda a técnicos internacionales para tratar de entender la situación.

La vía de infección utilizada fueron dispositivos de memoria USB distribuidos entre personal seleccionado del programa nuclear Iraní y el personal con acceso a la planta de Natanz.

El vector de ataque utilizado para la infección fue la explotación de vulnerabilidades aún no conocidas, llamadas vulnerabilidades de día 0, de Microsoft y Siemens.

Stuxnet[4] es el primer ciberataque que de forma masiva consiguió una destrucción física de su objetivo, en este caso las centrifugadoras. Esta puede haber sido la primera vez que una potencia haya utilizado armas cibernéticas para paralizar la infraestructura de otro país, logrando, con un *software* informático lo que hasta entonces solo se podía lograr mediante el bombardeo de un objetivo o el sabotaje mediante explosivos. Según la Administración estadounidense[4] el ataque provocó un retraso de entre dieciocho meses y dos años en el desarrollo del programa nuclear iraní.

Aunque el ataque consiguió su objetivo, también provocó problemas importantes al extenderse a otras infraestructuras vulnerables, fundamentalmente de Irán, pero también de otros países como Indonesia, India, Paquistán,

[4] Fuente: *New York Times*. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Rusia, Cuba e incluso los propios Estados Unidos. Seguramente, gracias a esta infección masiva y no prevista en otros países, se ha conocido y podido estudiar el ataque que de otra forma podría haber pasado inadvertido.

Ciberataque a Estonia 2007

En 2007 se iniciaron una serie de protestas en Estonia como consecuencia del traslado del Soldado de Bronce (monumento soviético homenaje a los soldados caídos en la II Guerra Mundial) desde el centro de Tallin a un cementerio. En Rusia este traslado se consideró una ofensa.

Estonia era ya entonces un país con una alta dependencia de las tecnologías de la información, donde muchos servicios públicos eran ofrecidos mayoritariamente por dichas nuevas tecnologías. Esto originó que las protestas derivasen pronto en ataques cibernéticos, provocando la caída de los sistemas objetivo y por lo tanto la falta de disponibilidad de los servicios ofrecidos por estos. En el momento álgido de los ataques, además de numerosos servicios públicos, los teléfonos móviles y las tarjetas bancarias dejaron de funcionar.

Este tipo de ataques es conocido como *DDoS*, acrónimo en inglés de Denegación de Servicio Distribuida, haciendo alusión a un ataque realizado simultáneamente desde muchos equipos que lanzan multitud de peticiones contra el servidor objetivo. Este es uno de los ataques más populares en internet, por su eficacia y sencillez.

Los principales objetivos fueron las páginas web del presidente de Estonia, del Parlamento, de las instituciones de gobierno, de los medios de comunicación y de los bancos del país. El país finalmente se aisló del internet exterior, para poner fin a los ataques.

El ataque provocó la respuesta de la OTAN que ayudó a Estonia desde el Centro de Ciberdefensa, desde donde se realiza el seguimiento de este tipo de incidentes. Este ataque se considera el primer ciberataque por denegación de servicio organizado contra un país del que se tiene noticia.

Titan Rain

Este ataque se inició en 2003 y duró al menos tres años. Se relaciona con el Gobierno chino y su necesidad de tecnología para el crecimiento de un país que se estaba convirtiendo en una nueva potencia mundial.

El Gobierno estadounidense acusó al Gobierno chino de estar detrás del ataque, lo que provoco enfrentamientos diplomáticos entre ambos gobiernos. Adam Paller, director del Instituto SANS (especializado en Seguridad de Sistemas), indicó que el ataque fue realizado por personal con una «intensa disciplina» y que «ninguna organización puede hacer esto a menos que sea un ejército», apuntando la autoría al Ejército chino.

Titan Rain atacó múltiples objetivos gubernamentales y empresariales de Estados Unidos y de Gran Bretaña. Entre los gubernamentales se encontraban: la NASA, el FBI, o el Departamento de Defensa, así como el Foreign Office británico. Respecto a las empresas afectadas, destacaron las relacionadas con proyectos de defensa como Loockheed Martin o el Laboratorio Nacional Sandia, dependiente del Departamento de Energía de los Estados Unidos, cuyos proyectos tienen por objetivo la prueba de componentes en armas atómicas, el desarrollo de los programas de energía y del medio ambiente, así como la protección de las infraestructuras nacionales.

Los *hackers* usaron ordenadores y páginas web chinas, con un bajo nivel de seguridad, utilizándolos como vía de infección para llevar a cabo el ataque, protegiendo de esta forma su origen.

Pilares de la colaboración en la protección de las infraestructuras críticas

Las infraestructuras críticas dan servicio a amplias extensiones de territorio y a un número muy elevado de personas, empresas e industrias. Por lo tanto, por definición, el impacto de la caída de una de ellas debe ser necesariamente global y extenso. Y ello convierte en dependientes tanto los servicios que proporcionan estas infraestructuras como las propias infraestructuras entre sí.

Hay que recordar, precisamente, que por «dependencia» se entiende la relación entre dos productos o servicios en la cual un producto o servicio es necesario para la generación del otro. En el caso que nos ocupa, las dependencias incluyen tanto los servicios esenciales como las infraestructuras que los soportan. De esta manera, para que las infraestructuras funcionen de manera adecuada se necesita de los servicios suministrados por otras infraestructuras o segmentos del mismo sector o de otros sectores diferentes y esto es lo que se conoce como interdependencias[5].

Lo que sí es cierto es que, ya sea a través de la conectividad, las políticas y procedimientos directos o la proximidad geoespacial, los sistemas críticos de infraestructuras interactúan y de forma cada vez más acusada. Estas interacciones crean a menudo complejas relaciones que se cruzan entre sí. Sin embargo, el modelado y el análisis de las interdependencias entre las infraestructuras y sus elementos críticos es un fenómeno relativamente nuevo y tremendamente complejo.

Los propietarios y gestores de infraestructuras, históricamente interesados en el correcto funcionamiento de sus propias instalaciones, a menudo muy

[5] Parlamento de España: Ley 11/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas (artículo 2.j). https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

bien acotadas, deben ahora lidiar con los problemas provocados por la ilimitada conectividad de las redes y de la tecnología.

Hay una necesidad creciente de analizar y comprender mejor la influencia que tienen entre sí múltiples sectores, que pueden inducir efectos secundarios potencialmente imprevistos sobre los demás, ya sea directa o indirectamente, y que pueden derivar, en casos extremos, en la generación de efectos cascada, o dominó, de consecuencias difícilmente previsibles[6].

En España, de acuerdo a nuestra legislación vigente, se entiende la Protección de las Infraestructuras Críticas (PIC) como el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de los servicios esenciales con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra las infraestructuras que los soportan y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia[7]. Así, en nuestro país, las políticas sobre PIC se sustentan en cinco principios básicos, todos ellos alineados con la Estrategia Nacional de Seguridad de 2013, que dotan de cohesión y coherencia a todo el sistema[8]. Estos son:

1. Coordinación.
2. Responsabilidad compartida y cooperación público-privada entre los diferentes agentes.
3. Equilibrio y eficiencia.
4. Planificación escalonada.
5. Resiliencia[9].

En nuestro país, la mayoría de las infraestructuras críticas pertenecen o están operadas por compañías privadas, como ya se ha apuntado. Esta situa-

---

[6] En el ensayo de Duddenhoeffer, Perman y Manic, publicado por el *Idaho National Laboratory*, los autores establecen el concepto de «nodo» y de «borde», para clarificar las diferentes relaciones de dependencia existentes entre las infraestructuras de servicios esenciales. De esta manera, para Duddenhoeffer «un nodo de infraestructura es una entidad que actúa como fuente, produce, consume o transforma un recurso (..) de la misma manera, sin embargo, un nodo puede representar factores políticos o sociales de influencia que no se manifiestan en forma física, pero que pueden afectar físicamente a la propia infraestructura». Por otra parte, el «borde es una entidad física o virtual queactúa como un conducto para el flujo para una cantidad física, información o influencia. Por lo tanto, un borde (o arco) entre dos nodos representa un nivel directo de dependencia». https://inldigitallibrary.inl.gov/sti/3578215.pdf

[7] Ibidem, 5.

[8] De la Corte, Luis, *et al*. *Seguridad nacional, amenazas y respuestas*. Madrid, Editorial LID (2014).

[9] El completo trabajo de John D. Moteff, realizado en agosto de 2012 para el Servicio de Investigación del Congreso de Estados Unidos efectúa una primera aproximación al término resiliencia desde el punto de vista de la pérdida y recuperación de los niveles de operación habituales de un proveedor determinado. Más interesante es la propia medida del término, su combinación con los factores de riesgo y las medidas y políticas esbozadas para mejorar los niveles de resiliencia existentes.
https://www.fas.org/sgp/crs/homesec/R42683.pdf

ción hace imprescindible que tanto las Adminstraciones Públicas como los operadores privados trabajen, asumiendo la responsabilidad que a cada uno les corresponda y de forma coordinada, en la protección de las infraestructuras críticas antes, durante y después de un eventual evento negativo. La plasmación de esta idea invoca el segundo de los principios arriba reflejados: el de la responsabilidad compartida y la cooperación público-privada[10].

Independientemente de la manera de obtenerlo, el éxito de cualquier modelo de cooperación público-privada debe estar basado en todas o algunas de las siguientes premisas:

– **Confianza.** Dado que la materia PIC aborda cuestiones muy sensibles, es esencial crear una atmósfera de confianza en la que ambas partes sean conscientes de la necesidad de cada uno de ellos de actuar con la discreción debida. Mantener una relación de confianza entre la Administración y las empresas privadas es fundamental para hacer crecer la colaboración[11]. Por la experiencia adquirida, se puede constatar que para fomentar la confianza son necesarios puntos de contacto únicos en ambas partes, con capacidad de decisión dentro de su organización, que tengan conocimiento de las posibilidades que tiene la otra parte para obtener el máximo partido de la relación. Además, es clave fomentar la colaboración en otras actividades de ciberseguridad, como ciberejercicios, cuestionarios, gestión de incidentes menores, participación en foros... de forma que sean naturales y automáticos los procedimientos de colaboración frente a cualquier tipo de actuación que deba realizarse conjuntamente en un futuro entorno real. La creación de mecanismos de cooperación informal entre el personal de ambas entidades es también una faceta indispensable para mejorar la confianza entre la Administración competente y la empresa. La confianza entre ambas partes permitirá, además, una mayor agilidad en la compartición de la información y la rapidez en la toma de decisiones que permitan gestionar el incidente eficazmente. Un ejemplo significativo del trabajo conjunto en España en esta materia se produjo precisamente en el marco del ataque BlackEnegy, ya comentado en páginas anteriores. Desde el *CERT* de Seguridad e Industria (CERTSI_), operado conjuntamente por el INCIBE y el CNPIC, se informó puntualmente sobre el ataque a las empresas del sector energético español como posibles objetivos de un ataque similar. La información que se compartió incluía un nivel ejecutivo, necesario para ayudar

[10] Conceptos ambos introducidos en el estudio de la Comisión Europea *Inventory of Crisis Management Capacities in the European Commission and Community Agencies*, mayo de 2010. Documento no público.

[11] Esta necesidad fue planteada como una de las conclusiones principales en el *Manual de Buenas Prácticas para las Políticas PIC* (RECIPE), publicado por la Dirección General de Interior de la Comisión Europea en marzo de 2011. http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/FINAL_RECIPE_manual.pdf

a entender la amenaza a la Alta y Media Dirección[12], y, obviamente, un nivel técnico dirigida a los operadores especializados de cada organización que desvelaba, entre otros parámetros, el origen del *malware*, la vía de transmisión, las vulnerabilidades explotadas, los indicadores de compromiso y las medidas necesarias para prevenirlo. Esto permitió a las empresas del sector implantar en sus organizaciones las medidas planteadas, permitiendo adelantarse a una repetición de ese mismo ataque y reforzando el sistema, en este caso eléctrico, de nuestro país.

