Asociación Española de empresas de Seguridad

Dinamizando la Industria de la Seguridad

Boletín Informativo

Número 69 - Abril 2019

Carta del Presidente

Estimados asociados:

Pasado ya el primer trimestre de este año 2019, me dirijo a vosotros para informaros de los objetivos de la Junta Directiva para los próximos meses:

1. Cumplimiento del presupuesto eso sí, sin dejar de crecer como Asociación y en objetivos
2. Mantener la representatividad de AES en la industria con la aspiración de expandir nuestra presencia en los sectores de nuevas tecnologías y sus muy amplias áreas de desarrollo ligadas a la seguridad
3. Organización de eventos para impulsar nuestra industria. Jornadas para asociados y para captación de nuevos asociados. La primera de ellas se prevé para el mes de junio.
4. Difusión del Manifiesto AES de protección de datos asociado a la vídeo vigilancia
5. Generación del Manifiesto 2020 / 2030. Sucesor del ya conocido y ampliamente difundido Manifiesto 2016-2019
6. Representación internacional: Euralarm y Eurosafe. Además de la participación de nuestros expertos en los Grupos de Trabajo del CEN- CENELEC para el desarrollo de normas de seguridad.
7. Colaboración con otras Asociaciones de la Industria
8. Información / acción sobre el Reglamento: estado de situación.
9. Reuniones periódicas de las áreas de trabajo y comunicación de sus estudios y avances a los asociados.
10. Organización Asambleas del CTN 108/SC79
11. Plan 100 @ 2020. Expansión de AES: nuevos asociados y nuevas áreas de trabajo y desarrollo de la seguridad
12. SICUR y Security Forum: Comenzar a preparar la edición 2020 de SICUR. La presidencia del Comité Organizador recae esta edición sobre AES.
13. El Instituto de Cualificaciones Profesionales, INCUAL, ha solicitado de AES información sobre las cualificaciones que afectan a nuestra industria. Se ha formado un grupo de trabajo a este fin.

Por otro lado, os informo de la celebración del XVI Encuentro entre Seguridad Pública y Seguridad Privada que tendrá lugar el 24 de abril.

Asimismo, le damos la bienvenida a la Asociación a los tres nuevos asociados que hemos tenido desde principios de año, las empresas CS Consultoría, EurotechZam y Microsegur. Seguimos sumando.

Antonio Pérez Turró
Presidente de AES

Boletín Informativo de AES
Revista Trimestral - Abril 2019 - núm. 69

Edita:
Asociación Española de Empresas de Seguridad
C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225 - Fax 915 766 094
www.aesseguridad.es - aes@aesseguridad.es

Consejo de Redacción:
Antonio Escamilla Recio
Julio Pérez Carreño
Antonio Pérez Turró
Manuel Porras Borrajo
Manuel Rodríguez-Reguero
Javier Ruiz Gil
Manuel Sánchez Gómez-Merelo
Óscar Tellez Carbajo
Iñigo Ugalde Blanco

Coordina:
Paloma Velasco Merino

Diseño, Maquetación y Realización:
ERRE comunicación
www.erre-comunicacion.es

La presidencia del Comité Organizador de SICUR, recae esta edición sobre AES.

Los tres ingredientes del estado de hipervigilancia chino: reconocimiento facial, videovigilancia y crédito social

Publicado en eldiario.es
27 de Marzo de 2019

Más aparcamientos y mayor videovigilancia para el próximo MotoGP en Jerez

Publicado en lavozdelsur.es
15 de Abril de 2019

Los sistemas de seguridad de viviendas en España funcionan al 18% de su capacidad

Publicado en Estrella Digital
17 de Abril de 2019

El mal funcionamiento de las alarmas de Notre Dame impidió reaccionar a tiempo

Publicado en ABC
18 de Abril de 2019

Las iglesias se blindan con alarmas

Publicado en La Voz de Galicia
20 de Abril de 2019

Los taxistas solicitan cámaras de seguridad en sus vehículos

Publicado en eldia.es
23 de Abril de 2019

El 80% de las compañías estadounidenses espera una brecha crítica a lo largo del año

"Las empresas corren un riesgo elevado de sufrir un ciberataque porque los datos críticos, las operaciones, la infraestructura y el capital humano no están bien priorizados y protegidos", aseguran desde Trend Micro.

Publicado en COMPUTERWORLD
24 de Abril de 2019

Benalmádena impulsa la instalación de videovigilancia en las vías más turísticas

Publicado en La Opinión de Málaga
24 de Abril de 2019

AES celebra su XIV Encuentro con Seguridad Pública

El pasado 24 de abril tuvo lugar en Madrid la decimocuarta edición del Encuentro de AES con los representantes de las Fuerzas y Cuerpos de Seguridad, en el que, en un ambiente de trabajo distendido y amigable, los representantes de la UCSP, SEPROSE, ICAE, ERTAINTZA Y MOSSOS, seguidos de los coordinadores de las áreas de trabajo de AES, explicaron sus líneas de actuación y objetivos para 2019.

