

"El espíritu de la normativa PIC se basa en la confianza mutua y en la confidencialidad de la información que se comparte"

Entrevistar a quien lidera el organismo que maneja el Catálogo Nacional de Infraestructuras Estratégicas de nuestro país -una "base de datos" que está calificada como 'secreta'- es harto complicado si lo que la periodista persigue es que el experto le dé algún dato concreto. Por eso, tras insistir -quizá en demasía-, nos quedamos con la apuesta clarificadora que nos ofrece Fernando Sánchez sobre la hoja de ruta planteada para el desarrollo del Sistema español para la Protección de las Infraestructuras Críticas (PIC), y a la espera de que, en breve, se publiquen las Guías con los contenidos mínimos de los diversos planes que marca la reciente Ley y su Reglamento.



Fernando Sánchez Gómez

Director del Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC)

Texto y fotos: Mercedes Oriol Vico.

- La actuación que el Gobierno español ha puesto en marcha para la protección de las Infraestructuras Críticas (IC), a las que usted prefiere llamar protección a los "servicios esenciales", que lidera el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), comprende una serie de infraestructuras, pero no todas ni en todos los casos. Aun con la Ley PIC y su Reglamento en la mano, la expectativa de los operadores gestores y propietarios de las mismas no se aclaran. ¿Nos podría detallar un poco más a qué instalaciones nos referimos y en qué ocasiones se aplica el Plan Nacional (PNPIC)?

La Ley PIC, en su artículo 3.1 -ámbito de aplicación-, es clara y establece que la normativa se aplicará a las infraestructuras críticas, consideradas éstas como aquellas cuyo funcionamiento es indispensable para la sociedad, por lo que una perturbación o destrucción tendría una gran repercusión sobre el servicio esencial que proporcionan. La identificación de estas IC se lleva a cabo a tra-

vés de la aplicación de unos parámetros de impacto cuyos criterios también vienen definidos en el artículo 2 de la Ley.

En cuanto al PNPIC, éste establece criterios y directrices desde el punto de vista de las capacidades operativas de las Fuerzas y Cuerpos de Seguridad (FCS) y, en su caso, de las Fuerzas Armadas. Su aplicación se hará por orden del secretario de Estado de Seguridad, en base a la activación de alguno de los niveles de amenaza que aparecen definidos en el Plan, afectando a todas o algunas de las infraestructuras estratégicas (las contenidas en el Catálogo), dependiendo de si el nivel de amenaza activado es general o se circunscribe a un determinado territorio o sector.

- Al ser el Catálogo de IC un documento calificado de "secreto", hay bastante confusión en los doce sectores estratégicos a los que hace referencia la Ley PIC (Administración, Espacio, Industria nuclear, Industria química, Instalaciones de investigación, Agua, Energía, Salud, Tecnologías de la Información y las Comunicaciones TIC-, Transporte, Ali-

mentación y Sistema financiero y tributario) sobre qué infraestructuras son las identificadas como "críticas". ¿Podría decirnos de cuántas infraestructuras estamos hablando?

El Catálogo de Infraestructuras Estratégicas es una base de datos de uso eminentemente operativo dirigida a su uso por las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y por aquellas otras instituciones o departamentos que tengan autorización para ello. Este catálogo fue clasificado como "secreto" mediante Acuerdo de Consejo de Ministros de fecha 2 de noviembre de 2007, y en él se encuentran referidas a día de hoy alrededor de 3.700 instalaciones, que a su vez se encuentran subdivididas en críticas, esenciales y complementarias. De entre este conjunto, las infraestructuras críticas -que es el ámbito de aplicación de la normativa PIC- suponen entre un 10 y un 15 por ciento del total de infraestructuras incluidas en el Catálogo, aunque aún queda mucho estudio y trabajo por realizar con todos los sectores implicados para actualizar el mismo, y su número se verá probablemente incrementado.



- Puesto que, por Ley, son ustedes -el CNPIC- el órgano encargado, entre otras múltiples tareas, de comunicar a las infraestructuras críticas que lo son, sería muy clarificador que nos comentase si los responsables de estas infraestructuras catalogadas ya están informados de esta identificación, así como de sus correspondientes pasos a dar. ¿Cuál es el plazo de comunicación del CNPIC a los operadores de IC? ¿Cuál es la hoja de ruta a seguir en la protección de infraestructuras críticas (pasos, plazos, guías, planes, etc.)?