- **Intercambio de información**. Que debe ser en ambas direcciones, válido para ambas partes y basado en presupuestos de confidencialidad y explotabilidad[13].
- **Respeto**. Ambas partes deben reconocer el valor añadido que supone la participación de la otra parte en la colaboración.
- **Transparencia**. Tanto en los procedimientos generales como en la información que se pone a disposición de la otra parte. La transparencia permite generar el ambiente necesario para que la colaboración sea fructífera pero para que tenga continuidad debe darse en ambos sentidos. La transparencia por parte de la Administración pública competente (en este caso, el CNPIC) permitirá compartir con las empresas privadas la información de incidentes que puedan afectar a estas, así como los medios con los que cuenta para poder ayudarles. Todo ello les ofrece a las empresas privadas un tiempo fundamental para preparar la respuesta a estos incidentes. Por su parte, la transparencia desde la empresa privada hacia la Administración, tanto en incidentes como en lo relativo a medios disponibles, permite una valoración del incidente por el órgano competente y posibilita una compartición de la información del incidente con otras entidades del sector que les permitirá tomar las medidas adecuadas para anticiparse al incidente.
- **Marco regulatorio claro**. Los operadores quieren saber claramente a qué se deben atener. Es recomendable tener pocas leyes y simples y, sobre todo, evitar duplicidades[14].
- **Neutralidad**. En el marco en el que se desarrolla la colaboración PIC no pueden existir intereses partidistas ni económicos[15].

---

[12] La implicación de la Alta Dirección en las políticas de seguridad a implantar por la organización es una condición *sine qua non* exigida por el CNPIC a la hora de plasmar los diferentes planes derivados de la Ley 8/2011. Fernando Sánchez, en el libro *Marco legal y de gestión de la protección de las infraestructuras críticas*, coordinado por Francisco J. Vanaclocha, asegura que «es preferible una aproximación voluntaria a la imposición, pero de alguna manera debe instarse a la cooperación de los operadores. El establecimiento de marcos de gobierno y la obtención del compromiso de la alta dirección es esencial para ello».

[13] Ibíd. 11. Esta necesidad de intercambio de información es precisamente lo que subyace tras la Propuesta de decisión del Consejo de 27 de octubre de 2008 relativa a una Red de información sobre alertas en infraestructuras críticas (CIWIN) [COM(2008) 676 final]. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52008PC0676

[14] Ibíd. anterior.

[15] La labor de «árbitro» del Sistema, como uno de los objetivos específicos de la legislación española sobre protección de infraestructuras críticas viene justificada por Fernando

- **Interés común**. Los resultados obtenidos deben beneficiar a ambas partes, de forma que exista el necesario *quid pro quo*.
- **Conciencia de las posibilidades y restricciones de cada uno**. Esto implica que cada parte debe conocer qué es lo que hace el otro y qué se le puede pedir.
- **Expectativas realistas**. En línea con lo anterior. Hay que tener en cuenta cuáles son los recursos, capacidades y limitaciones de cada uno para diseñar objetivos alcanzables. Algunas de las acciones que se pueden desarrollar, como ejemplo, podrían ser:

  - Conocimiento mutuo.
  - Participación en estrategias e iniciativas comunes.
  - Elaboración de guías, estándares o buenas prácticas.
  - Ejercicios y simulacros sectoriales
  - Empleo operativo: basado en una correcta capacidad de interlocución y reacción.

Lo que parece claro es que los pilares de la colaboración público-privada, más allá del cumplimiento de la legislación en curso, deben ser conceptos como los que se acaban de citar. Es únicamente sobre estas bases sobre las que se podrá construir una relación sólida que permita el intercambio fluido de información y el trabajo conjunto en aquellos incidentes que así lo necesiten. Y más, si el «campo de batalla» donde se va a operar debe hacer frente a una amenaza virtual cada vez más agresiva y sofisticada.

El sistema de planificación PIC y su encaje con la ciberseguridad

Normativa PIC, colaboración público-privada y ciberseguridad

La protección de las infraestructuras que aseguran el mantenimiento de los servicios esenciales se ha convertido en una prioridad para las diferentes naciones, teniendo en cuenta la dependencia que la sociedad tiene de los mismos y que incrementa exponencialmente año a año.

Por este motivo, en el ámbito de la Unión Europea, se aprobaron primero el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC)[16] y, más tarde, la Directiva 2008/114 del Consejo de la Unión Europea, de 8 de diciembre[17]. Ambos documentos vinieron precedidos en el tiempo por sendas Comunicaciones de la Comisión al Consejo y al Parlamento Europeo, donde

Sánchez en el artículo «Las políticas de protección de infraestructuras críticas en España», publicado en la *Revista Seguridad y Ciudadanía* n.º 11, de junio de 2014 (pp. 33 y ss.).

[16] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52006DC0786. El PEPIC se basó de manera muy especial en el *Libro Verde de 17 de noviembre de 2005, sobre un Programa Europeo para la Protección de Infraestructuras Críticas* [COM (2005) 576 final (no publicado en el Diario Oficial).

[17] https://www.boe.es/doue/2008/345/L00075-00082.pdf

se pedía la puesta en marcha de medidas urgentes en la lucha contra el terrorismo, tanto en su prevención, prevención y respuesta, como en la preparación y gestión de las posibles consecuencias[18].

A nivel nacional, las políticas sobre protección de infraestructuras críticas empezaron a ver la luz de forma temprana respecto a otras naciones de nuestro entorno. Ya en 2007 se aprobó, en mayo, un primer Plan Nacional para la Protección de las Infraestructuras Críticas que fue seguido en noviembre por la creación del Catálogo Nacional de Infraestructuras y la aprobación de un Acuerdo sobre Protección de Infraestructuras Críticas, que tuvo como primera consecuencia el nacimiento del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)[19].

El CNPIC, actor central desde ese momento en el campo que nos ocupa, se configura de este modo como el órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior (Autoridad competente en esta materia) en relación con la protección de las infraestructuras críticas en el territorio nacional[20].

Figura 5.1. Logo CNPIC.

El complejo carácter que la seguridad nacional ha adquirido en los últimos años, unido todo ello a la ya mencionada enorme dependencia que la sociedad actual tiene del sistema de infraestructuras que asegura la prestación de los servicios esenciales, evidenció, ya entonces, la necesidad de poner en práctica estrategias y políticas en esta materia para garantizar la seguridad en la normal prestación de los servicios esenciales frente a amenazas derivadas de posibles ataques deliberados[21].

[18] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52004DC0701
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52004DC0698

[19] http://www.cnpic.es/index.html

[20] Parlamento de España: Ley 11/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas (artículo 7). https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

[21] La prestación de los servicios esenciales y la disponibilidad de los mismos tiene un enlace claro con el concepto de continuidad de negocio aplicado por la mayoría de las com-

En España, se consideró prioritario desde aquel momento integrar en estas estrategias a las amenazas provenientes del ciberespacio como un potencial elemento disruptivo del normal funcionamiento de las infraestructuras críticas. El tiempo, vistos los acontecimientos que han tenido lugar en la última década, ha dado la razón a esa decisión estratégica que entonces adoptó el Ministerio del Interior a la hora de apostar por un concepto de seguridad integral, entonces muy incipiente a nivel internacional, que aunase las políticas, metodologías y operaciones concernientes a la seguridad física de los activos y las relativas a la seguridad lógica, o cibernética, de las redes y sistemas[22].

El panorama de seguridad internacional, la irrupción del terrorismo internacional y el auge del crimen organizado, como se acaba de mostrar, no han hecho sino poner de manifiesto los efectos que podrían tener sobre la salud pública, la industria o la economía nacionales determinados ciberataques dirigidos contra los sistemas de supervisión, control y adquisición de datos (sistemas SCADA) o los complejos sistemas informáticos que rigen el funcionamiento de los procesos de negocio y servicios de nuestras empresas estratégicas.

La legislación española, cuyo máximo exponente es la Ley 8/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas (comúnmente conocida como Ley PIC) introdujo como figura clave en las políticas del Gobierno el conocido como «Sistema de Protección de Infraestructuras Críticas»[23].

pañías privadas. De forma muy especial, el sector financiero tiene una notable madurez en la aplicación de políticas de continuidad de negocio que han arraigado con gran fuerza en la aplicación, por parte de las entidades de este sector estratégico, de la legislación sobre protección de infraestructuras críticas. Para mayor información sobre ello, consultar el artículo escrito por César Pérez-Chirinos en 2009, *Critical Financial Institutions: Business Continuity Scenarios and Costs*, en *European CIIP Newsletter*.
http://www.irriis.org/ecn/ECN %20issue %2012 %20v1 %2001.pdf

[22] El estudio *Protecting Critical Infrastructure in the EU* llevado a cabo por el *CEPS* (*Centre for European Policy Studies*) Task Force Report en 2010 (https://www.ceps.eu/system/files/book/2010/12/Critical %20Infrastructure %20Protection %20Final %20A4.pdf) efectúa, en este sentido, una clara recomendación al mencionar (p. 28-29*):* «the CEPS Task Force strongly recommends that a coordinated, holistic approach be adopted, encompassing both CIP and CIIP. An early recognition of the need for a coordinated approach between these two policy domains came in 2003 from the "G8 Principles for Protecting Critical Information Infrastructures" adopted by the G8 Justice & Interior Ministers, which clearly state that: In order effectively to protect critical infrastructures … countries must protect critical information infrastructures from damage and secure them against attack … Effective protection also requires communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies».

[23] El trabajo publicado en 2016 por la Fundación Borredá en el libro dirigido por César Álvarez, *El modelo de protección de infraestructuras críticas en España-Guía PIC*, desglosa los componentes del Sistema PIC y el esquema de planificación emanado de la Ley 8/2011.

Según dicha ley, el Sistema de Protección de Infraestructuras Críticas se compone de todos aquellos agentes (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. El Sistema se asienta, a su vez, en un sistema escalonado de planeamiento compuesto por los siguientes planes, ordenados de mayor a menor nivel: Plan Nacional de Protección de las Infraestructuras Críticas, Planes Estratégicos Sectoriales, Planes de Seguridad del Operador, Planes de Protección Específicos y Planes de Apoyo Operativo.

La piedra angular sobre la que se basa este Sistema, del cual su cúspide es la Comisión Nacional PIC, no es otra que un robusto esquema de cooperación en el que los diferentes agentes (y de forma muy particular los operadores críticos, sean estos públicos o privados) se encuentren representados y donde tengan capacidad de decisión a la hora de definir dichas políticas.

La forma de promocionar el Sistema PIC por el Gobierno de España, a través del Ministerio del Interior y del CNPIC, responde, en todo caso, a un delicado equilibrio en el que, por una parte, se requiere acceder a la cooperación mediante procesos de diálogo y colaboración genuina y, por otra, es preciso marcar una serie de reglas, de obligado cumplimiento, a las que todos los participantes han de acogerse. Todo ello es aún más importante en tanto en cuanto entran en juego aspectos cada vez más importantes, como es el

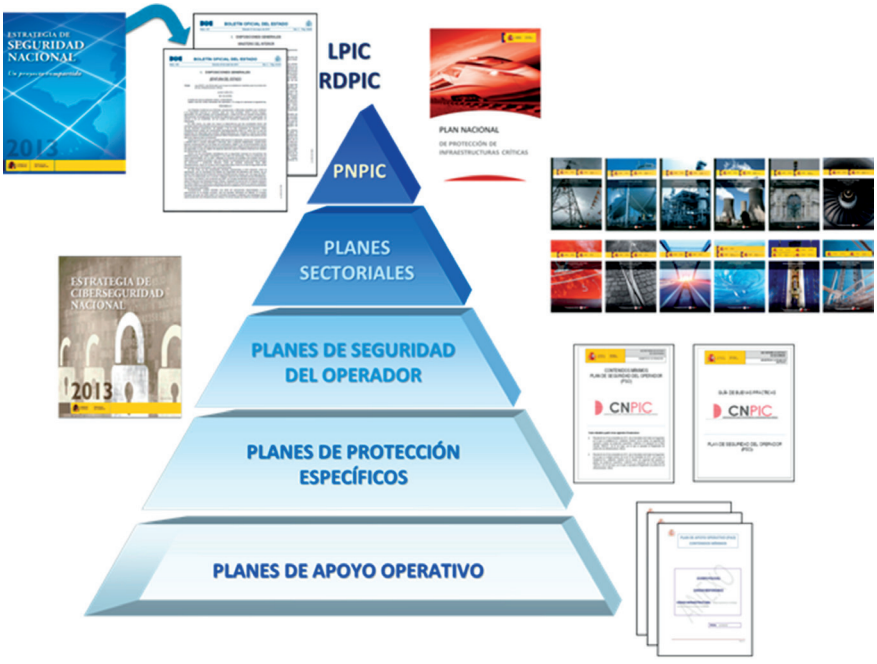

Figura 5.2. Esquema del Sistema PIC.

caso de la ciberseguridad, donde es fundamental contar con mecanismos ágiles e inmediatos de cooperación e intercambio de información entre todos los agentes implicados de alguna u otra manera en la securización del ciberespacio.