En primer lugar, intervino el Comisario Jefe de la UCSP, Sr. Yanguas, que explicó la reestructuración de su Unidad que cuenta en la actualidad con un total de 439 efectivos, de los cuales 300 se encuentran en las Unidades Territoriales y 139 en la Unidad Central. Se dedican a tres labores fundamentales: colaboración, inspección y tribunales y acreditaciones.

Hay un nuevo plan integral de coordinación con Seguridad Privada, bajo el lema “alianza de seguridades”, integrado por COLABORA, que se encarga de la cooperación policial, la formación y las relaciones institucionales, y RED AZUL, que gestiona, opera, informa y vigila.

Especial mención dentro de COLABORA, merece el Interlocutor Policial Sanitario, figura nueva que trabaja con la colaboración directa de los Directores de Seguridad de Centros Hospitalarios, frente a las agresiones que se producen en estos centros. Además, se hacen jornadas formativas para personal sanitario y para vigilantes de seguridad que trabajan en centros hospitalarios.

Dentro de la actividad de inspección, y el plan nacional de inspección 2018/2019, se están inspeccionando instalaciones nucleares y radiactivas.

Por último, también explicó el Comisario Yanguas, las jornadas que se están haciendo tanto nacionales, como internacionales, para dar a conocer nuestro modelo de seguridad privada a países de nuestro entorno y de Latinoamérica, a petición de estos.

Por su lado, Carles Castellano intervino para explicar las actividades de la Unidad de Seguridad Privada de Mossos, que se está centrando en la lucha contra el intrusismo, la colaboración y coordinación, la formación de vigilantes de seguridad en entornos de ocio para la lucha contra la violencia en estos entornos (salas de fiesta y discotecas).

Sobre la actividad de las CRA´s en Cataluña, aseguró sentirse satisfecho con el resultado. Ha habido algunas quejas sobre que no se atienden las alarmas, aunque, según comentó, esto se debe a que, cumpliendo el protocolo que tienen establecido para los avisos, si no reúnen alguno de los requisitos establecidos, consideran que no es un aviso real y por eso se produce este hecho. Solicitó de la Asociación que les informemos de los casos concretos donde estos hechos se han producido.

Sobre la adecuación al grado 3 que se marcaba en la Orden Ministerial 316 de 10 años y que finalizaría el 18 de agosto de 2021, el 18 de abril de 2019 emitieron una nota informativa que se ha enviado por correo electrónico a asociaciones y empresas.

El presidente de AES agradeció la mención honorífica que se ha concedido a AES recientemente desde la Generalitat.

El Coronel Sánchez Corbí, responsable del SEPROSE, se presentó a los que no lo conocían, ya que ha llegado nuevo al cargo en febrero de este año. Anteriormente ha trabajado en la lucha antiterrorista y en la UCO. En el tiempo que lleva tiene una visión positiva del sector al que espera poder aportar personalmente. Cree que la Policía Nacional está haciendo una buena labor y espera tener una buena colaboración. Lamentó no tener tantos efectivos como la Policía. Comentó que el programa COOPERA, que era solamente para empresas, se ha abierto a particulares y asociaciones, ya que quiere que sea un programa transparente y es de la opinión de que el intercambio de información nos beneficia a todos. Por último, manifestó su voluntad de la industria tuviera las puertas del SEPROSE abiertas.

El Coronel Caballero Fernández, responsable de la ICAE, explicó que el SEPROSE y la ICAE se encuentran incardinados en la misma Dirección General y ahora mismo están incluso en el mismo edificio, el de Batalla del Salado, y explicó las dificultades que se encuentra la Guardia Civil en le ámbito rural por la que se hace muy necesaria la colaboración con la Seguridad Privada especialmente en este medio (pocos efectivos, robos de ganado, dificultad de la Guardia Civil de llegar a donde se cometen actos delictivos…). Asimismo, agradeció la colaboración con la Policía Nacional.

Por último, Francisco Llaneza, de la Ertzaintza, explicó que se están dedicando a la implementación de la sede electrónica en la Seguridad Privada en el País Vasco, ya que vamos un poco tarde. Están trabajando en el proyecto de página web. También tienen 24 instalaciones radiactivas a las que tienen que inspeccionar y con respecto a las alarmas, reciben unas 8 o 9 mil al año y el tiempo medio de llegada de las patrullas es de 7 minutos.

Foto cedida por Cuadernos de Seguridad

A continuación, los coordinadores de las áreas de trabajo de AES, comentaron las actividades de sus áreas:

- Iñigo Ugalde, de la de Seguridad Física (alegaciones al reglamento, norma española sobre vida útil, aplicable a las puertas de seguridad).

- Manuel Sánchez, de la de Ingeniería e Instalación (análisis de nuevas tecnologías y mercados activos, coordinación con otras áreas de trabajo de la Asociación, apoyo a nuevos proyectos y novedades, recomendaciones a los planes de protección específicos).

