Cuevavaliente Ingenieros es una de las contadas empresas dedicadas exclusivamente a la consultoría e ingeniería de seguridad en España. Por ello es importante conocer a través de esta entrevista cómo ha afectado al sector de la consultoría las nuevas necesidades de las empresas derivadas de la aplicación de la legislación de protección de infraestructuras críticas (PIC). Entrevistamos para ello a Enrique Bilbao, ingeniero de Telecomunicación, socio y director técnico de Cuevavaliente Ingenieros.

Enrique Bilbao
Director técnico de Cuevavaliente Ingenieros

"Habría que recuperar la figura de empresa de asesoramiento o crear una nueva de experto consultor"

- La actividad de Cuevavaliente Ingenieros parece poco habitual en el sector de la Seguridad.

Dedicarse a la consultoría y a la ingeniería de forma exclusiva no es muy habitual, es cierto. Muchas empresas de seguridad, ya sean de vigilancia o de instalaciones y mantenimiento de sistemas, o de ambas actividades, incluyen entre sus servicios los de consultoría. No obstante, desde nuestro punto de vista es más interesante para los clientes que la planificación de su seguridad, el análisis de sus riesgos o la auditoría de sus medidas de protección se realicen por parte de empresas que no tengan otros intereses que el propio juicio de la situación. En este sentido, no somos la única empresa que presta este tipo de servicios, pero es cierto que no somos muchas las de este perfil.

- ¿Cómo ha afectado al trabajo de Cuevavaliente Ingenieros la aplicación de la legislación sobre protección de infraestructuras críticas a las empresas españolas?

Esta es una pregunta cuya respuesta es compleja. Por un lado, nosotros ya estábamos trabajando desde nuestra actividad de consultoría en asesorar a las direcciones de Seguridad de grandes empresas en la adopción de modelos de gestión basados en mejora continua, utilizando la normativa ISO 31000, implantando métricas para evaluar el desempeño de la seguridad, etc.

Por otra parte, ya éramos conscientes de la tendencia imparable de conjugar la seguridad tal y como la conocíamos con la ciberseguridad, ya que los riesgos deliberados habían cambiado de centrarse en amenazas sobre los medios físicos a hacerlo también en el ciberespacio. Unidos a empresas de ciberseguridad, ya habíamos prestado servicio a grandes empresas que querían reorganizarse en este sentido, desarrollando para ello una metodología de análisis de riesgos, por ejemplo, común a la seguridad tradicional y a la ciberseguridad.

Por ello, la obligación que se deriva de la legislación PIC de que los operadores críticos tengan que incluir en su organización un modelo de gestión de seguridad normalizado (con ISO 31000 por ejemplo) y que deban coordinar conjuntamente la seguridad tradicional y la ciberseguridad nos ha *pillado* con mucho camino recorrido.

- ¿Cuál es su opinión respecto de esta legislación, en general?

Por una parte, hay que tener en cuenta que nuestra empresa tuvo la fortuna de participar en los grupos de trabajo de apoyo al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) desde el principio, en 2011, formando parte del denominado Grupo Informal de Protección de Infraestructuras Críticas (GIPIC). Este grupo, coordinado y dirigido por el CNPIC, participó en múltiples documentos y guías, así como en los estudios de los Planes Estratégicos Sectoriales que han dado lugar a las designaciones de algunas empresas como operadores críticos.

Esta participación nos permitió entender en profundidad las necesidades que se pretendían cubrir desde la legislación PIC y los problemas que podrían afectar a las empresas designadas como operadores críticos, lo que a su vez nos ha permitido ofrecer a las empresas propuestas de asesoramiento muy ajustadas. Pero, sobre todo, nos hemos sentido muy identificados con el CNPIC por los pasos que han dado e, incluso, por el perso-

nal del centro que hemos conocido y del que tenemos una magnífica impresión, tanto desde el punto de vista de los conocimientos que han desarrollado como del grado de implicación y compromiso que muestran.

En general creo que como legislación de seguridad es muy rompedora, y no solo por los conceptos modernos que incluye desde un punto de vista de organización de la seguridad, sino también desde el propio enfoque de esa legislación y de la estructura de relaciones entre la Administración y las empresas que implica.

Es una legislación que trata a las empresas como colaboradores, no como simples *sufridores*. Los Planes Estratégicos Sectoriales se han realizado con la participación de las principales empresas de esos sectores, escuchándoles como no se había hecho antes, además de con la participación de los ministerios y organismos implicados.

También es una legislación que no impone medidas concretas ni sanciones, sólo impone modelos muy abiertos de organización que permitan garantizar que las empresas responden a los riesgos, pero con criterios propios.

Finalmente, establece un canal de colaboración mutua real, con los Planes de Apoyo Operativo que se conjugan con los propios planes de las empresas (los Planes de Protección Específicos) y con la existencia del CERT de Seguridad e Industria, que ya está prestando servicios reales a las empresas.

Desde nuestro conocimiento, la legislación PIC y el propio CNPIC son modélicos en comparación con el resto de los países en Europa.

- ¿Hasta qué punto Cuevavaliente Ingenieros está trabajando actualmente en el asesoramiento a las empresas afectadas por la legislación PIC?

Por el propio contenido de nuestro trabajo no hacemos publicidad de estos servicios, pero sí podemos decir dos cosas: hemos generado una base de conocimiento mutuo y un acuerdo estratégico de colaboración con una de las empresas punteras del sector de la ciberseguridad, Deloitte, que nos ha permitido ofrecer y, a veces contratar, importantes servicios de asesoramiento a operadores críticos para la elaboración de los documentos exigidos en la legislación PIC y para la reorganización de sus departamentos de Seguridad.

Y, en segundo lugar, hemos tenido la suerte de hasta la fecha haber participado en la elaboración de los PSO y los PPE de una docena de empresas.

Lo más importante es que la metodología de análisis de riesgos desarrollada por Cuevavaliente, plasmada en la aplicación informática GR2Sec, no sólo está siendo muy útil (incluso ya ha sido adquirida por algu-

nas empresas para su utilización), sino que además ha permitido identificar y evaluar riesgos conjuntos de amenazas físicas y ciberamenazas que antes no se habían tratado.

- ¿Qué sugerencias generales haría al sector respecto de la legislación PIC?

Se me ocurren tres tipos de sugerencias a hacer. Unas para las empresas, que no limiten sus modelos de organización ni las medidas a adoptar a aquellas amenazas y a aquellos activos señalados por la legislación PIC. Las obligaciones derivadas de su cumplimiento son una buena práctica a extender al resto de la empresa: análisis de riesgos conjunto, considerar amenazas o activos no incluidos, etc.

En cuanto a la Administración, en general, creo que es muy importante en lo que respecta a la seguridad privada armonizar su legislación con la de PIC. Seguir considerando a las empresas como colaboradores necesarios, no sólo como meros *sufridores* de la Ley. En ese sentido, la Ley de Seguridad Privada (exceptuando el tema no menor de las sanciones) parece seguir en parte ese camino, pero la oportunidad del Reglamento no se puede dejar pasar.

Adicionalmente, me gustaría destacar que, tras el cambio de la última Ley de Seguridad Privada, las empresas de asesoramiento y planificación de Seguridad hemos dejado de estar supervisadas por el Ministerio del Interior. Considerando la criticidad de la información manejada y la necesidad de asesoramiento experto por parte de los operadores críticos, sería positivo recuperar la figura de la empresa de asesoramiento o una nueva de experto consultor de seguridad, con las obligaciones y derechos que ello conllevaría.