Desde hace ya varios años se está realizando un estudio pormenorizado de las infraestructuras estratégicas, con la ayuda inestimable de los titulares de esas infraestructuras pertenecientes a los doce sectores implicados, y con los que se sigue trabajando para llegar a una identificación de aquellas infraestructuras que serán calificadas como críticas, o que, en su caso, serán incluidas en el Catálogo con otra clasificación diferente.

La hoja de ruta a seguir persigue la activación de la batería de planes que van desde el PNPIC a los Planes de Apoyo Operativo (PAO) en un plazo de unos dos años desde este momento. Para el PNPIC, documento ya en vigor desde mayo de 2005, se tiene proyectada su actualización y modificación, de manera que se tengan en consideración la normativa PIC aprobada recientemente.

En cuanto a los Planes Estratégicos Sectoriales (PES), el Real Decreto 704/2011, de desarrollo de la Ley PIC, ya establece un plazo de doce meses desde su publicación para la elaboración y aprobación de uno de ellos por cada uno de los doce sectores contemplados, tarea que corresponde a la Administración del Estado, en colaboración con el resto de agentes del Sistema. En la práctica, estos PES se irán aprobando de forma escalonada en función del sector que se vaya estudiando de forma secuencial.

Ana y Javier Borredá, directora general y presidente de editorial Borrmart, flanquean a Fernando Sánchez. Una imagen tomada en la visita institucional que hicieron al CNPIC.

La Ley y el Reglamento PIC establecen que será el CNPIC, una vez que tenga identificadas esas infraestructuras críticas, el que comunicará oficialmente la propuesta de designación como operador crítico al titular de las mismas, cuyo informe se remitirá para su aprobación a la Comisión PIC, que será en todo caso la encargada de comunicarle la designación definitiva y oficial de operador crítico. De cualquier forma, la consideración de una infraestructura como crítica y, consecuentemente, del operador como tal, será discutida y conocida por el susodicho operador previamente a su designación oficial.

Una vez que el operador es nombrado como crítico, por ser propietario de una infraestructura calificada como crítica nacional o crítica europea, se abre un plazo de seis meses para realizar el Plan de Seguridad del Operador (PSO), y una vez que sea aprobado dicho plan, otro plazo de cuatro meses para la confección de un Plan de Protección Específico (PPE) por cada una de la infraestructuras calificadas como críticas. Sin embargo, de facto, el conocimiento previo del operador de la criticidad de sus instalaciones, permitirá disponer de un mayor espacio de tiempo para la elaboración de los planes.

En cuanto a los PAO, el cuerpo policial competente territorialmente en la demarcación donde se encuentre ubicada la IC deberá realizar este plan en el plazo de cuatro meses a partir de la aprobación del PPE, debiendo contar con la colaboración del titular de la IC implicada. La aplicación de los respectivos PAO se llevará a cabo normalmente con la activación de alguno de los niveles de alerta previstos por el PNPIC.

- ¿Con cuántos grupos de trabajo está colaborando el CNPIC para el desarrollo de este ambicioso plan?

Desde un principio se ha contado con un grupo de personas procedentes de los distintos ministerios, así como de instituciones, órganos y empresas que han colaborado de forma homogénea en la elaboración de la normativa PIC. En la actualidad se mantienen activos cinco grupos de trabajo institucionales relacionados con la protección de las infraestructuras críticas, siendo el más importante de ellos y ya formalizado por el secretario de Estado de Seguridad el Grupo de Trabajo PIC, con participación de once ministerios e instituciones, que constituye el embrión del Grupo de Trabajo Interdepartamental para la Protec-



ción de las Infraestructuras Críticas que consagra la Ley 8/2011.

Además, el CNPIC mantiene numerosos foros y grupos de trabajo informales con empresas e instituciones privadas, en razón a la materia a tratar; entre ellas, se ha estado trabajando en el seno de un grupo informal formado por una serie de empresas y organizaciones públicas y privadas que han aportado su experiencia para llevar a cabo la elaboración de los borradores de contenidos mínimos de los distintos planes creados por la Ley 8/2011 y su desarrollo normativo.

- Si ha habido dicho acercamiento al sector privado desde el inicio, ¿por qué cree que se ha criticado tanto el que ustedes no hayan contado lo suficiente con los profesionales de las principales infraestructuras españolas, con los que se ven abocados a trabajar?

