Fernando **SÁNCHEZ GÓMEZ**

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

Fernando Sánchez Gómez es teniente coronel de la Guardia Civil, diplomado de Estado Mayor, y cuenta con 25 años de experiencia en el campo de la seguridad.
Ha participado también en el grupo de trabajo encargado de redactar el borrador de Estrategia Nacional de Ciberseguridad, aprobada en diciembre de 2013, así como del borrador de Estrategia Nacional de Seguridad Energética, aprobada en julio de 2015.
Ha participado, como representación española, en las discusiones en la Comisión Europea para la redacción de la Directiva sobre protección de infraestructuras críticas europeas, y es el punto de contacto del Estado español con la Unión Europea en esta materia.
Ha realizado varios cursos oficiales de la Guardia Civil, y participado en misiones internacionales con la UE y la ONU.
Es autor de diversas publicaciones y colabora asiduamente en la impartición de cursos sobre infraestructuras críticas.

El operador es el responsable primero de la seguridad de su instalación

El Centro Nacional para la Protección de las Infraestructuras Críticas, CNPIC, es una entidad dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior. Su director, el teniente coronel de la Guardia Civil, Fernando Sánchez, ejerce como coordinador en la elaboración y desarrollo de la normativa española sobre protección de infraestructuras críticas, que ha colaborado a redactar como director de los equipos de trabajo.

EL CNPIC

El CNPIC, que alcanza en 2017 su décimo aniversario, trabaja en doce sectores: Administración, Agua, Alimentación, Energía, Espacio, Industria Química, Industria Nuclear, Instalaciones de Investigación, Salud, Sistema Financiero y Tributario, Transporte y Tecnologías de la Información y las Comunicaciones.

Explica su director que "el CNPIC depende de la Secretaria de Estado de Seguridad, por lo tanto está en una posición ideal para coordinar desde el punto de vista operativo las Fuerzas y Cuerpos de Seguridad del Estado y, en general, todos los cuerpos de seguridad que prestan el servicio sobre las infraestructuras críticas, fundamentalmente desde el punto de vista estratégico y preventivo".

"Además, tenemos una faceta reguladora muy importante, ya que establecemos normas de planificación que los operadores críticos tienen que cumplir". Sin embargo, destaca que "el operador es el responsable primero de la seguridad de su instalación, tanto en España como en toda la Unión Europea. Las Fuerzas y Cuerpos de Seguridad, desde el punto de vista operativo, y nosotros, desde la coordinación, estamos para apoyarles, pero la responsabilidad de la seguridad reside primariamente en el operador".

> El sector nuclear ya tenía una labor de gestión de la seguridad muy avanzada. En otros sectores hemos empezado desde cero

LA COORDINACIÓN

La coordinación entre el operador, el CNPIC y las Fuerzas y Cuerpos de Seguridad del Estado es fundamental. Para ello existen diversas herramientas, como explica el teniente coronel Sánchez. "Una es la regulación a través de la propia Ley, que establece la figura del operador crítico como un sujeto no sólo obligado por la Ley, sino como parte del Sistema de Protección de Infraestructuras Críticas". Este sistema se arbitra de diferentes formas: "por un lado a través de nuestra capacidad reguladora, ya que el operador crítico tiene que informarnos sobre cómo está gestionando la seguridad en el conjunto de la corporación, y no sólo en la infraestructura crítica. Ahí ya tenemos esa labor de coordinación con el operador".

"Después, desde un punto de vista menos regulatorio, tenemos un canal abierto permanentemente, tanto por teléfono como vía web, con el responsable de seguridad, que es nuestro enlace. Este responsable debe ser una persona con capacidad de decisión y peso específico, y es quien puede enlazar con nosotros 24 horas al día y siete días a la semana", concluye Sánchez.

En mayo de 2016 se renovó el Plan Nacional de Protección de Infraestructuras Críticas, y se creó la Mesa de Coordinación de Protección de Infraestructuras Críticas, donde está representados los operadores críticos, a razón de uno por cada sector objeto de regulación. El sector nuclear tiene un representante en esa mesa.

EL DESARROLLO DE LA LEY Y LOS PLANES DE SEGURIDAD

El teniente coronel Sánchez reconoce que la Ley de Protección de Infraestructuras Críticas es compleja, porque se basa en un sistema de planificación muy piramidal, pero añade que "cumple con el objetivo de que todos los planes enlacen entre sí y el sistema de protección sea un conjunto cohesionado".