- Manuel Rodríguez-Reguero, de la de ciberseguridad (manifiesto recién publicado, trabajo actual dividido en tres etapas definiendo amenazas, estableciendo medidas de protección y gestión y determinando mecanismos para dar respuesta a ciber incidentes).

- Óscar Téllez, área de seguridad electrónica (denuncias contra el intrusismo en CCTV y control de accesos, aclaraciones en materia de subcontratación de PCI y elaboración de una guía conjunta de instalación de CCTV).

- Paloma Velasco, en ausencia del coordinador Manuel Porras, sobre el área de CRA (seguimiento del programa SÉNECA, protocolo de recepción de alarmas de incendio, reuniones con el Ayuntamiento sobre la APR Madrid Central y seguimiento de problemas por regiones o localidades de los asociados en la atención a las alarmas).

El encuentro finalizó con un almuerzo, como ya es tradicional.

La Junta Directiva agradece desde estas páginas la disposición de todos los miembros de las Fuerzas y Cuerpos de Seguridad en asistir a este encuentro anual.

Fuente AES

Objetivos de las Fuerzas y Cuerpos de Seguridad del Estado

POLICIA NACIONAL

Objetivos:

Incrementar presencia en el sector
Calidad de la formación
Más inspecciones y menos sanciones

MOSSOS

Objetivos:

Incremento de colaboración con el sector
Prevención e información contra terrorismo

GUARDIA CIVIL

Objetivos:

Incremento de su presencia en Comandancias. Descentralización
Ampliación nuevo programa COOPERA
Mayor presencia en la Seguridad Privada
Incremento de la colaboración y coordinación

El Potluck Forum habla sobre la “España Fractal” en su encuentro de abril.

El 25 de abril tuvo lugar el encuentro de primavera del Potluck Forum, en el que se habló y debatió sobre la “España Fractal”.

Es una realidad que cada vez más parte del territorio español se está quedando deshabitado y las personas que continúan habitando en él se encuentran más desasistidos y con menos servicios.

En este marco, Concha Jiménez, Directora General de Efectivo y Sucursales del Banco de España, hizo una brillante exposición sobre el cierre de oficinas bancarias y el acceso al efectivo en España. Explicó que en el período de 2008 a 2018 en España, hay 10.000 cajeros automáticos menos (un 17% menos) y 19.944 oficinas bancarias menos (un 44% menos), debido a la crisis, que hizo que se produjeran fusiones, ajustes de capacidad y reducción de costes, así como racionalización de la red y mejora de la eficiencia. En este contexto, existen en la actualidad en España 4.196 municipios (el 52%) que no tienen oficinas bancarias. La Comunidad Autónoma más afectada es Castilla y León, que tiene 1.700 municipios sin oficinas bancarias. Tampoco tienen otros servicios, claro está, como médicos o farmacias. Por ello hay un millón y medio de españoles afectados. Aún así, creen que no hay riesgo de exclusión financiera por el uso de la banca on line, pero la población en riesgo son las personas de avanzada edad que habitan en medios rurales. Por otro lado, no hay cobertura de internet suficiente.

Ante esta situación, se ofrecen unos canales alternativos de acceso al efectivo:

1) Oficinas móviles
2) Desplazamiento de agentes financieros
3) Cajeros automáticos desplazados
4) Cajeros multiuso
5) Oficinas de correos
6) Servicios de cash back (en gasolineras y grandes almacenes)
7) Compañías de transporte de fondos.

Con estos canales se han reducido a 3.400 municipios los que no tienen ningún servicio financiero y a un millón de habitantes afectados (2,1%).

Gonzalo Suárez y José Carlos Díez (economista y profesor en la UAH), entablaron un diálogo sobre la España en la era de la tecnología global. A juicio de José Carlos, España es un país solidario en el que la institución familiar funciona. Gracias a eso hemos salido de una de las crisis más graves de la historia. Es cierto que el problema de la despoblación existe, sin embargo, en nuestro país tenemos que “sacar pecho” por muchas cosas. Somos el tercer país mundial en extensión con mejor cobertura de fibra óptica. En Silicon Valley contratan a nuestros jóvenes y tenemos empresarios de fama mundial, como Amancio Ortega. Necesitamos a más como él.

En la mesa redonda en la que participaron Andrés Calvo (coordinador de la unidad de Evaluación y Estudios Tecnológicos de la AEPD), Antonio León (Presidente de Caja Rural de Granada) y Juan Antonio Puigserver (Secretario General Técnico del Ministerio del Interior), además de Concha Jiménez, José Carlos Díez y Gonzalo Suárez, se pidió a la Administración flexibilidad al legislar para que las empresas de seguridad puedan prestar sus servicios en ámbitos rurales en los que se están quedando sin ellos, y se preguntó por varios asuntos al representante de la Agencia Española de Protección de Datos.

La jornada fue de un gran interés y puso de manifiesto que, si bien es cierto que el riesgo de despoblación existe, también lo es que se están buscando y encontrando soluciones para que los habitantes de estos entornos rurales no carezcan de servicios que deben tener como el resto de los habitantes de nuestro país.