Bueno, eso depende de los profesionales a los que ustedes hayan tenido acceso, y en cualquier caso la generaliza-

¿cuál va a ser la inversión que va a realizar la Administración en la PIC, a corto, medio y largo plazo para las IC que gestiona?

Eso debería usted preguntárselo a las diferentes administraciones que gestionan infraestructuras críticas. A priori, las obligaciones establecidas a los operadores por parte de la normativa PIC son idénticas, independientemente de que los operadores sean públicos o privados, por lo cual el cumplimiento es igualmente imperativo.

En cualquier caso, la mayoría de las infraestructuras bajo gestión de las diferentes administraciones está muy concentrada sectorialmente y, en su mayor parte, están sujetas a regulaciones específicas (véase el caso de los puertos y aeropuertos, por ejemplo) que les obliga a tener implantados una serie de planes de seguridad, autoprotección, emergencia, etc. En este sentido, el esfuerzo económico en la mayoría de los casos (como en tantos otros de instalaciones gestionadas por

■ FICHA PERSONAL

Fernando Sánchez Gómez es el director del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), organismo dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior.

Es oficial de la Guardia Civil (Carrera Superior Militar) y diplomado de Estado Mayor. Ha desarrollado sus funciones en los últimos años en el campo de la Seguridad de Infraestructuras e Instalaciones de carácter estratégico (ámbito físico), tanto en la Dirección General de la Policía y la Guardia Civil, Dirección Adjunta Operativa (Estado Mayor), como en su cargo actual.

puesto que el espíritu de la normativa PIC se basa en la confianza mutua y en la confidencialidad de la información que se comparte, en aplicación de la "asociación público-privada" que debe imperar en esta materia. La colaboración con y entre todos los operadores es vital en un ámbito tan globalizado e interdependiente como el que nos ocupa, debiendo ser todos conscientes de los servicios esenciales que se ofrecen a la sociedad y de la importancia de asegurarlos.

Aún así, en caso de incumplimiento de las obligaciones que establece tanto la Ley como su desarrollo normativo, podrán ser aplicables en la mayor parte de los casos los distintos regímenes sancionadores sectoriales y eventualmente la normativa existente en materia de Seguridad Privada y Protección Civil.

- Las tres vías de actuación con que cuenta el centro que usted dirige son: la legislación, la cooperación y la creación de un sistema de protección de IC con medidas y planes dirigidos a ello. La primera está materializada desde el mismo arranque, en 2004, de la Estrategia Global sobre Protección de Infraestructuras Críticas y el Programa Europeo de Protección de Infraestructuras Críticas (PE-CIP) y posterior trasposición de la Di-

"Hemos trabajado mano a mano con representantes de empresas españolas de primer nivel y no hemos detectado más crítica que aquella constructiva"

ción de su pregunta se me antoja un tanto exagerada. Yo les puedo decir que hemos trabajado mano a mano con representantes de empresas españolas de primer nivel, con los ministerios responsables sectorialmente y con un buen número de organizaciones públicas y privadas y no hemos detectado más crítica que aquella constructiva con el fin de erigir un sistema que está destinado a ser no "el sistema del CNPIC", sino el de todos nosotros; en ello seguimos trabajando y tenemos la puerta abierta a todo tipo de observaciones, colaboraciones, propuestas y, por supuesto, críticas, pero eso sí, constructivas.

- El 20 por ciento de las IC están en manos públicas y, para dar ejemplo,

empresas privadas) está ya en buena parte realizado, debiendo, eso sí, adecuarse a la normativa PIC en la parte que les corresponda.

- El Reglamento no especifica sanciones, tampoco hay ningún órgano similar a la Agencia Española de Protección de Datos (AEPD), con poder controlador y sancionador en el cumplimiento. Además, de la con sabida repercusión social y nacional, ¿qué ocurriría en caso de que un gestor privado no implantase las medidas, políticas y planes correspondientes que marca la Ley PIC?

Es cierto que el Reglamento que desarrolla la Ley PIC y ésta misma no establecen un régimen sancionador,

rectiva 2008/114/CE; pasando por la puesta en marcha en España del primer PNPIC, la creación del CNPIC y la elaboración del primer Catálogo Nacional de Infraestructuras Estratégicas (en 2007); hasta llegar a la entrada en vigor de la Ley PIC y su Reglamento (en 2011). ¿Se ampliará este punto con reformas o legislaciones complementarias?