Por este motivo, se podría concluir en esta primera aproximación que la Ley PIC y el reglamento que la desarrolla (el Real Decreto 704/2011, de 20 de mayo)[24], han configurado un marco legal y una estructura organizativa que aporta un aire innovador para implantar una nueva política de seguridad, necesaria por otra parte, donde se establece la necesidad de garantizar la adecuada prestación de los servicios esenciales a través de mecanismos que posibiliten la seguridad integral de este tipo de infraestructuras. Para ello, la participación del sector privado es esencial y el modelo de colaboración público-privada, basado en preceptos de confianza y confidencialidad, la clave del mismo.

Nos detendremos a continuación brevemente sobre los cinco planes que conforman el esquema de planificación del Sistema PIC.

El Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC)

El Plan Nacional de Protección de las Infraestructuras Críticas (en adelante, PNPIC) representa la cúspide del complejo esquema de planificación integrada del que se ha dotado el Sistema PIC. Como ya se sabe, el PNPIC es elaborado por la Secretaria de Estado de Seguridad y tiene como objetivo establecer los criterios generales y las directrices precisas para movilizar las capacidades operativas del Ministerio del Interior, en coordinación con los operadores críticos y con el apoyo, en su caso, de las Fuerzas Armadas para articular las medidas preventivas necesarias para asegurar la protección permanente, actualizada y homogénea del conjunto de infraestructuras nacionales frente a aquellas amenazas de carácter deliberado que tengan como objetivo las mismas.

Este Plan, vigente desde mayo de 2007 y obsoleto en su mayor parte, se actualizó en febrero de 2016 mediante la instrucción número 1/2016 de la Secretaría de Estado de Seguridad. De este modo, se demuestra que la Secretaría de Estado de Seguridad, máximo órgano responsable del impulso y coordinación de las distintas medidas de seguridad de las infraestructuras críticas nacionales no es ajena, entre otras cosas, a las amenazas derivadas de este entorno digital en el que nos encontramos. En particular, consciente del auge de los incidentes contra activos digitales y lo que esto supone para el normal funcionamiento de los sectores estratégicos nacionales, el PNPIC garantiza la presencia de mecanismos de seguimiento de las labores de prevención, detección, respuesta y recuperación ante ciberincidentes.

[24] http://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf

El PNPIC se encuentra en su desarrollo operativamente vinculado con el Plan de Prevención y Protección Antiterrorista, también de reciente actualización (mayo de 2015). De este modo, el PNPIC complementa al anterior mediante el establecimiento de una serie de procedimientos de actuación asociados a cada uno de los niveles presentes en el conocido como «Nivel de Alerta en Infraestructuras Críticas» (NAIC). Para cada uno de los cinco niveles de los que consta el NAIC se determina un incremento gradual de las medidas de protección y vigilancia de las infraestructuras críticas nacionales. Como no podía ser de otra forma, en cada nivel NAIC se determinan una serie de medidas de seguridad, vigilancia y protección de carácter exclusivamente cibernéticas, medidas que afectan tanto a los órganos pertenecientes a Secretaría de Estado de Seguridad, al *CERT* de Seguridad e Industria (CERTSI) y a los operadores críticos nacionales.

Una de las principales novedades que presenta el PNPIC es la integración de todos los agentes del Sistema de Protección de Infraestructuras Críticas, entre los que cabe destacar, en materia de ciberseguridad, el rol que juegan los operadores críticos en el desarrollo de medidas de autoprotección, siendo fundamental el reporte de incidentes que afecten a su operativa diaria. Este nuevo requisito va acompañado de la necesidad de identificar en cada operador crítico la figura del Responsable de Seguridad TI corporativo (o CISO), como interlocutor natural en el ámbito de la ciberseguridad, con objeto de agilizar los intercambios de información específicos en la materia.

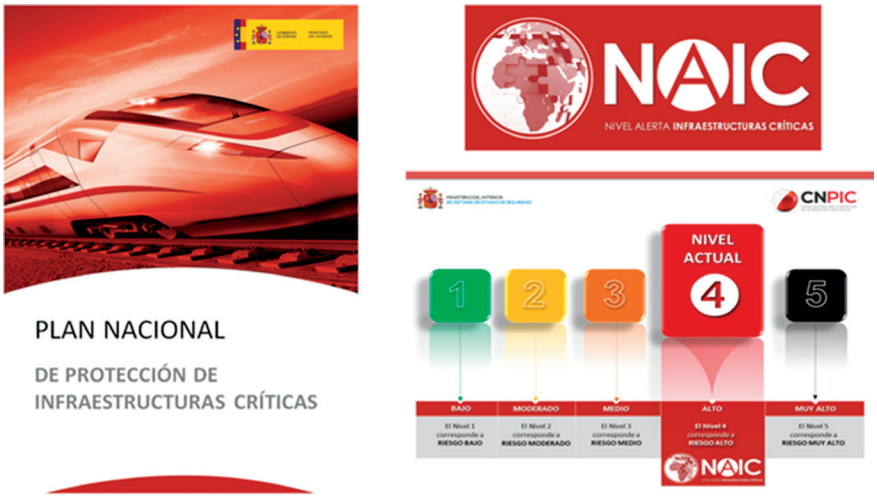

Figura 5.3. PNPIC.

Contenidos. Rasgos principales del nuevo PNPIC.

El PNPIC se estructura en un cuerpo principal y en un anexo, donde se recogen las medidas a implantar en cada nivel de activación del mismo por los diferentes agentes participantes. Al igual que el Plan de Prevención y Protección Antiterrorista, con el que está alineado, el PNPIC está clasificado como «Difusión Limitada», y su anexo como «Confidencial».

El PNPIC supone la culminación del Sistema de Protección de Infraestructuras Críticas emanado de la Ley 8/2011, PIC, y la implantación de todas las herramientas de planificación previstas en dicha norma. Asimismo, introduce como principal novedad la puesta en marcha de medidas operativas concretas sobre dos presupuestos fundamentales:

- La inclusión de la figura del operador crítico como partícipe del sistema de seguridad nacional.
- La inclusión de medidas de ciberseguridad, dando contenido al concepto de «seguridad integral».

La figura del Operador Crítico en el PNPIC.

Los principales actores participantes en el PNPIC son:

- Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Órgano ministerial encargado del impulso, la coordinación y la supervisión de cuantas actividades tiene encomendadas la Secretaría de Estado de Seguridad en relación con la Protección de las Infraestructuras Críticas, por lo que asume las funciones de coordinación del PNPIC.
- Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO). Órgano directivo de la Secretaría de Estado de Seguridad competente en la recepción, integración y análisis de la información estratégica disponible en la lucha contra todo tipo de terrorismo y radicalismo violento, encargado en lo respectivo a este Plan de la evaluación de la amenaza terrorista contra el Sistema de Protección de Infraestructuras Críticas (Sistema PIC).
- Fuerzas y Cuerpos de Seguridad del Estado (FCSE). Responsables de la protección a través de dispositivos preventivos y reactivos de las infraestructuras críticas que se encuentran ubicadas en su área de responsabilidad.
- Fuerzas Armadas (FAS). Encargadas de reforzar la protección a través de dispositivos preventivos y reactivos de las infraestructuras críticas que previamente se designen por el Ministerio del Interior.
- Operadores Críticos (OC). Los propietarios y/o gestores de las infraestructuras críticas que prestan servicios esenciales a la sociedad.

De todos ellos, la única figura que no está presente en el vigente Plan de Prevención y Protección Antiterrorista (PPPA) es la del operador crítico. El PNPIC prevé que este agente, emanado de la Ley 8/2011, sea corresponsable en la seguridad común en la parte que le afecta. Por ello, determina una serie de obligaciones y medidas operativas (que aparecen relacionadas tanto en el cuerpo como en el anexo del Plan) para su cumplimiento, estando además en coordinación con el propio PPPA. En este sentido, al operador crítico se le requiere entre otras cosas que:

- Designe obligatoriamente un responsable de Seguridad y Enlace que será a todos los efectos el punto de contacto natural entre el CNPIC y su organización.

- Los Planes de Protección Específicos (documentos de carácter operativo que se podrán ver en las siguientes páginas) tengan una graduación de medidas, donde se recojan los diferentes niveles de activación del PNPIC, y que deberán estar coordinados con los planes de los cuerpos policiales competentes.
- Acceda al intercambio de información y la actualización de datos de sus activos a una plataforma facilitada por el CNPIC (PI3), donde se centraliza la información disponible.
- Active los protocolos que se deriven del nivel de alerta declarado, en coordinación con las FCSE. Estos protocolos vienen recogidos en el anexo del Plan (cuatro medidas para el nivel 1, cinco para el nivel 2, otras cinco para el 3, cuatro para el nivel 4 y cuatro para el 5), siendo todas ellas, obviamente, acumulables.
- Participe en una mesa sectorial donde se evalúen los procedimientos de colaboración y comunicación existentes y se efectúe el seguimiento y coordinación de las medidas de protección activadas. Esta mesa se convocó el pasado día 15 de junio de 2016 por vez primera.

Igualmente, en el anexo del Plan vienen recogidos las responsabilidades y cometidos de los diferentes órganos del Ministerio del Interior (FCSE, CITCO y CNPIC) en cada uno de los niveles.

Las medidas de ciberseguridad en el PNPIC[25].

La ciberseguridad se incluye como complemento necesario a las medidas existentes tradicionalmente en el marco de la seguridad física. De esta forma, por primera vez se considera este aspecto en una instrucción operativa dictada por el Secretario de Estado de Seguridad. Entre otras medidas, destacan en el PNPIC:

- El rol del CERTSI_ y la Oficina de Coordinación Cibernética como interlocutores necesarios con los operadores en los diferentes niveles de alerta que se declaren.
- La obligación, por parte de los operadores críticos, de llevar a cabo labores de vigilancia digital y de reportar incidentes a los anteriores organismos. Para ello, se está trabajando en la definición de unos umbrales de seguridad (a partir de los cuales se debe comunicar el incidente) y en unos procedimientos concretos de intercambio de información.
- La designación de los responsables de Seguridad de la Información de los operadores críticos (CISO/responsables seguridad TI) para reportar incidentes y coordinarse con el Ministerio del Interior.

Como resumen, hay que apuntar que el PNPIC, al mismo tiempo que completa la batería legislativa que deriva de la Ley PIC, homogeniza las medidas operativas que contiene el Plan de Prevención y Protección Antiterro-

[25] *El modelo de protección de infraestructuras críticas en España-Guía PIC,* Editorial Borrmart S.A. dirigido por César Álvarez (pp. 37 y ss.).

rista, identificándose con los niveles de alerta consignados en este último. Finalmente, extiende responsabilidades y cometidos en ambos ámbitos a un nuevo actor, el operador crítico (en su mayoría organizaciones privadas), estableciendo un enlace operativo vinculante con la Secretaría de Estado de Seguridad y con las unidades de las FCSE a nivel territorial.

Los Planes Estratégicos Sectoriales (PES)

Los Planes Estratégicos Sectoriales tienen como misión principal conocer «cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento de estos, las infraestructuras estratégicas sobre las que se asientan, los operadores, propietarios o gestores de las mismas, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento»[26]. En definitiva, tiene por objeto obtener una idea global y completa de los diferentes sectores o subsectores estratégicos, de modo que se facilite y agilice tanto la identificación de operadores e infraestructuras críticas como las medidas necesarias para su protección, por lo que se puede decir sin temor a equivocarnos que estos planes son la base sobre la que se edifica todo el Sistema PIC. En lo que respecta a la ciberseguridad, los Planes Estratégicos Sectoriales permiten obtener información veraz de cuál es el nivel de dependencia del sector para con las tecnologías de información y comunicaciones.