Fuente AES

La Dirección de Seguridad en la Era de la incertidumbre e inseguridades

Estamos viviendo una época de incertidumbre política, económica y social principalmente por falta de transparencia, corruptas o indefinidas voluntades políticas y crisis global debido a la obsolescencia de viejos paradigmas de gestión y funcionamiento que afectan a países e instituciones, en general, y a los ciudadanos, en particular.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Siempre hay miedo a lo desconocido, e incluso en algunos ámbitos se piensa que estamos en tiempos de pérdida de libertad, si no en el sentido legal, sí en el psicológico y emocional, por falta de confianza en el sistema político, económico y social que, en gran medida, es consecuencia de la asimétrica globalización que vivimos.

Llevado al ámbito de la seguridad institucional y corporativa, hace falta destacar que cada organización y actividad presenta y demanda sus propios requisitos de seguridad, su propia forma de evaluar y gestionar el riesgo.

Actualmente los entornos se han vuelto mucho más complejos, sus circunstancias requieren de una mayor personalización y, por tanto, las soluciones de seguridad deben adaptarse o dimensionarse en consecuencia.

Las soluciones actuales ante riesgos, seguridad y cumplimiento están fragmentadas y, en cierta medida, adolecen de la necesaria visión holística que tanto demandamos pero poco cumplimos en nuestras organizaciones de seguridad y por sus responsables.

Reinvención y cambios de paradigma en seguridad

Estamos en momentos de oportunidad ante sectores como la seguridad pública y la seguridad privada, con avances importantes en las últimas décadas, que presentan resultados una madurez suficiente como para consolidar y aplicar nuevos modelos de seguridad humana.

En este sentido, hemos de comunicar mejor los riesgos y las seguridades, objetivas y subjetivas, responsabilizándose todas las partes implicadas, públicas y privadas, en garantizar la seguridad demandada que por derecho corresponde.

Hemos de mejorar la seguridad “en todos los ámbitos” y, especialmente, en aquellos en los que se basa el mantenimiento de la paz y la seguridad ciudadana, donde destacan, especialmente, todas las infraestructuras estratégicas y de funcionamiento considerado crítico del país.

Riesgos, amenazas y vulnerabilidades son la base de estudio y evaluación permanente del sistema que ha de garantizar la seguridad desde un punto de vista inicialmente preventivo.

Con la identificación, análisis y evaluación de los riesgos en cada caso y circunstancias podremos crear un perfil de seguridad objetivo, así como la priorización del listado de potenciales incidencias y la realización de un plan de acción estratégico y operativo o, lo que es lo mismo, un Plan Director de Seguridad y un Sistema de Gestión de la Seguridad de la Información teniendo en cuenta, además, las tendencias de las amenazas globales y locales, es decir, insistiendo en que hemos de pensar en global pero actuar en local.

En este sentido, no sólo hemos de cumplir con las regulaciones existentes, normas internacionales de prevención y protección para garantizar la seguridad y privacidad, sino que, sobre la base de experiencia y madurez conseguida, hemos de reinventarnos, aplicando y mejorando nuestros modelos de éxito y teniendo que, en actualidad, el enfoque estratégico se ha vuelto mucho más importante.

Por eso hemos de desarrollar planes estratégicos alineados con la misión de cada organización, subrayando la función de la seguridad dentro de todo el esquema de actividad con una permanente orientación global, no solo hacia la prevención y la protección sino hacia cumplimiento del esquema más básico de seguimiento, detección, respuesta y resolución de potenciales incidencias.

Es evidente e irreversible la necesidad de evolucionar en el rol de los responsables de la seguridad, del CISO y de CSO, hacia una posición global más estratégica y centrada en la continuidad del negocio o actividad.

Hemos de acelerar el paso desde nuestra condición de expertos en operaciones o tecnología a tener que entender realmente el negocio o actividad de cada organización.

Para ello, entre otras cosas, utilizaremos las tecnologías emergentes cada vez con mayor capacidad de gestión integral del riesgo y la seguridad para una perfecta adaptabilidad y personalización para cada entidad.

Disponemos de un mercado de sistemas de seguridad con múltiples herramientas, configuraciones, plataformas operacionales y diferentes programas para priorizar activos críticos y estratégicos, seleccionando las tecnologías, lanzar sus aplicaciones y evaluaciones e informar sobre los resultados como modelos de éxito.

Finalmente, todo el esquema y sus nuevos procesos no serán posibles sin un planteamiento de inteligencia preventiva que se fundamente de manera irreversible en esa integración real de la seguridad física y la seguridad lógica, y en esa redefinición del Director de Seguridad (CISO y CSO), lo que requiere nuevos planteamientos de formación y capacitación.

II Congreso AEINSE de Ingeniería de Seguridad

Una labor fundamental

Aunque no gozan de la misma visibilidad que otros profesionales, los ingenieros son esenciales para el sector de la seguridad. Así quedó de manifiesto en el congreso organizado por la Asociación Española de Ingenieros de Seguridad (AEINSE) y *Seguritecnia* en la sede madrileña del COEM, una jornada que permitió abordar desde la aplicación de la inteligencia artificial a los sistemas de seguridad hasta cómo serán las soluciones de videovigilancia dentro de unos años.