Actualmente está en proyecto el realizar una reforma al Plan Nacional para la Protección de Infraestructuras Críticas de 2007, para adaptarlo a la normativa existente. La implantación de los planes exigirá también una dedicación y empeño especial, de la mano de todos los agentes del Sistema PIC. Aparte de esto, no existe ninguna otra previsión a corto plazo, si bien como esta materia está en plena evolución y nos hallamos en pleno proceso de construcción, no se deben descartar otras iniciativas legislativas que completen el panorama, si esta necesidad se percibe más adelante.

- Respecto a la segunda -la cooperación-, que ustedes indican como baluarte de esta estrategia, es quizá una de las más complejas. ¿Existe de veras la cooperación? ¿Qué objetivos se tienen que lograr aún? El sector privado critica que es unidireccional, es decir, que CNPIC espera de ellos que les faciliten información y que, sin embargo, ustedes no ofrecen la misma disposición después... ¿Cómo se puede crear ese marco de generosidad y confianza necesario? Usted ha comentado que se trata de "tiempo y contacto permanente": ¿cómo han planificado estos aspectos con el sector público y privado?

Desde la creación de este centro a finales del año 2007 siempre se ha buscado una colaboración estrecha con todos los operadores, tanto del sector público como del sector privado, ofreciendo en todo momento la confianza necesaria para que proporcionen información sobre sus infraestructuras necesaria para su inclusión en el Catálogo Nacional de Infraestructuras Estratégicas. No estaríamos hoy en esta

situación de no existir esa verdadera cooperación, que evidentemente es perfectible y mejorable.

Una vez más, la generalización de que "el sector privado critica que es unidireccional" me parece excesiva y exagerada. No es así, y a las pruebas me remito. Ahora bien, somos conscientes de que, aunque solo sea por razones de capacidades humanas y de tiempo, aún no hemos podido llegar a una parte de los operadores que forman parte del entramado que componen los servicios esenciales en España, y ello puede causar en algunos de ellos un cierto sentimiento de "unilateralidad" que no es real; muy al contrario, nuestro objetivo es poder entablar un contacto provechoso con todos ellos y conocer sus puntos de vista y sensibilidades. En ese sentido nos ponemos a su disposición y les transmitimos el mensaje de que en su momento llegaremos a ellos.

La Directiva Europea 2008/114/CE del Consejo, de 8 de diciembre, sobre la identificación y designación de la Infraestructura vital europea y la evaluación de la necesidad de mejorar su protección solamente implica inicialmente (aunque próximamente será revisado) a dos sectores, Transporte y Energía. El Estado español, en la transposición de esta Directiva, ha sido más ambicioso y ha tenido

Sencillos y de trato abierto, Fernando Sánchez y su equipo conocen bien los desafíos que tienen ante sí. Un lance que, desde Secretaría de Estado, el Gobierno les confía para ser el bastión para la protección de las IC en España.

una visión de futuro más amplia, incluyendo doce sectores a nivel nacional. Esta visión más completa exige a su vez un ingente esfuerzo, y por ello se requiere de los operadores comprensión y tiempo, ya que el abordaje de los diferentes sectores se producirá conforme se vayan efectuando los estudios respectivos.

- ¿Se ha generado ya ese canal de comunicación operativo entre operadores, FCSE, CNPIC... en tiempo real? Y hablando de 'metaseguridad': ¿cómo se va proteger ese canal?

Para el desarrollo no solo de la gestión del Catálogo de Infraestructuras Estratégicas, sino también de un mecanismo de comunicación entre todos los agentes del sistema PIC, se comenzó a trabajar en 2009 en un proyecto denominado HERMES que tenía por objetivo final la acreditación por parte del Centro Criptológico Nacional





(CCN) para la gestión de información nacional clasificada.

En este sentido, los requisitos funcionales para la manipulación de información con distintos grados de clasificación hicieron necesario desarrollar dos plataformas tecnológicas diferenciadas:

1. Plataforma ARGOS, destinada a la gestión del Catálogo de Infraestructuras Estratégicas, y que permitirá la gestión de información clasificada como 'secreto'.
2. Plataforma PI3 (Plataforma de Intercambio de Información sobre Infraestructuras), destinada a proveer un mecanismo de información directo y eficiente entre todos los agentes del Sistema PIC, mediante el establecimiento de herramientas colaborativas como, por ejemplo, una destinada al desarrollo de documentos tipo Wiki, foros de discusión, gestor documental, etc. La plataforma permitirá gestionar información clasificada como 'difusión limitada'.