"El Sistema de Protección de Infraestructuras Críticas –explica–se basa en **cinco tipos de planes**. El **primero** es el Plan Nacional de Protección de Infraestructuras Críticas, creado en 2007 y que se ha actualizado en 2016 asimilándolo con el Plan Antiterrorista, de forma que contempla cinco niveles de amenaza y una serie de obliga-

> Estamos en la cabeza a nivel europeo en desarrollo normativo

ciones y requerimientos a las Fuerzas y Cuerpos de Seguridad del Estado, a las Fuerzas Armadas, al CNPIC y a los propios operadores. En el **segundo** nivel está el Plan Estratégico Sectorial. Para elaborarlo nos ponemos en contacto con los expertos, y en el caso del sector nuclear trabajamos con el CSN, el Ministerio, –entonces de Industria y hoy de Energía–, y con consultoras, para conocer al sector: sobre qué base normativa se apoya, qué servicios ofrece, quiénes son los agentes principales, qué grado de dependencia tiene con otros sectores, cuáles son las principales vulnerabilidades desde el punto de vista de seguridad o qué amenazas podemos encontrar. Después seguimos descendiendo haciendo un análisis de riesgos, y finalmente obtenemos la tipología de activos, y cuáles son los actores principales. Es un proceso interactivo, que hacemos conjuntamente con el operador".

Sobre esos dos planes se construyen **los planes de seguridad específicos y los planes de apoyo operativo**. La preparación de cada plan requiere alrededor de un año y, a partir de ahí, se empiezan a desgranar los planes de tipo inferior. "Precisamente ahora vamos a cerrar la etapa inicial de los primeros sectores, con los planes estratégicos sectoriales de energía, nuclear y financiero, y los planes de apoyo operativo ya se están empezando a redactar. Con esto ya tenemos cerrado el ciclo. Es lento pero nos permite establecer un sistema muy sólido y estable", concluye el director del CNPIC.

En el caso nuclear, el Plan de Protección Específico coexiste con el Plan de Protección Física Nuclear, donde ya participan las Fuerzas y Cuerpos de Seguridad del Estado. Según indica Fernando Sánchez, "los requerimientos nuevos por nuestra parte se refieren fundamentalmente al ámbito cibernético, porque la parte física está muy bien integrada". En cuanto a los planes de apoyo operativo, es ahí donde se enmarca la presencia de la Guardia Civil en las centrales nucleares. Afirma Sánchez que "el sector nuclear es diferente al resto porque ya tenía una labor de gestión de la seguridad muy avanzada, como ocurre con el marítimo o el aeronáutico, mientras que en otros sectores hemos empezado desde cero".

Tal y como nos informa el director, a medida que se va perfeccionando el sistema TIC y la ciberseguridad, los

> El concepto de seguridad integral exige al operador unas medidas de ciberseguridad en el mismo nivel que la seguridad física

planes de protección específicos se han ido integrando en los PPF. De hecho, hace algunos meses el secretario de Estado de Seguridad firmó los primeros planes integrados en el sector nuclear.

LA SITUACIÓN EUROPEA

Le preguntamos al director del CNPIC sobre el estado de desarrollo normativo de España con respecto al conjunto de los países europeos. Su respuesta es clara: "estamos en la cabeza, sin lugar a duda, a nivel europeo, y somos de los más avanzados, conjuntamente con Francia y Gran Bretaña".

El sistema francés, según nos explica, "es básicamente legal, aún más reglamentado que el nuestro", mientras que el británico "tiene menos de reglamentación y más de buena voluntad y cooperación. En nuestro sistema la base es la cooperación, tanto público-privada como público-pública, pero con un soporte normativo importante. Otros países, también muy avanzados como Alemania u Holanda, se dirigen más hacia el campo de la ciberseguridad, y estamos en el pelotón de cabeza en ese sentido".

Señala también Fernando Sánchez que "participamos conjuntamente con el CSN en el grupo de trabajo que está redactando una nueva guía, en el ámbito del OIEA, y hemos sido invitados a participar en reuniones en Viena, para ver cómo es el modelo español de ciberseguridad".

LA CIBERSEGURIDAD Y LA SEGURIDAD INTEGRAL

La influencia de las tecnologías de la información y la comunicación en el ámbito de la seguridad es indudable. En este sentido, el director del CNPIC señala que "fuimos los primeros en España, y uno de los primeros a nivel internacional, en incorporar el concepto de "seguridad integral" en la Ley".

Se trata de reconocer que la seguridad "no considera sólo la parte física –las puertas, vallas, controles de acceso, cámaras o vigilantes– sino que hay mucho más, relacionado con la ciberseguridad, que puede afectar de forma muy grave no sólo a la seguridad de una organización sino incluso a la prestación del servicio".

Partiendo de esta premisa, "desarrollamos el concepto de segu-ridad integral, que exige al operador unas medidas de ciberseguridad en el mismo nivel que la seguridad física. Lo que encontramos en un principio es que la organización de las empresas separaba la dirección de seguridad –eminentemente fí-sica– de la gestión de las TIC –básicamente dirigida a la web y la gestión económica–, con una cla-

ra falta de coordinación entre ambas".