Por Bernardo Valadés y Juanjo S. Arenas

Divulgar y ayudar a entender la tecnología entre los actores de las seguridades pública y privada. Así de rotundo se mostró **Alfonso Bilbao**, presidente de la Asociación Española de Ingenieros de Seguridad (AEINSE), al referirse al objetivo principal del II Congreso AEINSE de Ingeniería y Seguridad.

En su alocución de bienvenida a los asistentes, el director de Desarrollo de Negocio de Inerco Security reivindicó el papel de la tecnología en el ámbito de la seguridad. Y también la de los ingenieros encargados de interpretarla y generarla, cuya labor ética juzgó "fundamental" y propia de ser tenida en cuenta en la regulación de la seguridad privada "aunque dicho perfil profesional no sea considerado personal de seguridad", observó.

En sintonía con Bilbao, **Ana Borredá**, directora de *Seguritecnia*, puso en valor el colectivo de los ingenieros de seguridad como parte "importantísima" del presente y el futuro del sector. Y destacó que es igualmente relevante que el mismo cuente con "una asociación fuerte y solvente" que contribuya a materializar los objetivos expuestos por su presidente.

Inteligencia artificial

Tras la apertura formal del congreso, **Jordi Alonso**, responsable de la división de CCTV de Casmar, inició la primera sesión de ponencias ocupándose de una de las tecnologías disruptivas que más importancia tiene en la seguridad actualmente: la inteligencia artificial.

A modo de introducción, diferenció entre los conceptos *machine learning* y *deep learning*. En el caso del primero, "se trata de un método de análisis de información que requiere el uso de expertos y es propenso a errores", detalló, mientras que el segundo "aprende de los datos, es fácil de ampliar y se muestra más rápido con el empleo de unidades de procesamiento gráfico (GPU)".

Centrándose en el *deep learning*, también denominado aprendizaje profundo, y su aplicación a la seguridad, Alonso explicó que se está empleando en la protección perimetral, en los sistemas de lectura de matrículas, de detección automática de incidencias y de reconocimiento facial y en los drones. Y después de exponer algunas de las ventajas que supone su empleo, señaló que contribuye a que los sistemas de seguridad sean más fiables. "Con esta tecnología disminuyen drásticamente los falsos positivos, es posible trabajar en entornos más complejos y las configuraciones son más sencillas", resumió.

Seguridad perimetral

Quien también hizo referencia a la seguridad perimetral fue **José Manuel Alcázar**, director adjunto de Magal S3. Concretamente, una vez descrito el funcionamiento de un perímetro a través de sensores y zonas limitadas que generan alarmas, hizo una comparación entre los sistemas tradicionales y los modernos.

En lo relativo a los primeros, advirtió que un fallo de instalación o fenómenos naturales como el viento pueden ser causantes de falsas alarmas. Y de cara a evitar situaciones de "auténtico desastre" para el operador, dio a conocer las soluciones de Magal S3. "Hemos creado sistemas perimetrales modernos duplicando el patrón del cable sensor y monitorizando cada metro de este último. La tecnología nos permite crear zonas virtuales y ajustar la sensibilidad deseada en cada una de ellas, puede integrarse con plataformas de gestión y vídeo, es inmune al corte y reduce las falsas alarmas en un 90 por ciento", indicó.

"Unas ventajas", prosiguió, "a las que se deben sumar un menor tiempo de instalación, configuración y mantenimiento, la reducción de los costes en materia de componentes, fabricación, infraestructura y obras, el empleo de *software* que sustituye a los equipos de calibrado analógicos y la integración con sistemas de gestión de vídeo", concluyó.

Intercomunicación

Seguidamente, **Marta Cerezo**, gerente nacional de Commend, invitó a los presentes a reflexionar sobre la necesidad de añadir la intercomunicación a los edificios de seguridad avanzada. "Con la imagen solo tenemos una parte de la información de la escena. Entonces, ¿por qué no le sumamos el audio?", se preguntó.

Al respecto, la ponente manifestó que las normas IEC 62820, ratificadas por Aenor en marzo del año pasado, son las encargadas de establecer los requerimientos y guías de aplicación de los denominados sistemas de intercomunicación de seguridad avanzada (ASBIS, por sus siglas en inglés). "Y esas normas contemplan, además, un procedimiento de consultoría en el que se evalúan los riesgos y sus grados y se definen los elementos opcionales adicionales, así como los procedimientos operacionales y de respuesta a incidentes", esclareció.

Este último es uno de los beneficios que aportan dichas normas junto a la mejora efectiva de la seguridad operativa del día a día, la ampliación de competencias del ingeniero de seguridad a la hora de desarrollar proyectos y una percepción de que lo invertido no es un gasto. "Si tuviéramos que definir qué son los ASBIS, está claro que nos estamos refiriendo a sistemas de comunicación que salvan vidas y son claves en situaciones de emergencia", enfatizó.

