
# FORO SICUR. AES - APROSER

El pasado 21 de febrero, en el marco de FORO SICUR, se celebró la jornada **"CALIDAD E INFRAESTRUCTURAS CRÍTICAS: ENFOQUE DESDE UN URGENTE Y NECESARIO NUEVO REGLAMENTO DE SEGURIDAD PRIVADA"**.

Un año más, AES y APROSER organizan conjuntamente una jornada de candente actualidad durante SICUR, la feria de seguridad más importante de España y sin duda de las más relevantes de Europa.


**El presidente de APROSER, Ángel Córdoba,** fue el encargado de inaugurar la jornada, poniendo de relieve la necesidad de la exigencia de la calidad en los servicios de seguridad privada, exigencia esta que debería contemplar el Reglamento. Como explicó, ni los servicios ni la calidad pueden ser los mismos en un comercio que en una infraestructura crítica.

**Carlos Cantelar,** expuso la calidad como parámetro esencial del diseño de servicios de seguridad privada en las infraestructuras críticas. Desde la definición de calidad de la RAE, pasando por la especificación técnica de las empresas de APROSER como un servicio de gestión profesional y deontológico de los servicios de seguridad privada, la Ley de Seguridad Privada 5/2014 y la de Infraestructuras Críticas, 8/2011, la principal necesidad de cualquier organización explicó, es garantizar la continuidad de sus operaciones, y para ello necesita garantizar la necesidad de todos sus activos tanto tangibles como intangibles.

Las empresas de seguridad privada deben ser innovadoras, flexibles y ágiles para adaptarse a nuevos escenarios y riesgos a los que deben hacer frente.

Los pilares del servicio, detalló, deben ser la inteligencia, las personas, la tecnología y los procedimientos. La suma de estos cuatro pilares es la calidad.

Las empresas de seguridad privada de nuestras asociaciones están comprometidas con la Seguridad Privada y con la Seguridad de la Sociedad.

**Eduardo Cobas,** por su parte, se centró en el enfoque de los proveedores de servicios y las propuestas e iniciativas de Aproser. Explicó la lógica del cambio normativo (mayores exigencias, mayor legitimidad, nuevas competencias, mayor contribución a la seguridad pública) y de la necesidad de un desarrollo reglamentario del artículo 19.4 *("para la contratación de servicios de seguridad privada en los sectores estratégicos definidos en la legislación de protección de infraestructuras críticas, las empresas de seguridad privada deberán contar, con carácter previo a su prestación, con una certificación emitida por una entidad de certificación acreditada que garantice, como mínimo, el cumplimiento de la normativa administrativa, laboral, de Seguridad Social y tributaria que les sea de aplicación)* "en serio y en condiciones". La certificación, advirtió, no puede convertirse en una carga burocrática.

Hay que adoptar iniciativas, como el sistema profesional y deontológico de APROSER. E impulsar iniciativas, desde la normativa europea y los comités de normalización, como el 439 de servicios de seguridad privada.

**Ana Marzo** habló sobre el impacto del Reglamento de Protección de Datos a la videovigilancia para la protección de infraestructuras críticas. Pidió mayor colaboración con la seguridad privada en las Infraestructuras Críticas, así como en la ciberseguridad.

En su opinión es necesario regular la vídeo vigilancia a través de normativas sectoriales. Austria y Bélgica, por ejemplo, explicó, tienen una Ley de Protección de Datos local, que complementa al Reglamento de Protección de Datos Europeo.

En España este aspecto debería regularse en el Reglamento de Seguridad Privada, para recoger aspectos como el tiempo en que deben quedar guardados los datos, la no obligación de guardarlos bloqueados, cómo tratar los datos de vídeo vigilancia de los trabajadores de las infraestructuras críticas, ya que pueden dar problemas dentro de estas por una mala situación laboral, o cómo regular el sistema de entrada de la huella dactilar ya que necesita el consentimiento expreso del individuo salvo excepciones.

**Pedro Galindo** del CITRAM, explicó el papel del CECON en las Infraestructuras Críticas, ya que desde dicho centro se controla todo el Consorcio Regional de Transportes de Madrid con cinco millones de usuarios al día. Se coordinan más de 40 operadores públicos y privados, con una visualización de más de 20.000 cámaras y un seguimiento de más de 5.000 vehículos.

Para ello cuentan con las siguientes herramientas:

- GESTOR DE INCIDENCIAS (GEIS)
- SUPERVISOR GRÁFICO (SGRAF)
- CCTV INTERMODAL
- SISTEMA DE INFORMACIÓN AL USUARIO (SGIP)
- SISTEMA DE GESTIÓN DE INTERCAMBIADORES (SGI)
- MÓDULO DE ALERTAS TEMPRANAS (EWS)
- MOTOR DE DECISIÓN (DOE)
- MÓDULO DE DISTRIBUCIÓN DE INFORMACIÓN (MDI)
- APP "MI TRANSPORTE"

Tanto el metro como los autobuses urbanos en Madrid capital y resto de provincia, el ferrocarril suburbano de cercanías, los autobuses interurbanos, el metro ligero y los intercambiadores, tienen sus propios centros de control.

**Manuel Sánchez y Julio Pérez** fueron los encargados de explicar el "Documento de AES de recomendaciones para el diseño de instalaciones de sistemas de seguridad para la protección de infraestructuras críticas y estratégicas". Este interesante documento, que recoge un análisis de riesgo global que se realizará de forma conjunta sobre los activos de la organización, tiene en cuenta todos los riesgos, dando una visión global y gestionando los riesgos de forma conjunta (convergencia). De esta forma contempla cinco aspectos:

1. Seguridad física
2. Seguridad electrónica
3. Seguridad informática
4. Seguridad organizativa
5. Seguridad personal

Y pone de relieve la inteligencia como factor diferencial de la prevención.

El documento establece en los planes de seguridad, unas fases del proyecto, así como unas áreas de implantación de las medidas.

Según recoge la legislación, *"los Planes de Protección Específicos incluirán todas aquellas medidas que los respectivos operadores consideren necesarias en función de los análisis de riesgos realizados respecto de las amenazas, en particular, las de origen terrorista, sobre sus activos, incluyendo los sistemas de información.*

*Cada Plan de Protección Específico deberá contemplar tanto de medidas permanentes de protección, como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas o con relación a una amenaza concreta.*

*La Secretaría de Estado de Seguridad, a través del CNPIC, establecerá los contenidos mínimos de los Planes de Protección Específicos que cumplirán las directrices marcadas por sus respectivos Planes de Seguridad del Operador".*

Los sistemas de seguridad física y electrónica que se recogen en el documento son:

- Sistemas de detección de intrusión
- Sistemas de vídeo vigilancia
- Sistemas de control de accesos
- Sistemas de megafonía
- Sistemas de seguridad física

Además, se determinan unas áreas de implantación de los sistemas y unas matrices para su implantación. El documento, que se está rematando en la actualidad, estará pronto disponible en la web de AES.

**Antonio Pérez, presidente de AES,** fue el encargado de cerrar la jornada emplazando a los asistentes a una nueva en el FORO SICUR de 2020, organizada asimismo por AES y APROSER.