El desarrollo de las mencionadas plataformas finalizó hace más de un año, si bien los requisitos necesarios para la acreditación de sistemas para la gestión de información nacional clasificada establecen que los aplicativos desarrollados deben estar certificados según la normativa *Common Criteria* por un laboratorio independiente. Actualmente, el proyecto se encuentra a la espera de recibir esta certificación por parte del laboratorio, tras lo cual continuarán los trámites necesarios para obtener la acreditación final por parte del CCN.

De este modo, se pretende garantizar la ausencia de vulnerabilidades conocidas y el óptimo desarrollo y optimización de mecanismos de seguridad no solo respecto a *software*, sino también de las interconexiones entre distintos sistemas.

- ¿Cómo están planificando el tercer pilar: el Sistema PIC? ¿En qué fase se encuentra, sus medidas correspondientes y los diversos planes?

El Sistema de Protección de Infraestructuras Críticas está compuesto por diferentes instituciones, órganos y empresas, procedentes tanto del sector público como del sector privado, y todos ellos con sus diferentes responsabilidades en el correcto funcionamiento de los servicios esenciales que se ofrecen a los ciudadanos.

En cualquier caso, a pesar del ingente trabajo realizado, nos encontramos aún en un estado incipiente de desarro-

"El Estado español ha sido más ambicioso y ha tenido una visión más amplia, incluyendo doce sectores"

llo en el que es preciso impulsar el proceso desde el ámbito político y desde los consejos de Dirección de las empresas. Deben aún constituirse a lo largo de 2012 la Comisión PIC y los Grupos de Trabajo Interdepartamental y sectoriales que den contenido y estructura al propio sistema; y deben materializarse los diferentes planes, de manera escalonada, durante 2011 y hasta 2014. Es decir, lo que se está viendo actualmente es tan solo la 'punta del iceberg' que debe llegar a ser el Sistema PIC y los planes derivados de éste. Estamos tan solo al principio de una aventura apasionante para la cual lo primero que se necesita es concienciación y colaboración desinteresada y genuina de todas las partes.

- El Plan Nacional de IC ya ha entrado en vigor, pero usted ha comentado que hay que reformarlo. ¿Nos podría explicar por qué y en qué?

Como he dicho anteriormente, debe tenerse en cuenta toda la legislación que ha sido aprobada sobre PIC desde 2007, así como el Plan Nacional Antiterrorista al cual está vinculado, y que fue modificado el año pasado.

- ¿Cómo ve el papel de la Seguridad de la Información o de Sistemas (la

"lógica") frente al de la Seguridad Patrimonial (la "física"), en este nuevo planteamiento de protección de IC?

El papel de la seguridad lógica de las infraestructuras está cobrando cada vez más importancia, teniendo en cuenta que la gran mayoría de los servicios esenciales se proveen gracias al correcto funcionamiento de sistemas tecnológicos e industriales. En ambos casos es necesario aplicar mecanismos de seguridad que minimicen el impacto de

un posible incidente, sin que esto repercuta en el adecuado aprovisionamiento del servicio que proporcionan.

No obstante, la seguridad física y la lógica no deben verse como términos contrapuestos y antagónicos, sino que es necesario asumir que ambos se necesitan mutuamente. En este sentido, si bien existe una avanzada cultura de Seguridad, la nueva normativa PIC plantea la necesidad de proveer una Seguridad Integral a las infraestructuras, de modo que todos los eslabones de la cadena sean igual de robustos, siendo este aspecto uno de los grandes objetivos que se persigue desde el CNPIC.

- ¿Qué sectores están más maduros para plantear este desafío?

No se puede establecer un grado de madurez diferenciado sector por sector. El grado de concienciación de los operadores, sean éstos públicos o privados, también es variable pero, en general, se puede afirmar que las empresas y organizaciones españolas tienen un alto grado de madurez en lo que respecta al ámbito PIC, en comparación con otros países.

Los sectores más avanzados en el desarrollo de estrategias que pueden converger con el planteamiento efectuado por la normativa PIC (debido a la exis-

tencia previa de regulaciones específicas o de amenazas específicas que han debido ser abordadas por las compañías durante los últimos años) son quizás el Financiero y Tributario, el de las TIC, el Nuclear y el del Transporte. Junto a éstos, el sector de la Energía también tiene desarrollos muy elaborados que, sin embargo, es preciso coordinar al existir diferentes 'velocidades' dependiendo del operador de que se trate. Precisamente es el de la Energía el sector más trabajado, junto con el del Transporte, por el CNPIC desde su creación en 2007, sectores ambos sobre los que incide la Directiva Europea sobre infraestructuras críticas europeas, de 8 de diciembre de 2008.