Convergencia IP

"El presente y el futuro es la seguridad integral y basada en IP". Así comenzó su intervención **Bruno Azula**, *Key Account Manager* de Axis Communications, centrada en la convergencia. "El futuro es la convergencia a IP de todos los dispositivos que dan servicio a la seguridad. Pero no solo hablamos de videovigilancia, sino también de telefonía, control de accesos, intrusión, etc. Todo lo que gira alrededor de la seguridad va en esta dirección, lo que nos va a permitir ofrecer muchos más servicios", completó. "Además, todos estos elementos estarán interconectados entre sí y podrán interactuar entre ellos", explicó el profesional.
En este contexto también tiene una gran importancia la convergencia de las seguridades física y lógica debido a que las amenazas son cada vez más ciber, además de la convergencia relacionada con los usos. En concreto, esta se basa en que los sistemas de seguridad, como por ejemplo las cámaras, ya no solamente se centran en la seguridad propiamente dicha, sino que estos sistemas también pueden ayudar a gestionar tanto los clientes como el personal, además de optimizar procesos y conseguir una eficiencia operacional.

Convergencia de amenazas

La convergencia de las amenazas y de las medidas de seguridad fue la protagonista de la ponencia de **Manuel Carpio**, *Cybersecurity Senior Advisor* de Inerco Security. Para ello, comenzó contextualizando el panorama en el que se desenvuelven las compañías: "las amenazas cambian, los malos convergen y nosotros, a ser posible, tenemos que ir a su par o un paso por delante. Además, como las amenazas son holísticas, los malos buscan nuestro punto más débil, por lo que debemos comportarnos de manera integral", inició su ponencia.
Carpio realizó también un breve repaso de ciberataques como WannaCry, Stuxnet, Mirai o Shodan. "¿Qué podemos hacer para protegernos contra este tipo de amenazas ciberfísicas, en las que no hay clara una separación entre el mundo físico y el lógico? Lo primero, llevar a cabo una gestión global de inteligencia en seguridad", aseguró. "En Inerco desarrollamos esta idea a través de varios sistemas que hoy en día no están juntos. Se trata de sumar sistemas de inteligencia en Internet, sistemas PSIM (P*hysical Security Information Management*) y sistemas de control industrial para generar un *Big Data* con el que detectemos falsos positivos y, lo más importante, se generen sistemas de alerta. Sin embargo, habría que tener también un plan de continuidad de negocio por si todo falla", finalizó su intervención.

Gestión operativa

El control electrónico de acceso como herramienta de gestión operativa fue el tema presentado por Locken durante el Congreso. En concreto, **Carlos Fernández**, director de Desarrollo de Negocio de la Región Mediterráneo de la compañía, realizó una introducción destacando que, de todas las disciplinas de seguridad del mercado, "el control de accesos es el de mayor impacto en las empresas y sus trabajadores". "El desafío para las organizaciones de seguridad es cambiar el paradigma, ya que no se trata de mantener a los malos fuera y de proteger al máximo nivel las instalaciones, sino que también tenemos que proporcionar y explotar los datos y rentabilizar las instalaciones", continuó.
A continuación, con el objetivo de presentar la solución de Locken, **Laura García**, *Product Manager* de la firma, trató las características de su *hardware*. "Nuestro *hardware* está adaptado a todo tipo de soluciones y tiene dos pilares: fiabilidad y movilidad", citó entre otras características.
Por su parte, **Diego Chicot**, *IT Manager* de Locken, se encargó de la parte *software*, de la que destacó su evolución gracias al *feedback* obtenido por parte de sus clientes. Además, explicó que el *software* tiene un triple objetivo: la automatización, la integración y la personalización.

> ***A través del congreso de AEINSE se pretende divulgar y ayudar a entender la tecnología entre los diferentes actores de la seguridad***

Microservicios PaaS

Tras el *coffee break*, **Óscar Sanz**, director del Departamento Electrónico de Desico, se ocupó de la migración a la nube en el sector de la seguridad, no sin antes explicar lo que consideró "un lugar muy abstracto al que van a parar las cosas". "La nube es una red mundial de servidores, cada uno con una función única, diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenidos o servicios", detalló.

En cuanto a las estrategias de migración a la nube, se refirió a las ventajas y limitaciones de los conceptos SaaS (*Software* como servicio), IaaS (Infraestructura como servicio) y PaaS (Plataforma como servicio), menos conocido y que facilita implementar aplicaciones mediante microservicios. "PaaS obliga a replantear una aplicación desde cero, pero aporta beneficios como una gran capacidad de escalado y concurrencia, el desacoplamiento de las funciones, la tolerancia a los fallos y un coste limitado a la utilización de recursos", precisó.

Sanz finalizó destacando que los microservicios basados en PaaS mejoran el modelo de IaaS eliminando las tareas de mantenimiento, los costes de licenciamiento y las limitaciones de escalado horizontal, así como pagando por ciclos de CPU efectivos. Y como ejemplo mostró un sistema de control de accesos soportado sobre dicho concepto.