Cabe destacar que el proceso de elaboración de un Plan Estratégico Sectorial es una tarea eminentemente técnica y multidisciplinar, de manera que es necesario el concurso de expertos tanto de la rama en cuestión como en seguridad. La mecánica de redacción de este tipo de planes exige la creación de grupos de trabajo complejos donde participan expertos de los diferentes ministerios competentes, otros organismos públicos y privados, empresas, operadores, consultoras y asociaciones profesionales.

A nivel global, el Plan Estratégico Sectorial (PES) se basa en un análisis general de riesgos donde se contemplan las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afectan al sector o subsector en cuestión en el ámbito de la protección de las infraestructuras.

Su elaboración, como ya se ha explicado, se lleva a cabo en el seno de un grupo de expertos incardinado dentro del Grupo de Trabajo (GTIPIC) y coordinado por el CNPIC. En estos trabajos, principalmente en el desarrollo del análisis de riesgos general y estratégico del sector, se cuenta con la participación activa y el asesoramiento técnico de aquellos operadores estratégicos identificados en cada sector. Un Plan Estratégico Sectorial tipo se

[26] José Ignacio Carabias, en su artículo «Protección de infraestructuras críticas y planificación». *Revista Seguritecnia*, n.º 409, junio de 2014.

estructura en cuatro capítulos, cuyo contenido se muestra sucintamente a continuación[27]:

1. En primer lugar, se elabora un estudio y análisis de la normativa sectorial a nivel comunitario y nacional que es de aplicación específica a dicho sector. Su objetivo estriba en poder conocer toda la base normativa que regula el funcionamiento sectorial para determinar aquella que puede ser de mayor interés desde el ámbito PIC para que el desarrollo y el resultado de los trabajos del Plan no vayan en contraposición de los criterios, reglas y normas que regulan dicho sector.
2. En segundo lugar, se dirige un estudio del funcionamiento y de la organización del sector, identificando cuáles son los servicios esenciales que se prestan en el mismo y que deben ser objeto de protección. Del funcionamiento y estructura de los servicios esenciales se obtendrá una segmentación del sector compuesta por los diferentes ámbitos de actividad que se desarrollan y la tipología de infraestructuras o segmentos sobre los se sustentan los ámbitos de actividad. A modo de ejemplo, el Sector de la Energía, se subdivide en varios subsectores como son la electricidad, el gas y el petróleo. Dentro del subsector de la electricidad existirían los ámbitos de la generación, transporte, distribución y operación-control. Siguiendo con la segmentación del subsector de la electricidad, el ámbito del transporte de electricidad estaría compuesta por los segmentos o tipología de las infraestructuras siguientes: líneas de transporte (400 y 200 kV) y subestaciones de transporte. Una vez determinado y realizado el estudio del funcionamiento de los servicios esenciales prestados a nivel sectorial, se está en condiciones de identificar cuáles son aquellas infraestructuras estratégicas sobre las que se asientan los diferentes servicios esenciales. A su vez, se localizan los operadores más relevantes, en función de la titularidad y de la gestión de las tipologías de infraestructuras ya identificadas como fundamentales para el correcto funcionamiento de los servicios esenciales. Del estudio del funcionamiento y organización del sector, se establecen además las diferentes interdependencias intrasectoriales (con otros ámbitos del mismo sector) e intersectoriales (con otros sectores estratégicos). El objetivo es diseñar un mapa de interdependencias que ayude a identificar a nivel sectorial, por cada una de las tipologías de infraestructuras definidas, sus dependencias de entrada (de quién depende la infraestructura) y de salida (quién depende de la infraestructura).
3. El tercer capítulo aborda la realización de un análisis de riesgos general y estratégico en el que se contemplan las vulnerabilidades y ame-

[27] La estructura, organización y contenido de un Plan Estratégico Sectorial tipo aparece desarrollada en mayor detalle en el artículo de Fernando Sánchez, «Protección de infraestructuras críticas: El Sistema de planeamiento como herramienta de implantación (I)», publicado en la *Revista Seguridad y Ciudadanía* n.º 12, de diciembre de 2014 (pp. 31 y ss.).

nazas potenciales, tanto de carácter físico como lógico, que puedan afectar al sector o subsector en cuestión, estimando el impacto que tendría en la sociedad. Para ello se cuenta con unas tablas de estimación (basadas en los criterios horizontales de criticidad derivados de la Directiva 2008/114, sobre protección de infraestructuras críticas europeas) donde se parametrizan los daños/impacto sobre las personas, económico y medioambiental y, finalmente, la incidencia sobre el servicio prestado. Estas tablas, eminentemente técnicas y de una extrema complejidad, son elaboradas *ad hoc* para cada uno de los Planes Estratégicos Sectoriales por equipos de trabajo especializados.

4. Finalmente, el capítulo cuarto, de carácter más organizativo, aborda las propuestas necesarias para la implantación de medidas de diferente tipo, a saber:

   - Organizativas y técnicas, necesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los diferentes escenarios que se prevean.
   - Preventivas y de mantenimiento.
   - De coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

Cada uno de los Planes Estratégicos Sectoriales deberá ser aprobado por la Comisión Nacional de Protección de las Infraestructuras Críticas, presidida por el secretario de Estado de Seguridad y compuesta por representantes de diez ministerios y organismos. Los planes, de carácter clasificado, son gestionados y custodiados en un registro central por el CNPIC, sin perjuicio de que cada ministerio y organismo del Sistema dispongan de una copia de estos, siempre y cuando cuenten con las medidas de seguridad previstas por la Ley para la custodia, archivo y manejo de material clasificado. A su vez, el CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes.

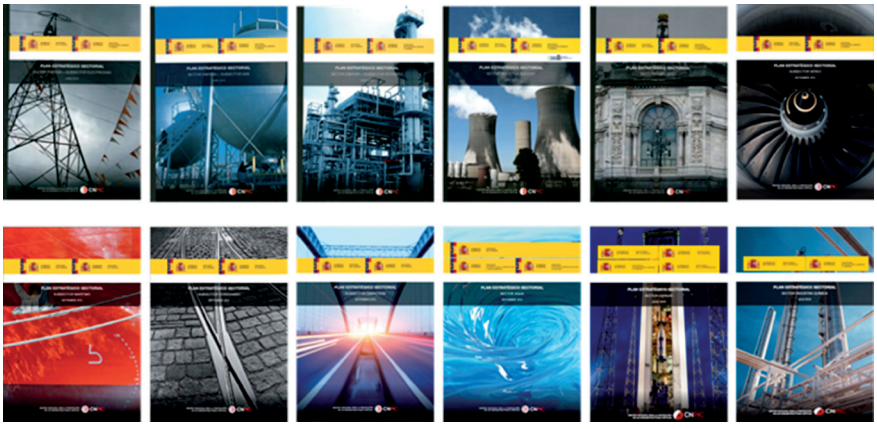

Figura 5.4. Planes Estratégicos Sectoriales aprobados en 2016.

Durante el año 2014 se acometió el desarrollo y posterior aprobación por parte de la Comisión Nacional de Protección de las Infraestructuras Críticas de los planes referentes al Sector Energía (electricidad, gas y petróleo), Industria nuclear y Sistema Financiero. Posteriormente, se hizo lo propio en 2015 con el Sector Agua y el Sector Transporte (marítimo, aéreo, carreteras y ferroviario). En 2016 se aprobaron los correspondientes a los sectores Espacio e Industria Química y se está actualmente redactando el relativo al sector de las Tecnologías de la Información y Comunicaciones (TIC).

Los Planes de Seguridad del Operador (PSO)[28]

El Plan de Seguridad del Operador es aquel documento de carácter estratégico en el que el operador crítico, una vez designado oficialmente a través de Resolución del secretario de Estado de Seguridad, ha de recoger cuáles son las políticas generales de seguridad de su organización para garantizar la protección y la seguridad del conjunto de activos de los que es titular o gestor.

Como se ha podido ver en el epígrafe anterior, referido a los Planes Estratégicos Sectoriales, una vez se ha procedido al nombramiento de operador crítico tras su identificación, se inicia un proceso marcado en el artículo 13 de la Ley PIC. Entre las obligaciones a las que se enfrenta, se destaca como primera de ellas la de elaborar un PSO en el plazo de seis meses a partir de la notificación de la resolución de su designación. Este Plan (solo uno por operador crítico designado) se presentará al CNPIC para su evaluación y, si procede, su aprobación por el secretario de Estado de Seguridad u órgano en el que este delegue. El Plan de Seguridad del Operador tiene la finalidad, así, de integrar todos aquellos criterios de seguridad integral que los operadores críticos aplican al conjunto de las infraestructuras de las que son propietarios o gestores.

El Plan de Seguridad del Operador, como instrumento de planificación del Sistema de Protección de Infraestructuras Críticas, contendrá al menos los siguientes aspectos:

1. La política general de seguridad del operador y su marco de gobierno.
2. La relación de servicios esenciales prestados por el operador.
3. La metodología de análisis de riesgo (amenazas físicas y lógicas) que aplica.
4. Los criterios de aplicación de las medidas de seguridad integral.

[28] La estructura y contenido de un Plan de Seguridad del Operador tipo aparece desarrollada en mayor detalle en el artículo de Fernando Sánchez, «Protección de infraestructuras críticas: El Sistema de planeamiento como herramienta de implantación (II)», publicado en la *Revista Seguridad y Ciudadanía* n.º 13, de junio de 2015 (pp. 22 y ss.).

Para marcar el camino a seguir y asesorar al operador en su redacción, el CNPIC elabora una guía en la que se recogen los contenidos mínimos sobre los que se debe de apoyar el operador a la hora del diseño y elaboración de su Plan. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la normativa de referencia. En dicha guía, igualmente, se pretende orientar a aquellos operadores que hayan sido o vayan a ser designados como críticos en el diseño y elaboración de su respectivo Plan, con el fin de que estos puedan definir el contenido de su política general y el marco organizativo de seguridad, que encontrará su desarrollo específico en los Planes de Protección Específico (objeto del próximo epígrafe) de cada una de sus infraestructuras críticas. La Guía de Contenidos Mínimos es públicamente accesible y fue aprobada mediante Resolución de 8 de septiembre de 2015 de la Secretaría de Estado de Seguridad (BOE n.º 224, de 18 de septiembre)[29].

Dado que el desarrollo de estos planes está condicionado por la aprobación de los respectivos PES que aplican a cada operador crítico, hasta el momento se han podido completar aquellos relativos al Sector Energía, Industria Nuclear, Sistema Financiero, Agua y Transporte, Espacio e Industria Química, estando en fase de iniciación los correspondientes a los sectores TIC, Alimentación y Salud.

Los Planes de Protección Específicos (PPE)[30]

Del sistema de planificación hasta ahora esbozado se deriva una responsabilidad compartida entre el operador crítico (propietario y/o gestor de las infraestructuras críticas que presta servicios esenciales) y el Gobierno de España, representado por la Secretaría de Estado de Seguridad del Ministerio del Interior, como garante de que los servicios esenciales sean proporcionados en condiciones de seguridad, integridad y calidad, en beneficio de la población civil, las instituciones públicas y el sistema empresarial del país.

Para ello, las dos primeras piezas de dicho sistema de planificación ya han sido, en su mayor parte, como se ha visto en estas líneas, diseñadas por el Estado (Plan Nacional de Protección de las Infraestructuras Críticas y Planes Estratégicos Sectoriales), mientras que la redacción de los Planes de Seguridad del Operador es una responsabilidad de los operadores críticos. Todos estos documentos son de carácter estratégico, elaborados, revisados y, en su caso, aprobados, en el ámbito de la Administración General del Estado por los departamentos u organismos competentes.

[29] http://www.boe.es/boe/dias/2015/09/18/pdfs/BOE-A-2015-10060.pdf

[30] La estructura y contenido de un Plan de Protección Específico tipo aparece desarrollada en mayor detalle en el artículo de Fernando Sánchez, «Protección de infraestructuras críticas: El Sistema de planeamiento como herramienta de implantación (II)», publicado en la *Revista Seguridad y Ciudadanía* n.º 13, de junio de 2015 (pp. 50 y ss.).

Tras estos planes de carácter superior, la implantación del Sistema PIC tiene su continuación en el marco territorial y operativo a través de los Planes de Protección Específicos y de los Planes de Apoyo Operativo, sobre los cuales las Adminstraciones Públicas tienen responsabilidad en la aprobación y revisión de los primeros y en la elaboración, aprobación y revisión de los segundos.

