JESÚS DE LA MORA. DIRECTOR DE CONSULTORÍA. SECURITAS SEGURIDAD ESPAÑA

Infraestructuras Críticas

Necesidad de articular la protección con herramientas de gestión de la seguridad

EN ocasiones es bueno echar la vista atrás para comprobar los avances que hemos tenido en España en cuanto a la protección en general y, en especial, en lo que afecta a las infraestructuras críticas, sobre todo como consecuencia de la Ley PIC 8/2011, normas y disposiciones de desarrollo, así como la importancia del CNPIC, entre otros. Sin duda las estructuras de las compañías cada día van tomando más conciencia de que la protección articula y garantiza los servicios esenciales para la sociedad, por lo que más allá de las áreas de gestión de la seguridad, por primera vez, los máximos responsables de las compañías privadas, siendo conscientes del coste que ello supone en algunos casos, permiten garantizar las operaciones con garantías y, sobre todo, la confianza que da estar preparados para detectar, hacer frente, controlar o llevar a cabo actuaciones para recuperar la actividad, ante posibles ataques que tengan su origen en el terrorismo o actuaciones derivadas del concepto «ciber» (ciberataques, ciberdelincuencia, etc.). En este sentido, y desde que se comenzaron a identificar los primeros operadores críticos, hace ya dos años, sería oportuno indicar que en nuestro país se están dando pasos muy importantes en la eficiencia a la hora de proteger nuestras infraestructuras críticas.

Otro avance, quizás más lento, pero irreversible es, sin duda, la convergencia de las diferentes seguridades, que tienden a unificarse bajo el paraguas de un mismo responsable, si bien tienen que pasar algunos años para que se generalice esta situación en las compañías. Pero hay otra convergencia que por primera vez se está produciendo en nuestro país, y es sin duda la que considero más relevante, se trata de la convergencia entre la propia administración, a través del CNPIC principalmente, los operadores críticos (la mayoría en manos privadas), y las empresas de seguridad, consultoras, etc., que desemboca en un trabajo común, tomando conciencia de una corresponsabilidad y de la necesidad de trabajar y colaborar juntos en este proceso.

También hay que destacar los profesionales que se están formando y especializando en las IC (seguridad física / seguridad lógica), para lo cual la normativa de seguridad privada es un gran pilar dentro de la protección de este tipo de instalaciones. También las nuevas tecnologías y la especialización del personal de seguridad, entre otros.

Pero más allá de las medidas de protección y los PSO y PPE , considero que hay una carencia significativa en cuanto a la implantación de herramientas de

gestión de la seguridad. Sin duda hemos dado pasos muy importantes en la protección, pero se ha avanzado poco en el desarrollo de herramientas de análisis para la gestión de este tipo de instalaciones.

Las instalaciones en general, y las IC en particular, necesitan herramientas de gestión que sean transversales con relación a la protección de las instalaciones, teniendo en cuenta las principales áreas afectadas por la seguridad, sobre todo a nivel de indicadores.

En Securitas llevamos años perfeccionando un modelo de gestión que abarque todas las necesidades a través de nuestra herramienta Securitas Connect, la cual permite, dentro de un entorno web, con dispositivos y soluciones de movilidad, disponer de información en tiempo real, donde interactúan todas las partes afectadas (cliente, gestores y personal de seguridad, principalmente). Se trata de una herramienta multi instalación que permite la gestión de todos los aspectos que afectan al ámbito de la seguridad, destacando, entre otros, los siguientes:

• A nivel operativo, permite generar las supervisiones, tareas, informes, con notificaciones automáticas de incidencias, incorporando todo tipo de formularios que permiten una digitalización completa de los procesos operativos, además de una visualización a nivel de control de presencia, geolocalización, incluyendo localización indoor, así como la visualización de las cámaras de seguridad, entre otros.

• Con indicadores de calidad que permitan medir el desempeño y eficacia del servicio, así como generando estadísticas de forma gráfica y analítica para valorar el cumplimiento de los compromisos adquiridos o pactados, estableciendo para ello KPIs a medida.

• Con herramientas de análisis que permitan analizar el comportamiento de los sistemas de seguridad, el origen de las posibles anomalías, el tipo de respuesta y su resultado, además de indicadores sobre la gestión de alarmas y el resultado de las mismas.

• Estableciendo un Plan de Formación específico, acorde a la instalación, actividad y riesgos del cliente, identificando para ello dentro del catálogo de cursos las acciones formativas a desarrollar y haciendo un seguimiento de las mismas con relación al progreso de cada usuario.

• Con acceso a la información relevante sobre programación de servicios y documentación general de las instalaciones, manuales, procedimientos operativos, planos, etc.

Los datos que se generan con esta herramienta son muy importantes pero aún más importante es el data mining o explotación de los datos para manejar un volumen importante de información, por lo que se hacen necesarios métodos de análisis para su procesamiento, siempre desde dos ámbitos: por un lado, existe la necesidad de que el cliente tenga visibilidad de la información más relevante, sobre todo en el día a día, así como transformar el conjunto de los datos en inteligencia para conocer tendencias, tomar decisiones y optimizar recursos. Es evidente que la información bien tratada permite adelantarnos a los acontecimientos y, como consecuencia de ello, se pueden llevar a cabo actuaciones preventivas o de reacción. Lo importante no es la información, sino cómo se utilice la información para hacer inteligencia de la misma.

Las empresas necesitan de este tipo de herramientas, y sobre todo las IC, las cuales permiten, como un engranaje dentro de la protección, trabajar con «datos» tratados y obtener «inteligencia» de los mismos con el fin de ser más eficientes, por ejemplo elaborando mapas de riesgo donde se tengan en cuenta todas las áreas de las instalaciones, principalmente las zonas más sensibles, y «enfrentar» las posibles amenazas con las vulnerabilidades, para analizar aspectos de probabilidad, impacto, posibles pérdidas, etc. En definitiva se trata de establecer una metodología que permita transformar los datos en información y éstos en inteligencia. La toma de decisiones siempre tiene que tener una base sólida, sobre todo cuando se trata de garantizar la protección de los activos y el desarrollo de la actividad de las empresas.

Aunque en un contexto global estas herramientas sean una pequeña parte de la seguridad, sin duda ayudan de forma significativa a afrontar las amenazas que tenemos en el mundo y, en especial, en Europa.

Fotos: *Securitas/Pixabay*

Contactos de empresas, p. 7.