Valor añadido

Por lo que respecta a **Alberto Ruano**, director de Comunicación de FF Videosistemas, se centró en una de las líneas de negocio de la compañía, denominada Value Imaging, para demostrar cómo se puede aportar valor añadido más allá de las soluciones tradicionales de videovigilancia.

Para que ello sea así, la oferta de la empresa se articula en torno al equipo de gestión de vídeo G-Core, la analítica de vídeo con inteligencia artificial y la aplicación Briefcam. "Implementada mediante la plataforma G-SIM y *hardware* con conexión inalámbrica de alta capacidad 5G, el resultado es una analítica inteligente que facilita prevenir, analizar y dar respuesta. Y que tiene numerosas aplicaciones en el mundo real, desde la corrección de la pérdida desconocida hasta las ciudades inteligentes y seguras, pasando por los estudios de mercado o la optimización del tráfico", expresó.

Para concluir, Ruano resaltó que este tipo de avances deben dar cobertura tanto a los departamentos de seguridad como al conjunto de una organización. Y también juzgó "esencial" el empleo de la inteligencia artificial y la correcta elección de los proveedores. "Lo más importante no es contar con las mejores herramientas, sino con el conocimiento adecuado para desarrollar las soluciones más óptimas", estimó.

Seguridad 6.0

Y antes de participar en la mesa redonda dedicada al futuro del mercado de CCTV, **Gerardo Estalrich**, director de Desarrollo de Negocios de Bosch, compartió unas reflexiones relativas a los sistemas de seguridad, condicionados hoy en día por el Internet de las Cosas (IoT, por sus siglas en inglés). "Estamos en el estadio de la seguridad 6.0 y el IoT implica gestionar millones de datos, que han de ser seguros, fiables y accesibles", reparó.

Con el objetivo de garantizar la seguridad de los datos, el ponente explicó que los productos de Bosch cuentan con certificaciones digitales, encriptaciones, contraseñas y gestiones de usuarios, etc. Asimismo, la compañía trabaja en la fiabilidad de la analítica de vídeo a través de algoritmos "para que la información que nos llegue sea real" y también en la accesibilidad de los datos con soluciones como la doble grabación directa a red (iSCSI). "Y para que la información esté disponible, tenemos un programa específico para integradores y desarrolladores, así como herramientas SDK con ejemplos de código y SQL para metadatos", manifestó.
Por último, Estalrich indicó que Bosch colabora activamente con la industria de la seguridad a través de la plataforma sin ánimo de lucro Open Security & Safety Alliance.

Mesa redonda "El CCTV en 2025"

Inteligencia, nube y datos: el futuro de la videovigilancia

Para concluir el II Congreso AEINSE de Ingeniería de Seguridad se dio paso a una mesa redonda formada por **Gerardo Estalrich**, *Business Development Manager* de Bosch; **Bruno Azula**, *Key Account Manager* de Axis Communications; y **Javier Tallón**, director comercial de FF Videosistemas; bajo la moderación de **Juan José Hernández**, tesorero de AEINSE. En concreto, durante este coloquio se trató el futuro de los sistemas de vídeo, poniendo el foco de atención en el año 2025.
Para comenzar, Javier Tallón destacó tres aspectos fundamentales en este ámbito: *software*, integración y migración a la nube. "Debido al volumen de datos generado por el vídeo necesitamos un *software* que filtre, automatice y haga llegar la información de forma clara, precisa y directa para que el tiempo de respuesta sea

mínimo. Además, tenemos que dotar a los sistemas de una capa superior para garantizar se está haciendo un uso correcto de la información y evitar así posibles filtraciones", comenzó su intervención.

A ello Gerardo Estalrich le añadió que, en el futuro, las cámaras van a tener inteligencia. “La cámara va a ser un sensor, va a formar parte del mundo del Internet de las Cosas y va a tener múltiples prestaciones, siendo el futuro de los sistemas de comunicación tener *deep learning* en el propio dispositivo”, afirmó. Sin embargo, también puso el foco en las pequeñas instalaciones de seguridad: “dentro de cinco años va a haber instalaciones más pequeñas que no van a necesitar tantas prestaciones en las cámaras. Además, seguirá habiendo un mercado *low cost* de cámaras válido para este tipo de instalaciones, añadió.

Tendencias

Por su parte, para Bruno Azula las principales tendencias la videovigilancia del futuro serán la inteligencia artificial, el uso de la nube, la gestión de la privacidad y la integración de sensores, entre otras. “Todo esto puede hacer que nazcan nuevos usos, como el 5G, en el que importa la rapidez”, argumentó. Asimismo, según el representante de Axis surgirán más funcionalidades, se llevarán a cabo más analíticas, se producirá un menor consumo y se tendrá muy en cuenta el impacto medioambiental.

Pese a todo esto, para Estalrich y Tallón los sistemas de vídeo no desplazarán a los sistemas de intrusión tradicionales a corto plazo. Distinta opinión mostró Azula, quien aseguró que este hecho es una realidad en instalaciones pequeñas y medianas debido a que las cámaras son fáciles de mantener y de instalar, a lo que añadió su bajo índice de falsas alarmas.