El Plan de Protección Específico es aquel documento operativo donde el operador crítico debe definir las medidas concretas ya adoptadas y las que se vayan a adoptar para garantizar la seguridad integral (física y lógica) de aquellas infraestructuras que sean catalogadas como críticas. Es decir, el operador ha de elaborar un Plan por cada uno de los activos identificados como críticos.

El Plan de Protección Específico de cada infraestructura deberá contemplar la adopción tanto de medidas permanentes de protección como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta sobre una o varias infraestructuras por este gestionadas. Al igual que en el caso de los Planes de Seguridad del Operador, los operadores cuentan con una guía de Contenidos Mínimos (igualmente aprobada por Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad) para el desarrollo de los Planes de Protección Específicos[31].

Cabe destacar en este caso que, dado el elevado número de planes existentes, en el desarrollo del sistema de planificación e implantación territorial de los mismos se requiere la intervención de las distintas Delegaciones de Gobierno y Fuerzas y Cuerpos de Seguridad del territorio donde se encuentran enclavadas las diferentes infraestructuras críticas identificadas.

Por todo ello, y con el fin de culminar el establecimiento del sistema de planificación establecido en la Ley 8/2011 a nivel territorial, en atención a las especiales obligaciones que exige la citada Ley a las Adminstraciones públicas competentes, y teniendo en cuenta los numerosos agentes que participan en su implantación (Delegaciones del Gobierno, Comunidades Autónomas y Fuerzas y Cuerpos de Seguridad) se dictó por parte del Secretario de Estado de Seguridad una Instrucción, de fecha 10 de septiembre de 2015, dirigida a todos los agentes responsables, donde se termina de definir el marco de actuación de estos. Dicha instrucción tiene como objeto contribuir a agilizar la implantación del citado sistema de una manera eficaz, ágil, homogénea y armonizada en las diferentes Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía, desde el punto de vista de la seguridad y protección de las infraestructuras.

[31] Ibíd. 29.

Los Planes de Apoyo Operativo (PAO)

La Ley PIC prevé que, sobre cada infraestructura crítica, las Fuerzas y Cuerpos de Seguridad competentes, para llevar a cabo su protección, desarrollarán un Plan de Apoyo Operativo en el que se diseñará un plan de reacción e intervención en apoyo de los mecanismos de seguridad implementados por cada organización en sus respectivos Planes de Protección Específicos. Esto supone, por tanto, un trato «preferencial» sobre las instalaciones críticas en caso de incremento del nivel de alerta previsto por el PNPIC.

El Cuerpo policial competente deberá redactar, tras serle notificada la aprobación del Plan de Protección Específico por la Secretaría de Estado de Seguridad, un Plan de Apoyo Operativo para dicha infraestructura, donde se establecerán las medidas planificadas de vigilancia, prevención, protección y reacción que deberá adoptar dicho Cuerpo policial y, en su caso, su coordinación con otras Fuerzas y Cuerpos de Seguridad.

El Plan de Apoyo Operativo deberá contemplar las medidas preventivas y reactivas a desarrollar en función del nivel de riesgo establecido en el Plan de Prevención y Protección Antiterrorista y/o el Plan Nacional de Protección de las Infraestructuras Críticas o de confirmarse la existencia de una amenaza inminente.

Las medidas propuestas en el Plan de Apoyo Operativo serán complementarias a aquellas de carácter gradual previstas por el operador crítico en su Plan de Protección Específico, el cual deberá servir como base para la redacción del primero. Para ello, el Cuerpo policial competente deberá tener acceso al contenido del citado Plan de Protección Específico y podrá requerir la colaboración del Delegado de Seguridad de dicha infraestructura crítica. Por su parte, el operador deberá poder tener acceso, de forma limitada, al contenido de dichos planes para armonizarlos con los Planes de Protección Específicos de sus propias instalaciones. De la misma manera, las unidades operativas de las Fuerzas y Cuerpos de Seguridad competentes deberán coordinarse con los servicios de seguridad de los operadores para la protección de las instalaciones afectadas.

El Plan de Apoyo Operativo, cuya elaboración será supervisada por la Delegación del Gobierno o, en su caso, por el órgano de la Comunidad Autónoma con competencia en materia de seguridad, se ajustará a los contenidos mínimos establecidos por la Secretaría de Estado de Seguridad que se adjuntan como anexo a la Instrucción de 10 de septiembre de 2015, ya mencionada en el anterior epígrafe.

Finalmente, una vez elaborado un Plan de Apoyo Operativo, el Cuerpo policial competente lo remite a la Delegación del Gobierno que, a su vez, lo cursa al CNPIC para su aprobación y validación por la Secretaría de Estado de Seguridad.

De esta manera, el ciclo planificador, iniciado con el PNPIC, se ve cerrado con la aprobación de los diferentes Planes de Apoyo Operativo con la intervención y delimitación de responsabilidades de todos los agentes responsables en materia de protección de infraestructuras críticas. Obviamente este es un proceso largo, que será culminado a principios de 2017 en lo respectivo a los sectores de la Energía y Sistema Financiero y Nuclear. Una vez esté rematado se puede decir que el Sistema PIC que emane de dicho proceso tendrá la robustez y agilidad necesarias para abordar la problemática de la protección de nuestras infraestructuras y servicios esenciales con garantías de éxito, con los controles necesarios y con la cooperación público-privada como eje conductor de las actividades e iniciativas que se desarrollen.

Herramientas para la colaboración

Como ya se ha visto, el Sistema de Protección de Infraestructuras Críticas integra una serie de planes de seguridad en los que la ciberseguridad tiene un papel fundamental, como complemento a aquellas medidas de seguridad de carácter más tradicional que se contemplaban hasta el momento de crear este sistema holístico. Sin embargo, la ciberseguridad requiere en algunas ocasiones el establecimiento de otra serie de medidas particulares que garanticen la comunicación, cooperación y colaboración entre los distintos agentes con capacidad de actuación. En el ámbito de la protección de las infraestructuras críticas, se considera fundamental no solo el asegurar una adecuada protección cibernética de las infraestructuras[32], sino además el garantizar que se implementan herramientas relativas a la participación e integración de todos los agentes responsables de una u otra manera en la ciberseguridad. A continuación se detallan las medidas implantadas al efecto hasta el momento por el CNPIC.

Apoyo frente a incidentes

Las tecnologías empleadas por las infraestructuras críticas no difieren de aquellas empleadas en otro tipo de entornos, por lo que las amenazas a las que se ven expuestas son las mismas, si bien el impacto de su materialización sí que puede amplificarse en entornos críticos. Por lo tanto, los operadores críticos deben protegerse frente a ataques que puedan afectar a

[32] La Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 30 de marzo de 2009, sobre protección de infraestructuras críticas, «Protegiendo a Europa de ciberataques a gran escala e interrupciones: mejora de la preparación, la seguridad y la respuesta» [COM (2009) 149 final], hace por primera vez, a nivel europeo, un llamamiento a la convergencia de la seguridad física y la seguridad lógica, ante la evidencia de la utilización de la red por criminales y terroristas como medio de llevar a cabo sus acciones contra las infraestructuras críticas.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

la confidencialidad, integridad o disponibilidad de sus activos tecnológicos, siendo conscientes de que la interconectividad, que predomina en este tipo de entornos, puede facilitar la propagación de un incidente hacia todo el entorno tecnológico de la organización.

De forma adicional, cabe destacar el hecho de que cuando se tiene conocimiento de un incidente, es muy difícil asignar *a priori* una tipología concreta. De hecho, incidentes en los que todo apunta a que van dirigidos exclusivamente hacia el robo de información pueden formar parte de un ataque más complejo que tenga por objeto inhabilitar el servicio o afectar al correcto funcionamiento de la infraestructura. Los intereses de los atacantes pueden diferir por tanto en cada ataque y, siendo compleja su identificación, suelen estar referidos a la obtención de un beneficio económico, a la publicidad de sus acciones o propaganda de determinadas ideologías o, en casos extremos, a causar terror en la población.

Como se ha reseñado repetidamente a lo largo de este artículo el CNPIC plantea, además de ser uno de sus precursores en España, el concepto de seguridad integral[33], trabajando de forma dinámica y continua para garantizar la seguridad a los sistemas de información y telecomunicaciones que soportan las infraestructuras. En este campo se han fortalecido las capacidades de prevención, detección, respuesta y recuperación para hacer frente a las ciberamenazas, desarrollando:

– Un Equipo de Respuesta a Incidentes Cibernéticos (*CERT* de Seguridad e Industria–CERTSI_), con sede en León, operado por el Instituto Nacional de Ciberseguridad (INCIBE), en conjunción con el CNPIC y que se ha erigido en el punto de referencia nacional para la resolución técnica de incidentes de ciberseguridad que puedan afectar a la prestación de los servicios esenciales[34].

[33] Exigible a los operadores críticos, entre otras, por la *Guía de Contenidos Mínimos* aprobada mediante Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad (BOE n.º 224, de 18 de septiembre).
http://www.boe.es/boe/dias/2015/09/18/pdfs/BOE-A-2015-10060.pdf

[34] El CERT de Seguridad e Industria (CERTSI_) es, entre otras acciones, consecuencia del *Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo,* de fecha 4 de octubre de 2012 (actualizado con fecha 21 de octubre de 2015).
El mencionado acuerdo fijó las bases de la colaboración entre la SES y la SETSI para impulsar en España los aspectos de seguridad en el ámbito de la Sociedad de la Información en general, la protección de las infraestructuras críticas y la lucha contra los delitos informáticos (también conocidos como «ciberdelitos») y el ciberterrorismo, dando respuesta a los objetivos planteados por la Estrategia Española de Seguridad de 2011 y la Agenda Digital para España. Dicha colaboración fue planteada sobre la base de un mecanismo de coordinación entre el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y el entonces INTECO (hoy INCIBE) en la resolución de incidentes y mitigación de sus efectos, así como en el intercambio de información de interés.

– Una Oficina de Coordinación Cibernética (OCC) en el seno del CNPIC, como punto de contacto nacional de coordinación operativa 7 × 24 para el intercambio de información.

En lo que respecta a la gestión de incidentes de ciberseguridad, es importante resaltar que por parte del CNPIC y el CERTSI_ se ha desarrollado la *Guía de reporte de ciberincidentes para operadores críticos*, con objeto de establecer una clara delimitación de la tipología de ciberincidentes que deben de ser reportados, así como la forma y momento de hacerlo en cada caso.

De este modo, esta guía tiene por objeto dar cumplimiento a lo dispuesto en el PNPIC, desarrollando en detalle cuál es el tipo de acciones que debe de llevar a cabo el operador crítico según el Nivel de Alerta sobre infraestructuras críticas que se encuentre activo en un momento determinado (a la hora en que se escribe este artículo nos encontramos en nivel 4, coordinado con el Nivel de Alerta Antiterrorista). Cabe destacar que el aumento gradual de medidas asociadas en materia de ciberseguridad conlleva una serie de obligaciones no solo para los operadores críticos, sino también, muy especialmente, para el CNPIC y el CERTSI_ como responsables de la administración de la ciberseguridad de las infraestructuras críticas nacionales, con la adquisición de un compromiso para la intervención y resolución de las incidencias en un marco temporal variable, según escale el nivel de la amenaza.

El equipo de respuesta a incidentes cibernéticos de seguridad e industria (CERTSI_)

El *CERT* de Seguridad e Industria (CERTSI_) es el *CERT* Nacional competente, por Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015, en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas[35].

Creado en octubre de 2012 a través de un Acuerdo Marco de Colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, recientemente actualizado el pasado 21 de octubre de 2015, el CERTSI_ se configura como la entidad tecnológica encargada de la gestión de incidentes de naturaleza cibernética que afecten a los operadores de los servicios esenciales en España.

Este equipo de respuesta es el resultado de la suma de capacidades y competencias del Instituto Nacional de Ciberseguridad (INCIBE) y del Centro

[35] El Consejo Nacional de Ciberseguridad (Comité especializado) es un órgano colegiado de apoyo al Consejo Nacional de Seguridad con la finalidad de informar y asesorar a aquel en el ámbito de la ciberseguridad, de acuerdo con lo previsto por la Estrategia de Seguridad Nacional de junio de 2013.

Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y, por consiguiente, añade a las responsabilidades ya existentes sobre empresas y ciudadanos, previas a la firma del Acuerdo SES-SETSI, aquellas que se derivan de la necesidad de mejorar la protección de las infraestructuras críticas y la provisión de los servicios esenciales[36].