"Por eso, definimos la figura del responsable de seguridad y enlace, que gestione no sólo la seguridad física sino que contemple también la parte cibernética, aunque no sea especialista; eso ha obligado a que muchas empresas estén reorganizándose internamen-te".

EL CERTSI, UN ELEMENTO CLAVE DE COORDINACIÓN

Dentro del CNPIC existe un servicio dedicado a la ciber-seguridad, dentro del cual está la Oficina de Coordinación Cibernética del Ministerio del Interior. El enlace con el MINETAD se realiza con el Instituto de Ciberseguridad, INCIBE, a través del CERT *(Computer Emergency Response Team)* de Seguridad de Industria, CERTSI.

Situado en León, el CERTSI es el centro de respuesta a incidentes cibernéticos, un órgano muy técnico "donde el valor añadido no son los medios ni las capacidades técnicas sino el conjunto de los profesionales, que son expertos con un alto nivel técnico", indica el Teniente Coronel Sánchez.

La labor de desarrollo tecnológico y apoyo cibernético a los operadores corresponde al Centro, pero la competencia es del Ministerio del Interior, a través del CNPIC.

LAS POSIBLES AMENAZAS

Las amenazas pueden tener diferentes orígenes y afectar a distintas partes de las instalaciones. Preguntamos al director del CNPIC por el proceso de detección y seguimiento de una posible amenaza.

"Hay un canal abierto permanen-temente –indica– entre el responsable de seguridad y enlace y nosotros. Si se produce una emergencia de tipo radiológico o nuclear ya existen organismos de respuesta perfectamente estructurados. Si hay una emergencia de otro tipo de seguridad, se activa la Célula de Crisis del Ministerio del Interior o incluso, si tiene que escalar, el Departamento de Seguridad Nacional".

Diferente situación se presenta si hablamos de ciberseguridad. "La competencia en materia de ciberseguridad del sector privado corresponde

> Cualquier empresa que esté conectada a Internet a través de una página web puede ser atacada, y si no está protegida puede sufrir pérdidas importantes

100 % a nosotros, a través del CERTSI. Si la crisis se produjera en el ámbito de las administraciones públicas, la competencia estaría en el Centro Criptológico Nacional".

Fernando Sánchez ilustra con claridad la diferencia entre la coordinación ante un posible ataque a la seguridad física o radiológica, y un ciberataque. "En un ataque o incidente de tipo físico, el tiempo de respuesta es mayor, y la dirección de la central se pone en contacto con el jefe de la Comandancia o incluso a un nivel superior y se van dando instrucciones. En el caso de un ciberataque, hay que tener en cuenta que el efecto es desconocido y, por lo tanto, la respuesta se va decidiendo sobre la marcha, pero en cuestión de segundos. Además, son los propios expertos, tanto de la instalación como del CERTSI, los que se ponen de acuerdo para trabajar conjuntamente", concluye.

EL CASO DE LOS CENTROS HOSPITALARIOS

Los hospitales y centros sanitarios tienen material radiactivo, pero no se consideran infraestructuras críticas. A este respecto, señala el teniente coronel Sánchez que "precisamente estamos iniciando los estudios para el Plan Estratégico Sectorial de la Salud, porque uno de los temas que tenemos interés en analizar es cómo se gestiona el material radiológico que hay en los hospitales".

"Nuestro objetivo es que ese Plan Estratégico esté finalizado a lo largo del año y, a partir de ahí, identificaremos quién es operador crítico y seguiremos el proceso".

EL INCIBE

El INCIBE es un organismo cada vez más conocido por el público, especialmente después de los recientes ataques cibernéticos sufridos en España y muchos otros países.

Según señala Fernando Sánchez, "inicialmente tenía como objetivo fundamental el apoyo en materia de ciberseguridad al ciudadano y a la empresa en general, aportando información para concienciar en cuestiones básicas".

Sin embargo, el acuerdo suscrito hace unos años entre el Minetad y el Ministerio de Interior "dio capacidad al INCIBE para que, a través del CERTSI, entrara en la parte de los operadores críticos, y es ahí donde se está desarrollando la mayor inversión".

Una de las iniciativas conjuntas son los CyberEx, ciberejercicios que ya van por la quinta edición, en los que participan las centrales nucleares y que recrean un ataque cibernético.

Por otra parte, la actividad que lleva a cabo el INCIBE dirigida a la ciudadanía es fundamental, según afirma el director del CNPIC, porque "no hace falta ser una infraestructura crítica para ser víctima de un ciberataque. Cualquier empresa que esté conectada a Internet a través de una página web puede ser atacada, y si no está protegida puede sufrir pérdidas importantes". ■