Infraestructuras críticas: urgen más filtros a los operadores

La vida cotidiana está sujeta a un entorno constante de infraestructuras críticas: las comunicaciones, el transporte, el sector nuclear son sólo algunos de los ámbitos que generalmente solemos mencionar cuando hablamos de lo importante que es defender determinadas instalaciones “vitales” para la sociedad. Sin embargo, no son sólo éstas las infraestructuras que podrían considerarse esenciales y tampoco es homogénea la manera como la legislación “tutela” dichos enclaves.

El sector nuclear, por ejemplo, lleva muchos años de delantera cuando nos referimos a la normativa que les regula. Es un sector históricamente polémico, sujeto a decisiones políticas controvertidas y víctima de múltiples protestas municipales o ecologistas. Seguramente por ello, ha sabido desarrollar una reglamentación muy específica de la mano de las Administraciones Públicas, y por tanto es un modelo de regulación ejemplar para otras instalaciones consideradas también críticas.

En el transporte podríamos decir que la regulación es desigual: avanzada en el ferrocarril de vía rápida (AVE), pero indefinida para los trenes de media y larga distancia y para los convoyes de cercanías, y más vaga para las instalaciones aeroportuarias.

Si observamos qué sucede entre las compañías de energía que suministran la electricidad, el gas y el agua, veríamos que el sector carece de estándares y que, a la postre, cada empresa aplica su propio plan a su manera.

Lo que no sucede en la industria que suministra o realiza instalaciones de seguridad o vigilancia, donde por ejemplo la cuestión del manejo o prevención de explosivos está muy regulada.

La lista podría ser mucho más amplia. Antes se circunscribía a embajadas, bases militares y prisiones. Ahora encontramos hasta centros de datos y sedes de agencias de noticias y, por qué no, a la cadena alimentaria.

Proteger toda la cadena

En puridad, tendríamos que empezar a reconocer todos los que trabajamos en este ámbito que la mejor garantía para evitar sustos radica en proteger el conjunto de la cadena de protección de una zona determinada: sus accesos, sus barreras físicas de entrada y perimetrales, sus sistemas electrónicos, de intrusión, de robo, de fuego, sus esclusas, sus cámaras acorazadas y cajas fuertes, sus alarmas y sus sistemas de transmisión... Hablo de las cuatro “virtudes

cardinales” de la teoría de la seguridad desde el tiempo de las catapultas romanas: detectar, advertir, proteger y reaccionar.

Controlar estos cuatro aspectos en una infraestructura crítica no es nada fácil. Al revés, resulta extremadamente complejo. Y por desgracia hemos de reconocer que la amenaza terrorista ha acelerado la toma de conciencia sobre la necesidad urgente de homogeneizar los sistemas de protección de dichas instalaciones (366 atentados en el mundo en 2015, 145 detenciones en España). Es la Administración Pública la que lógicamente tiene la última palabra. A los operadores nos corresponde asesorar y aportar conocimiento y soluciones a la cada vez mayor sofisticación de los ataques, ya sean físicos, cibernéticos o de cualquier otra índole.

8 CONSEJOS PARA LA SEGURIDAD EN INSTALACIONES DE ALTO RIESGO
Hacer una auditoría de seguridad o una evaluación de riesgos
Invertir en seguridad garantiza la continuidad de las operaciones
Elija un sistema con capacidad para evolucionar
Para sacar todo el partido a sus sistemas de seguridad, deben estar completamente integrados
Saque partido al internet de las cosas
La seguridad debe ser parte integrante de su negocio
Enseñe a sus empleados a estar vigilantes
Recuerde que por fiable que sea la seguridad, es imposible evitar un ataque

Porque si hay algo de lo que nadie duda es que los ataques cambian. Cambian las tecnologías y los tipos de agresiones, que pueden venir de empleados deshonestos, de criminales, de manifestantes violentos, de grupos antisistema y por supuesto de grupos terroristas. Las técnicas que provocan situaciones de riesgo van siempre por delante de nuestra prevención. De ahí que algunos no nos cansemos en reclamar la conveniencia de certificar productos y empresas que

garanticen la seguridad que todos deseamos. En definitiva: que no todo el mundo pueda instalar cualquier cosa.

Conviene, por consiguiente, tener en cuenta una serie de factores clave a la hora de elegir un partner: el tipo de actividad que se desarrolla en la instalación, la zona circundante, el movimiento de personas, el tiempo de reacción de los servicios locales de emergencia y las consecuencias que un accidente o un ataque podrían tener en el negocio, tanto en sus actividades como en su reputación.

Más filtros

Por eso reclamo filtros. Reclamo que las normativas sean homogéneas y que se diga con claridad meridiana qué y cómo hay que certificar. Y lo digo después de haber dedicado toda mi vida profesional al sector de la seguridad y de estar trabajando en Gunnebo, la única empresa que en España completa el portafolio global de necesidades de protección física y electrónica de estas instalaciones.

Y nos falta mucha información sobre “momentos de riesgo” y estadísticas para valorar mejor las incidencias. Sabemos que se producen muchas alertas sin riesgo que conviene analizar. Por eso es preciso también hacer análisis de riesgo en profundidad en la inmensa mayoría de nuestras zonas críticas.

Solamente cabe asegurar una cosa: nuestro país no es menos seguro que los de nuestro entorno, probablemente al contrario. Pero conviene no bajar la guardia ni reducir presupuestos, no vaya a ser que acabemos teniendo al enemigo en casa.

Antonio Pérez

Director Seguridad Física y Compartimentación de Gunnebo España, S.A.

Presidente Asociación Española de Empresas de Seguridad