En este sentido, cabe destacar que habitualmente los *CERT* no se encargan únicamente de la gestión de incidentes, sino que ofrecen de forma habitual otro tipo de servicios de utilidad para su público objetivo. En el caso particular del CERTSI_, el inicio de las actividades en el ámbito PIC se diseñó sobre la base de la identificación y definición de un catálogo de servicios en el ámbito de la prevención, detección y respuesta ante incidentes, que se ha ido mejorando y complementando aprovechando la experiencia y madurez del propio centro a lo largo de estos últimos tiempos[37].

En la actualidad, dicho catálogo contempla servicios adicionales de valor añadido, como son la realización de ciberejercicios con periodicidad anual o la compartición de información acerca de vulnerabilidades «día cero» (vulnerabilidades que aún no han sido publicadas por el fabricante). De este modo, se pretende dotar a los operadores críticos de información y capacidades privilegiadas con objeto de complementar la, sin duda necesaria, gestión autónoma de la ciberseguridad.

La Oficina de Coordinación Cibernética del Ministerio del Interior

En el año 2014, mediante la Instrucción 15/2014, de la Secretaría de Estado de Seguridad, se creó dentro del CNPIC la Oficina de Coordinación Cibernética (OCC) que se configuró desde ese instante como el órgano técnico de coordinación de la Secretaría de Estado de Seguridad en materia de ciberseguridad. Su objetivo es conseguir una mayor eficiencia en la gestión de aquellos aspectos de la Estrategia de Ciberseguridad Nacional que se encuentran

[36] Algunas de las actuaciones acordadas en el ámbito de la protección de las infraestructuras críticas son:
1. La respuesta a Incidentes de Seguridad TIC en las infraestructuras críticas y los operadores de servicios esenciales.
2. La puesta en marcha de auditorías de seguridad y esquemas de acreditación sobre sistemas de información que dan soporte a las infraestructuras críticas.
Dichas medidas, recogidas en los Contenidos Mínimos publicados por Resolución del Secretario de Estado de Seguridad en relación a los Planes de Seguridad del Operador y a los Planes de Protección Específicos, serán actualizadas de forma periódica por el CNPIC, y contarán con la colaboración del INCIBE en la variable de ciberseguridad.
3. La realización de simulacros y ciberejercicios sobre infraestructuras críticas.

[37] De acuerdo con lo determinado en el Acuerdo SES-SETSI, el equipo técnico del CERTSI_ atenderá los incidentes de acuerdo con las prioridades definidas en los umbrales y procedimientos fijados por ambas entidades. Asimismo, el servicio se desempeñará en horario continuado (24 × 7 × 365) con un acuerdo de nivel de servicio (SLA) que permita dar una respuesta ágil a los incidentes de los que se tenga constancia.

bajo la competencia del Ministerio del Interior, siendo además el punto natural de interlocución del Ministerio con el CERTSI_ en materia tecnológica[38].

En este sentido, las actuaciones que lleva a cabo la OCC se refieren normalmente al intercambio de información en materia de ciberdelincuencia y ciberterrorismo; a la coordinación de acciones de respuesta ante incidentes, integrando las capacidades de las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado cuando sea necesario; a la emisión de información de alerta temprana sobre ciberamenazas; a la supervisión en materia de ciberseguridad de los planes de seguridad que conforman el PNPIC y a la participación en proyectos de I+D.

Por otra parte, el PNPIC contempla en determinadas situaciones el establecimiento de Dispositivos Extraordinarios de Ciberseguridad. Para su diseño e implementación, la OCC se ha erigido como el órgano responsable de efectuar la coordinación técnica entre los responsables de seguridad de los sistemas y tecnologías de la información de los operadores críticos, las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado y el CERTSI_.

Recientemente, en virtud de otra instrucción de la Secretaría de Estado de Seguridad (2/2016 de 10 de febrero) la OCC se constituyó también en punto de contacto del Estado Español en el marco de lo prescrito por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información[39].

---

[38] En noviembre de 2014, mediante Instrucción 15/2014 del Secretario de Estado de Seguridad, se crea la Oficina de Coordinación Cibernética (OCC). De manera específica, la OCC es identificada como la unidad responsable de la coordinación técnica entre la SES y sus organismos dependientes y el CERTSI_. Para ello, se le ha dotado de los mecanismos de intercambio de información seguros necesarios para comunicarse tanto con dicho CERT como con las distintas unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado, agilizando la difusión de información que pueda ser de interés para cualquiera de las partes.

[39] La Directiva 2013/40/UE determina en su artículo 13 que los Estados miembros deberán garantizar la existencia de un punto de contacto nacional operativo a efectos del intercambio de información sobre ciberataques. Asimismo, establece la necesidad de que estos cuenten con procedimientos para que, en caso de solicitud de ayuda urgente, la autoridad competente pueda indicar, en un plazo máximo de ocho horas a partir de la recepción de la solicitud de ayuda, si la misma podrá ser atendida y la forma y el plazo aproximado de ello. La instrucción 2/2016 tiene por objeto la designación de la Oficina de Coordinación Cibernética como punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros. De esa manera, la OCC se constituyó, desde febrero de 2016, en el punto de contacto nacional operativo en el marco de lo establecido en el artículo 13 de la Directiva 2013/40/UE. Esta Oficina dispondrá de las necesarias capacidades de operación veinticuatro horas al día, siete días a la semana, con el fin de responder a las solicitudes de ayuda en el plazo máximo marcado por la citada Directiva. Para ello contará, también, con un enlace permanente con las unidades responsables de las Fuerzas y Cuerpos de Seguridad del Estado y con aquellos otros órganos de esta Secretaría de Estado con competencias en la materia.

Figura 5.5. Logo de la Oficina de Coordinación Cibernética del Ministerio del Interior.

Alerta temprana e intercambio de información

En los últimos años se ha podido observar que, en materia de ciberseguridad, se está asistiendo a un cambio de paradigma en lo referente al intercambio de información sobre ciberincidentes y a las acciones de alerta temprana derivadas del conocimiento de las amenazas que presenta el entorno en el que desarrollan su actividad los operadores de servicios esenciales. Este cambio de paradigma se basa en el paso de los viejos usos y costumbres de un mundo poco conectado, en el que el acceso a la información disponible era restringido y normalmente referido a sistemas propietarios, a un escenario en el que la hiperconectividad y el acceso instantáneo a todo tipo de información es omnipresente; escenario en el que, por supuesto, se ven inmersos los sectores estratégicos nacionales.

En este nuevo escenario, un potencial ciberdelincuente o ciberterrorista cuenta con una multiplicidad de recursos de los que antes no disponía: información sobre sistemas de control industrial, información sobre los protocolos que usan esos sistemas, sobre sus vulnerabilidades, sobre quiénes los administran, sobre su pertenencia, así como cuantiosas herramientas para poder vulnerar la seguridad de dichos sistemas de control industrial...

Ahora bien, en este nuevo escenario hiperconectado que puede ser aprovechado por quienes buscan obtener algún beneficio a través de la disrupción de la confidencialidad, la disponibilidad o la integridad de los sistemas, también se está empezando a utilizar como recurso indispensable a la hora de

luchar contra las amenazas que presenta la operativa de sistemas de control industrial en un entorno conectado y global. Los dos pilares de este nuevo paradigma son la alerta temprana y el intercambio de información, que funcionan sobre la base de unos principios muy sencillos:

- Cuanto antes se tenga conocimiento de una amenaza y su naturaleza, antes se podrán dedicar recursos para evitar que llegue a materializarse o, si esto ocurre, a mitigar el impacto producido. En el mundo hiperconectado, conocer que tus sistemas pueden ser comprometidos y difundir este conocimiento sobre la base de una red colaborativa de usuarios mutuamente interesados es técnicamente posible.
- La información sobre incidentes reales y cómo han sido mitigados es de gran utilidad a la hora de elaborar contramedidas, mejorar los sistemas y protocolos así como publicar guías de buenas prácticas a fin de evitar que un incidente de similares características vuelva a reproducirse. La tendencia de ocultar la información de resolución de incidentes se está abandonando progresivamente y ahora prima la difusión y obtención de información sobre aquellos incidentes que pueden afectarnos. Esto es una consecuencia lógica del nivel de avance tecnológico de la sociedad industrializada: la cantidad de conocimiento sobre las vulnerabilidades de nuestros sistemas que se genera en un entorno hiperconectado supera a aquel conocimiento que pueda ser generado por equipos individuales en la gestión de sus sistemas y su seguridad, por lo que estratégicamente es más ventajoso el unirse a comunidades de intercambio de información que aislarse de estas redes.

Por todo ello, una de las principales líneas de acción del CNPIC, junto con el INCIBE, es precisamente el impulso, desarrollo e implantación de proyectos que tienen como claro objetivo ofrecer soporte tecnológico a los responsables de la administración de la ciberseguridad en operadores de servicios esenciales y sus infraestructuras y redes, para que puedan establecer estas redes de intercambio de información y alerta temprana. Este soporte se realiza en dos niveles distintos: a nivel individual, con aplicativos adaptados a las características del operador crítico y, a un nivel más amplio, mediante plataformas o proyectos dirigidos al conjunto de operadores de los distintos sectores estratégicos.

Como ejemplo del nivel individual de acción, y enmarcado en la Estrategia de Ciberseguridad Nacional[40], se ofrece el servicio Detector de Incidentes, que es una plataforma tecnológica de alerta temprana y vigilancia tecnológica, por la que el CERTSI_ lleva a cabo el despliegue y operación de servicios de inteligencia en ciberseguridad mediante el establecimiento de acuerdos con entidades de referencia internacional en materia de ciberseguridad,a fin

[40] Línea de acción n.º 3: *Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas* (pp. 34 y ss.).
http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional

de obtener información actualizada que se utiliza en las labores de investigación para la detección proactiva de amenazas. Mediante este servicio se puede analizar, en las propias instalaciones del operador, el tráfico de internet entrante y saliente, contrastando la información obtenida con las listas de recursos maliciosos conocidos y de indicadores de compromiso que suministra en tiempo real el servidor de gestión centralizada del INCIBE. Esta funcionalidad permite al operador crítico reducir de forma drástica el tiempo de detección de compromiso de sus activos tecnológicos al contar en sus propias instalaciones con la información actualizada de amenazas en curso.

En el plano de la acción colectiva, el servicio ÍCARO ofrece a los operadores críticos una plataforma en la que intercambiar información acerca de ciberamenazas. ÍCARO es una plataforma que centraliza la información aportada por los operadores de servicios esenciales de los distintos sectores estratégicos, de tal forma que el CERTSI_ puede contrastar y verificar dicha información para posteriormente ofrecérsela a todos los operadores que conforman la comunidad de intercambio de información. Un aspecto muy importante de este sistema es la utilización de estándares internacionales para estructurar dicha información y posteriormente intercambiarla, de tal forma que las labores pueden automatizarse. De esta forma, el operador puede desplegar en sus instalaciones una instancia de ICARO que se sincroniza automáticamente con la plataforma central y puede tanto obtener información como aportar nuevos datos para complementar los que ya se encuentren analizados por el *CERT*. La información sobre una amenaza concreta puede ser muy diversa, llegando a incluir muestras de *malware*, listados de IPs con actividad maliciosa, indicadores de compromiso, reglas de *firewall*, guías de mitigación y buenas prácticas, etcétera.

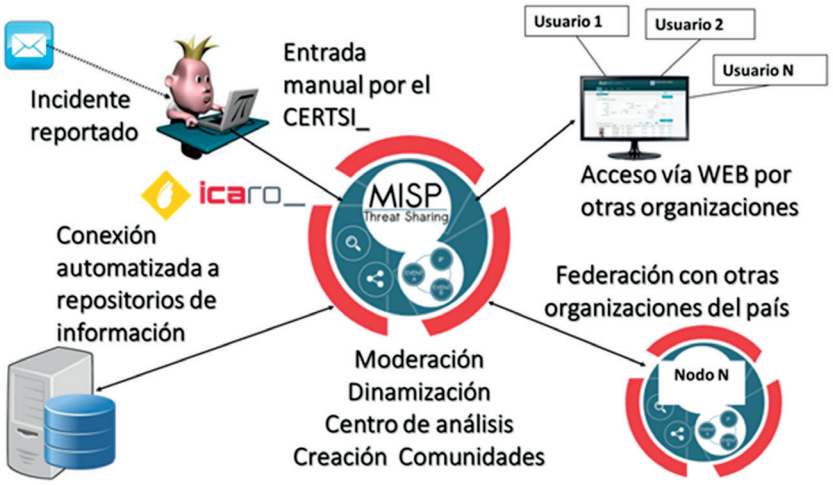

Figura 5.6. Funcionamiento plataforma ÍCARO.