- ¿Es válido o está preparado el modelo actual de Seguridad (con la Ley de Seguridad Privada, de 1992) para afrontar este tipo de estrategias globales? ¿Cree que sería necesaria una reforma?

Aunque ésta no es materia de mi competencia (y para ello existen profesionales muy capacitados), la normativa de Seguridad Privada está ya en permanente proceso de revisión y actualización, lógica por otra parte si tenemos en cuenta que la propia sociedad ha evolucionado enormemente en los últimos 20 años.

La mayor novedad que plantea la normativa de protección de infraestructuras críticas, y éste es posiblemente el mayor reto en términos de futuro que afronta el CNPIC, es la consecución de un modelo de Seguridad Integral (seguridad física y seguridad lógica) que se aplique no sólo a las infraestructuras críticas españolas, sino que pueda ser también implantada a medio-largo plazo en las estrategias generales de Seguridad de las organizaciones y empresas nacionales, sean éstas públicas o privadas.

- ¿Qué diferencia existe entre el responsable de Seguridad y Enlace de una IC y el delegado de Seguridad de la IC? ¿Debe ser el directivo de Seguridad de dicha infraestructura, o solo

debe poseer la habilitación de director de Seguridad?

La creación de la figura del responsable de Seguridad y Enlace tiene una clara intención: que la persona que lo ejerza sea un interlocutor válido con los po-

ser su formación? Finalmente: si para infraestructuras como las nucleares, el personal de Seguridad Privada requiere de una formación específica, ¿plantean ustedes una especialización similar para infraestructuras críticas

"La mayor novedad de la normativa es la consecución de un modelo de Seguridad Integral que se aplique también a las estrategias generales de Seguridad de las organizaciones"

deres públicos, con la capacidad de decisión y los conocimientos técnicos de seguridad adecuados a la materia que se está manejando, facilitando de esta forma la colaboración y el correcto trasvase de información entre la Administración (el CNPIC en este caso) y el Operador Crítico. Para ello, y como indica la Ley 8/2011, es necesario tener la habilitación de director de Seguridad o la equivalente, según su normativa específica, con lo cual se deja la puerta abierta a la posibilidad de otras titulaciones específicas reconocidas por la Administración española.

Por su parte, el delegado de Seguridad de la infraestructura que sea catalogada como crítica deberá ser una persona capacitada con los suficientes conocimientos y experiencia en materia de seguridad, pero sin que le sea exigible la habilitación requerida en el párrafo anterior.

Ambas figuras no tienen por qué ser excluyentes, pudiéndose darse el caso en algunos operadores críticos de poder ejercer una misma persona los dos puestos.

- Toda esta estrategia requiere de personal especializado y con experiencia. ¿Cómo ve la preparación de los responsables de Seguridad (CSO) y los de Seguridad de la Información (CISO) con los que están en contacto? Y puesto que son sus interlocutores cualificados, ¿cómo piensa que debe

(no es lo mismo proteger un centro comercial, por ejemplo, que una infraestructura eléctrica...)? ¿De qué manera se podría conseguir?

Como ya les he expuesto anteriormente, el centro lleva ya varios años en contacto con muchos operadores, trabajando con ellos y realizando estudios sobre las diferentes infraestructuras críticas. La conclusión final que hemos podido sacar de esa estrecha colaboración es que las empresas tienen en su seno grandes profesionales de la Seguridad y, gracias a ellos, hemos podido comprender algunos de los entresijos de los sectores objeto de estudio.

Como respondí en una pregunta anterior, uno de los retos principales a conseguir en el futuro es esa 'integralidad' de los departamentos de Seguridad de las empresas, de manera que se engloben en uno único las dos seguridades -física y lógica-. Este concepto implicará necesariamente una evolución en los contenidos formativos de los profesionales de seguridad de las infraestructuras críticas, pero esto es algo que, a día de hoy, es prematuro. Tanto el contenido como la trayectoria formativa a seguir deberá ser madurado convenientemente y serán las autoridades competentes, con la necesaria colaboración de los operadores y de los expertos en el sector, los que diseñen en su momento la especialización exigible a los profesionales de la Seguridad en el marco PIC. **S**