Ciberejercicios

La realización de ciberejercicios es una pieza fundamental en la estrategia del Gobierno en materia de ciberseguridad, por ello, desde el año 2012, el CNPIC, junto con el INCIBE, a través del CERTSI_[41], se ha involucrado en la organización de los ejercicios CyberEX[42]. En las primeras convocatorias de CyberEX (2012 y 2013) el objetivo principal a alcanzar para las entidades participantes era la evaluación de las capacidades técnicas y organizativas, por lo que el ejercicio se basó en la simulación de ataques técnicos a servicios perimetrales. En 2014, el público objetivo fueron operadores de servicios esenciales y también se procedió a la ejecución de simulaciones generalistas, al tener un carácter multisectorial. La última convocatoria, en 2015, enfocado en el negocio, se centró ya en operadores del sector estratégico financiero.

Para la actual convocatoria de 2016[43] se ha apostado de nuevo por una visión multisectorial; siguiendo el plan previsto, se comienza la alternancia entre las ediciones sectoriales y multisectoriales, que permitirán mantener un contacto cercano con los operadores de nuestros servicios esenciales. Además, en la actual edición se pasará de dieciocho participantes a treinta.

En cuanto a las pruebas a realizar durante la fase de ejecución, se llevarán a cabo tres, que buscarán entrenar distintos aspectos de la seguridad de las entidades. Estas son: un ataque/defensa para tratar de entrenar las capacidades de reacción frente a ataques, una prueba para entrenar las capacidades de coordinación y toma de decisiones técnicas y estratégicas en una crisis y, finalmente, una prueba de análisis para entrenar las capacidades de análisis técnico de un incidente.

---

[41] La realización de simulacros y ciberejercicios sobre infraestructuras críticas es uno de los objetivos del Acuerdo SES-SETSI en materia de ciberseguridad. En dicho documento, se coincide en que la realización de simulacros y ejercicios que sean capaces de probar el nivel de protección corporativa con el que cuentan los operadores de infraestructuras críticas, la resistencia de las infraestructuras críticas y de los sistemas de información que las soportan y la capacidad de coordinación real entre los agentes implicados en caso de ciberataques constituye un mecanismo efectivo y de alto valor, no solo para el CNPIC como órgano competente, sino también para los propios operadores críticos.
Basados en la experiencia desarrollada en la realización de los ciberejercicios Ciberex y buscando su continuidad y consolidación, el CNPIC e INCIBE diseñan y coordinan conjuntamente ciberejercicios que permiten la mejora de los procedimientos de actuación, las técnicas, las capacidades, la preparación y la concienciación de los operadores de infraestructuras críticas y de otros prestatarios de servicios esenciales, a partir de su entrenamiento y del mejor conocimiento de los riesgos y amenazas en el ámbito de las tecnologías de la información y las comunicaciones.

[42] https://www.cyberex.es/international/es/inicio
https://www.certsi.es/servicios-operadores/cyberex

[43] https://www.incibe.es/sala-prensa/notas-prensa/comienzan-los-ciberejercicios-nacionales-cyberex-2016-destinados-mejorar

Se prevé que durante la ejecución de las pruebas otras entidades públicas como Fuerzas y Cuerpos de Seguridad del Estado o entidades reguladoras puedan adquirir el rol de observador.

Como novedad en 2016, se procederá a la ejecución de los ciberejercicios a partir de un entorno tecnológico estable (plataforma) que permite la realización de competiciones y entrenamiento de conocimientos sobre ciberseguridad de los participantes, con el diseño de escenarios que se puedan desplegar en la plataforma. Se contará con cuatro tipos de escenarios que pueden ser implementados en esta plataforma: ataque/defensa, descargables, *Capture The Flag* (*CTF*) y didácticos. En el empleo de esta plataforma, con cada ciberejercicio, el CERTSI_ determinará si se llevará a cabo el ciclo de vida completo de desarrollo de un ciberejercicio o únicamente la fase de ejecución. Esto permitirá reutilizar ciberejercicios, amortizando su coste con cada iteración.

Además de CyberEX, el CNPIC ha participado como coorganizador y jugador en otros cuatro tipos de ciberejercicios en los últimos meses, tanto nacionales como internacionales, como las Jornadas PSCIC, en el marco del proyecto *CIISC*-T2 (*Critical Infrastructure: Improvement of Security Control Against the Terrorist Threat*). CIISC-T2 es un proyecto ya finalizado y cofinanciado por la Comisión Europea a través del programa CIPS en el que CNPIC, junto con el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), Isdefe y Kemea (autoridad griega) son cobeneficiarios. Dentro del paquete de trabajo WP3 «Cyberexercise to protect critical infrastructures», la OCC y el CERTSI_ han participado como coordinador y jugador, respectivamente, y la ejecución de este paquete se ha visto materializada en el ciberejercicio de las II Jornadas PSCIC[44]. Es importante destacar que dentro del paquete de trabajo WP4 «Cyberexercise to protect potencial european critical infrastructures» el CNPIC participó como líder en la planificación de un ciberejercicio a nivel europeo en 2015 como continuación del llevado a cabo en el 2014.

Por otro lado, la Administración española, como país miembro de la OTAN, ha participado como planificador y jugador en el ejercicio CMX-16, teniendo el CNPIC un rol relevante en la recreación de los escenarios. *CMX* (*Crisis Management Exercise*) son ejercicios organizados por OTAN con la participación de los países aliados. A nivel nacional, estos ejercicios son liderados por el CESEDEN y para la convocatoria de este año se han recreado dos eventos nacionales, un altercado en un buque en aguas nacionales y un ataque a una infraestructura crítica portuaria. Además, como cada año, el CNPIC ha participado en el ciberejercicio Locked Shields, organizado por el Centro de Excelencia de Ciberdefensa de la OTAN.

Finalmente, en el ámbito europeo, la OCC está participando como jugador en el ejercicio paneuropeo Cyber-Europe 2016, coorganizado, a nivel nacional, por

[44] https://www.jornadaspscic.isdefe.es/?lang=es

el Departamento de Seguridad Nacional (DSN) de Presidencia del Gobierno. En este mismo ámbito europeo, se organizó en Madrid en febrero de 2016, conjuntamente por la Unidad de Acción contra el Terrorismo (UAT) de OSCE (Organización para la Seguridad y Cooperación en Europa) y el CNPIC, un taller internacional consistente en un ejercicio de simulación (*table-top exercise*) sobre protección de infraestructuras críticas energéticas contra ataques informáticos, siguiendo el modelo de colaboración público-privada, con presencia de hasta quince grandes entidades del sector energético nacional.

Acuerdos de colaboración

La eficaz y eficiente colaboración entre el sector público y el sector privado en el ámbito de la protección de las infraestructuras críticas debe sustentarse sobre los siguientes pilares:

- Intercambio de información. El CNPIC asegura, mediante las plataformas de comunicación incluidas en el sistema informático de gestión del Catálogo Nacional de Infraestructuras, la comunicación y el intercambio de información tanto con las Fuerzas y Cuerpos de Seguridad y con los organismos competentes para la seguridad de los distintos sectores estratégicos como con los operadores críticos. En materia de ciberseguridad, a través del CERTSI_ circula cualquier tipo de información relevante que pueda mejorar el conocimiento del entorno, ya sea a nivel sectorial, organizativo o individual.
- Responsabilidad compartida. No se puede cargar al Estado con la responsabilidad exclusiva del aseguramiento del correcto funcionamiento de los servicios esenciales, al estar cerca del 80 % de las infraestructuras críticas que los suministran en manos del sector privado. En este sentido, los servicios ofrecidos por el CNPIC de forma general y por la OCC y el CERTSI_ de forma particular, en materia de ciberseguridad, tienen como uno de sus objetivos mejorar la concienciación de los operadores, con el fin de que sean capaces de responder autónomamente ante incidentes cibernéticos. Con todo, el CERTSI_ y la OCC siempre estarán como soporte de aquellos operadores críticos que requieran una ayuda excepcional.
- Confianza mutua. Las colaboraciones público-privadas se basan fundamentalmente en el establecimiento de relaciones sólidas entre los participantes. Se da por hecho que, si bien la participación en colaboraciones público-privadas es voluntaria, una vez se forma parte de una de ellas se asume que las conclusiones son vinculantes. La confianza mutua es la única manera de salvar la barrera del natural recelo a informar sobre incidentes, sobre todo cuando esta información pueda ser aprovechada por la competencia.

Sin embargo, no basta con la definición de esos tres pilares para garantizar una adecuada cooperación público-privada. Más si cabe cuando el intercam-

bio de información se lleva a cabo mediante medios tecnológicos para los que es necesario asegurar la confidencialidad de la información transmitida. Por este motivo fundamentalmente, los servicios del CERTSI_ se ofrecen siempre bajo la suscripción de un acuerdo de confidencialidad en materia de ciberseguridad que obliga a las partes suscriptoras (actualmente alrededor de cien, lo que supone una «bolsa» de un centenar de beneficiarios de lo que puede ser considerado como uno de los mayores foros de intercambio de información de nuestro país). De forma adicional, los operadores críticos firman igualmente otro acuerdo de confidencialidad con el CNPIC para garantizar que la información disponible en el Catálogo de Infraestructuras se maneja de forma apropiada y con las garantías necesarias. No obstante, los operadores que firman acuerdos deben garantizar igualmente que manejan adecuadamente la información aportada desde el CNPIC, el CERTSI_ o la OCC, de modo que se ratifique la confianza mutua mencionada anteriormente.

Controles recomendados

Además de las herramientas tratadas durante este capítulo, que ya se están utilizando para potenciar la colaboración público-privada, existen otras que nos permitirán seguir fomentando la colaboración y con ella la ciberseguridad. Un claro ejemplo es la adopción de controles o medidas de seguridad internacionalmente reconocidos para la protección de los sistemas de un determinado sector. De esta forma se garantiza la estandarización de los mismos y la personalización para el sector, siguiendo criterios de eficacia y facilidad para su implantación.

Al tener controles comunes, es posible comparar el nivel de seguridad de las empresas del sector y por lo tanto detectar si existe un problema de seguridad en alguna de ellas. Igualmente, frente a una nueva amenaza sería sencillo conocer la vulnerabilidad del sector y tomar las medidas necesarias para minimizar el riesgo lo antes posible.

Estos controles deberían fijarse conjuntamente entre la autoridad pública y las empresas del sector afectado, aportando la primera las amenazas existentes en el sector y las segundas el conocimiento de sus sistemas y su criticidad. Partiendo de esta información se determinarán los controles que son más eficaces, así como el nivel de implantación necesario. Debido a que las amenazas varían, también deben hacerlo los controles; esto nos obliga a mantener una gestión de los controles activos y una comunicación con las empresas afectadas por los mismos.

En el caso del sector de la energía y concretando en las infraestructuras esenciales de este sector, se podrían utilizar algunos de los siguientes estándares para definir los controles más apropiados:

– ISO 27019, guía para la gestión de la Seguridad de la información en sistemas de control del sector de la energía.

– Instituto SANS, instituto especializado en la formación e investigación en ciberseguridad.
– NIST que depende del Departamento de Comercio de Estados Unidos.

Estos estándares tienen un reconocimiento internacional importante, necesario para poder alcanzar un consenso sobre su necesidad y eficacia, así como para encontrar personal formado en los mismos, o bien para facilitar la formación del personal necesario. A continuación hacemos una pequeña descripción de los mismos.

ISO 27019

La Organización Internacional de Normalización (ISO) tiene como objetivo la creación de estándares internacionales y está formada por diversas organizaciones nacionales de estandarización. La serie de normas ISO 27000 son estándares de seguridad publicados por ISO que contiene las mejores prácticas en seguridad de la información para desarrollar, implementar y mantener controles para los sistemas de gestión de la seguridad de la información (SGSI o *ISMS*, acrónimo en inglés de *Information Security Management System*). Dentro de esta familia de estándares se encuentra la ISO 27019, enfocada a extender la seguridad a los procesos de sistemas de control (sistemas usados en procesos de producción industriales para controlar equipos o máquinas) del sector de la energía, permitiéndole implementar un sistema de gestión de la seguridad de la información.

La ISO 27019 es un documento técnico que, basado en la ISO 27002 (centrada en la implantación de los controles para la gestión de la seguridad de la información) se centra en su aplicación a los sistemas de control usados en el sector de la energía. El objetivo del documento es extender los estándares ISO 27000 a los procesos de sistemas de control y automatización de forma que permita al sector de la energía implementar un sistema de gestión de la seguridad de la información acorde con la ISO 27001.

SANS Institute

El Instituto *SANS* (*SysAdmin Audit*, *Networking and Security*) es una organización educativa que desde 1989 trabaja en la formación y certificación de especialistas en seguridad de la información, así como en documentos de investigación relacionados con esta especialidad. El Instituto genera y mantiene una gran colección de documentos de investigación sobre diversos aspectos de la seguridad de la información. De las publicaciones realizadas por el *SANS* Institute, podemos destacar la publicación periódica de los veinte controles críticos de seguridad para una ciberdefensa efectiva. Estos controles resumen de una forma práctica las medidas de seguridad más efectivas para implementar la seguridad en una empresa.

NIST

NIST son las siglas del *National Institute of Standards and Technology*, que depende del Departamento de Comercio de Estados Unidos y es responsa-

ble de desarrollar estándares de ciberseguridad, guías, test y métricas. Entre sus objetivos se encuentra el aumento de la fiabilidad y la capacidad de recuperación de las infraestructuras de sistemas. Esta tarea requiere una inversión sustancial en el diseño y el desarrollo de los sistemas y redes informáticas. Los documentos son desarrollados de forma conjunta por expertos de todo el mundo y revisados en un proceso público por expertos de la industria afectada por el documento, profesores especializados y personal del propio *NIST*. El *NIST* trabaja para conseguir un conjunto estructurado de procesos de sistemas de seguridad que, basándose en las normas internacionales ya establecidas, ofrece un importante punto de partida para realizar la documentación. Dentro de los documentos publicados destaca la Publicación 800-160, Ingeniería de Seguridad de Sistemas (*Systems Security Engineering*) que, publicado en mayo de 2014, ofrece un enfoque integrado para la construcción de sistemas resistentes, ayudando a las organizaciones a desarrollar una infraestructura de sistemas resistentes frente a los ataques cibernéticos y otras amenazas. Otra publicación a destacar realizada por el *NIST* es la *Guía para la seguridad de los sistemas de control industrial* (*Guide to Industrial Control Systems*): esta guía define controles de seguridad para los sistemas *SCADA* (*Supervisory Control and Data Acquisition*), equipos *PLC* (*Programmable Logic Controllers*) y sistemas *DCS* (*Distributed Control Systems*).

Ámbito internacional

La colaboración público-privada, al igual que la ciberseguridad, no conocen fronteras y por tanto es inútil restringir sus actividades a ámbitos delimitados geográficamente. Teniendo esto presente, el Sistema de Protección de Infraestructuras Críticas en España facilita el encaje de las actividades llevadas a cabo a nivel nacional con aquellas que se emprenden internacionalmente. Muchos de los ciberejercicios presentados en este artículo se diseñan y planifican desde una perspectiva global, pero existen otro tipo de actividades que tienen por objeto fomentar la colaboración público-privada.

En particular, cabe destacar que a nivel de la Unión Europea, el CNPIC es miembro de diversos Grupos de Trabajo enmarcados en el ámbito de la ciberseguridad y de la Protección de las Infraestructuras Críticas. Dentro del Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) existen una serie de iniciativas en las que el CNPIC participa asiduamente, como son: la red de Información para Infraestructuras Críticas (*CIWIN*), el Grupo de Protección Civil- Subgrupo PIC (Comisión Europea) y el Grupo de Expertos sobre PIC Estados Unidos-Unión Europea-Canadá. En este ámbito europeo, se celebró en mayo de 2016 en Ámsterdam, ejerciendo Países Bajos la Presidencia del Consejo de la Unión Europea, una reunión de alto nivel sobre ciberseguridad con participación de altos funcionarios de los Estados miembros encargados de la seguridad cibernética y directivos de empresas de telecomunicaciones, así como responsables de la seguridad de infraestructuras críticas, donde estuvo igualmente representado este Centro.

En lo que respecta al marco de las relaciones con Iberoamérica, y de la mano de la Organización de Estados Americanos (OEA), el CNPIC ha coorganizado con el INCIBE (en Chile, julio de 2015 y en Paraguay, noviembre de 2015) sendos talleres sobre «Protección de Infraestructuras Públicas y Ciberseguridad» con el objetivo de formar en la materia a entidades públicas y privadas de los países de la zona, con la asistencia de once Gobiernos latinoamericanos.

Con un marcado carácter de intercambio de experiencias internacionales en materia de la Protección de Infraestructuras Críticas y la Ciberseguridad, se creó el conocido como *Proceso Meridian* en el año 2005. Ese año se llevó a cabo una primera Conferencia celebrada en Londres. A día de hoy se ha conformado como un foro internacional de gran prestigio, formado por cerca de cuarenta países de los cinco continentes, donde participan exclusivamente gobiernos y cuya presidencia rotatoria es otorgada a países con reconocido prestigio y experiencia en este campo. España ha venido participando en todas las Conferencias Meridian desde el año 2007, a través del CNPIC, y desde el 2012 es miembro de pleno derecho del Comité Directivo, habiendo ostentado durante 2015 la presidencia del Proceso Meridian. Por este motivo el CNPIC organizó en León, entre los días 21 y 23 de octubre de 2015, la 11.ª Conferencia Meridian. Esta se combinó con otro evento global de ciberseguridad, dedicado a empresas y ciudadanos, que se celebró también en León entre los días 19 y 21 y que lideró el Instituto Nacional de Ciberseguridad (INCIBE). Todo ello ha supuesto conjuntamente una de las iniciativas de ciberseguridad de mayor entidad puestas en marcha por un Gobierno a lo largo de 2015.

Bibliografía

Legislación y Normativa Nacional

Ley 8/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas. Boletín Oficial del Estado n.º 102, de 29 de abril de 2011.

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Boletín Oficial del Estado n.º 121, de 21 de mayo de 2011.

Plan Nacional de Protección de Infraestructuras Críticas, de 7 de mayo de 2007. Modificado por Instrucción 1/2016, de 10 de febrero, de la Secretaría de Estado de Seguridad. No publicado en el Boletín Oficial del Estado.

Estrategia de Seguridad Nacional. Catálogo de Publicaciones de la Administración General del Estado. Gobierno de España, junio de 2013.

Estrategia de Ciberseguridad Nacional. Catálogo de Publicaciones de la Administración General del Estado. Gobierno de España, diciembre de 2013.

Plan Nacional de Ciberseguridad. Aprobado por el Consejo de Seguridad Nacional en octubre de 2014. No publicado en el Boletín Oficial del Estado.

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se establecen los contenidos mínimos de los planes de seguridad del operador y planes de protección específicos conforme a lo dispuesto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de infraestructuras críticas. Boletín Oficial del Estado n.º 225, de 19 de septiembre de 2015.

Instrucción número 15/2014, de 19 de noviembre, de la Secretaría de Estado de Seguridad, por la que se crea la Oficina de Coordinación Cibernética del ministerio del Interior. No publicado en el Boletín Oficial del Estado.

Instrucción número 3/2015, de 25 de mayo, de la Secretaría de Estado de Seguridad, por la que se actualiza el Plan de Prevención y Protección Antiterrorista. No publicado en el Boletín Oficial del Estado.

Instrucción número 10/2015, de 10 de septiembre, de la Secretaría de Estado de Seguridad, por la que se regula el proceso de implantación del Sistema de Protección de Infraestructuras Críticas a nivel territorial. No publicado en el Boletín Oficial del Estado.

Instrucción número 2/2016, de 20 de mayo, de la Secretaría de Estado de Seguridad, por la que se regula la coordinación en materia de ciberseguridad en el ámbito del Ministerio del Interior. No publicado en el Boletín Oficial del Estado.

Acuerdo Marco de Colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo. Actualizado con fecha 21 de octubre de 2015. No publicado en el Boletín Oficial del Estado.

Legislación y Documentación Oficial Comunitaria

Directiva 2008/114, sobre la identificación y designación de infraestructuras críticas europeas y la necesidad de evaluar su protección. Diario Oficial de la Unión Europea, Ley 345/75, de 23 de diciembre de 2008.

Directiva 2013/40, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión 2005/222/JAI del Consejo. Diario Oficial de la Unión Europea, Ley 218/8, de 14 de agosto 2013.

Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Diario Oficial de la Unión Europea, Ley 194/1, 19 de julio de 2016.

Programa Europeo de Protección de Infraestructuras Críticas (PEPIC). Comunicación de la Comisión de 12 de diciembre de 2006 sobre un Programa Europeo para la Protección de Infraestructuras Críticas [COM (2006) 786 final-Diario Oficial C. 126 de 7 de junio de 2007].

Propuesta de decisión del Consejo de 27 de octubre de 2008, relativa a una red de información sobre alertas en infraestructuras críticas (CIWIN) [COM(2008) 676 final-no publicada en el Diario Oficial].

Libro Verde de 17 de noviembre de 2005 sobre un Programa Europeo para la Protección de Infraestructuras Críticas [COM (2005) 576 final].

Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 20 de octubre de 2004, «Lucha contra el terrorismo: preparación y gestión de las consecuencias» [COM (2004) 701 final-Diario Oficial C 52 de 2.3.2005].

Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 20 de octubre de 2004, «Prevención, preparación y respuesta a los ataques terroristas» [COM (2004) 698 final-Diario Oficial C 14 de 20.1.2005].

Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 30 de marzo de 2009, sobre protección de infraestructuras críticas, «Protegiendo a Europa de ciberataques a gran escala e interrupciones: mejora de la preparación, la seguridad y la respuesta» [COM (2009) 149 final].

CEPS (*Centre for European Policy Studies*) Task Force Report: «Protecting Critical Infrastructure in the EU», marzo de 2010.

Comisión Europea: «Inventory of Crisis Management Capacities in the European Commission and Community Agencies», mayo de 2010.

Comisión Europea: «Manual de Buenas Prácticas para las Políticas PIC (RECIPE)», marzo de 2011.

Publicaciones

ÁLVAREZ, César, *et al.* (2016), «El modelo de protección de infraestructuras críticas en España». Madrid, Editorial Borrmart S.A.

CARABIAS, José Ignacio, «Protección de infraestructuras críticas y planificación», *Revista Seguritecnia*, n.º 409, junio de 2014.

DE LA CORTE, Luis *et al*. (2014), «Seguridad nacional, amenazas y respuestas». Madrid, Editorial LID.

DUDENHOEFFER, D. D. *et al*. (2006), «Critical Infrastructure Interdependency Modelling», trabajo publicado para el Idaho National Laboratory, ref. INL/EXT-06-11464.

MOTEFF, John D. (2012), «Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress». Trabajo publicado por el *Congressional Research Service*, Washington.

PÉREZ-CHIRINOS, César, *Critical Financial Institutions: BusinessContinuity Scenarios and Costs*, en European CIIP Newsletter, agosto-septiembre de 2009, Volumen 5, n.º 2.

SÁNCHEZ, Fernando J., «Las políticas de protección de infraestructuras críticas en España», *Seguridad y Ciudadanía*, revista del Ministerio del Interior, n.º 11, junio de 2014.

SÁNCHEZ, Fernando J., «Protección de infraestructuras críticas: el Sistema de planeamiento como herramienta de implantación (I)», *Seguridad y Ciudadanía*, revista del Ministerio del Interior, n.º 12, diciembre de 2014.

SÁNCHEZ, Fernando J., «Protección de infraestructuras críticas: el Sistema de planeamiento como herramienta de implantación (II)», *Seguridad y Ciudadanía*, revista del Ministerio del Interior, n.º13, junio de 2015.

VANACLOCHA, Francisco J. *et al*. (2013), «Marco legal y de gestión de las infraestructuras críticas». Madrid, Editorial McGraw-Hill.