En cuanto a los sistemas de control de accesos, la discrepancia se volvió a abrir paso en la mesa. Mientras que los representantes de Bosch y Axis afirmaron que estos no se van a ver desplazados por los sistemas de vídeo, Javier Tallón opinó lo contrario basándose en los sistemas de reconocimiento facial para sostener su opinión. “Realmente, con los controles de acceso de huella o tarjeta no se conoce cuántas personas pasan; no obstante, con el reconocimiento facial sí se puede saber”, explicó.

La nube

Además, la nube se tornó como uno de los grandes pilares a tratar en la mesa redonda debido a su importancia en el futuro de la videovigilancia, aunque para Gerardo Estalrich “el almacenamiento de vídeo va a ser complicado en la nube de aquí a cinco años”.

Pese a ello, los intervinientes mostraron su confianza en los servidores en la nube desde el punto de vista de la seguridad, pese a la actividad de los ciberdelincuentes. “La nube es fiable hasta el día en el que quien quiera entrar, entre. En ese momento tendremos que dar un paso atrás y volver a los sistemas físicos”, señaló Tallón, a lo que Azula le añadió que “da igual dónde esté la información, ya que aunque la guardemos con mil llaves alguien va a acabar entrando”.

Finalmente, Ana Borredá y Alfonso Bilbao clausuraron este Congreso agradeciendo la asistencia a todos los presentes.

Principales conclusiones del II Congreso AEINSE de Ingeniería de Seguridad

El II Congreso AEINSE de Ingeniería de Seguridad dejó varias conclusiones en torno a los diversos temas que se abordaron durante la jornada. Algunas de ellas son las siguientes:

- Desde la Asociación Española de Ingenieros de Seguridad (AEINSE) se sugirió que la labor de dicho colectivo debería ser tenida en cuenta en la regulación de la seguridad privada.
- La inteligencia artificial se ha convertido en una herramienta indispensable en los sistemas de seguridad,

ya que, gracias a sus numerosas aplicaciones, contribuye a generar información muy precisa y completa. Además, posibilita operar en entornos complejos.

- Con el objetivo de que sean más completos y brinden una mayor ayuda en situaciones de emergencia, los proyectos de seguridad deberían contemplar los sistemas de intercomunicación de seguridad avanzada (ASBIS, por sus siglas en inglés) desde el diseño.
- Al gestionar una ingente cantidad de datos, los sistemas de seguridad electrónica deben incorporar soluciones que garanticen su protección, fiabilidad, accesibilidad y disponibilidad.
- La convergencia de los dispositivos y de las seguridades física y lógica será el futuro de una seguridad cuyos elementos deben interrelacionarse entre sí.
- Los ciberdelincuentes están evolucionando constantemente, por lo que las organizaciones deben ir a su par o un paso por delante. Para ello, pueden utilizar la inteligencia como base de su estrategia.
- La inteligencia, la nube y el uso y gestión de los datos se tornarán como alguno de los elementos a tener cuenta en la videovigilancia del futuro. Además, las cámaras tendrán múltiples prestaciones no solo relacionadas con la seguridad.
- Pese al avance de la videovigilancia, esta no desplazará en el futuro ni a los sistemas de intrusión tradicionales ni a los controles de accesos, aunque no hay una opinión generalizada al respecto entre los profesionales de la seguridad.

AGENDA 2019

FERIAS Y CONGRESOS

- Expo Security Méjico. Del 7 al 9 de mayo, Ciudad de Méjico.
- SECUTECH 2019, 8 al 10 de Mayo, Taipéi, Taiwan.
- Infosecurity Méjico. 22 y 23 de mayo, Ciudad de Méjico.
- Security Forum, 28 y 29 de mayo. Barcelona.
- Organización Iberoamericana de Protección Contra Incendios - OPCI, XVII Congreso, 29, 30 y 31 de mayo de 2019, en el Centro de Convenciones de la Universidad Católica de Colombia, Bogotá.
- IFSEC, 18 al 20 de junio en Londres.
- Seguridad Expo, 27 al 29 de agosto, Santiago de Chile.
- IEEE (53rd) International Carnahan Conference on Security Technology, 1 al 3 de octubre, Anna University in Chennai, India.
- Municipalia, Lérida, 22 al 24 de octubre.
- Sicurezza, 13 al 15 de noviembre en Milán.
- EU Fire Safety Week 2019, 18 al 21 de noviembre. Bruselas.
- Preventica Dakar, 19 al 21 de noviembre, Dakar.
- Milipol París, 19 al 22 de noviembre de 2019. París. Francia
- Intersec 2020, Dubai 19. - 21.1.2020 (EAU)
- INTERSCHUTZ 2020, 15 al 20 de junio del 2020 en Hannover, Alemania.

El V Congreso Edificios Inteligentes aborda el concepto de Edificio Inteligente desde un punto de vista integral y multidisciplinar.

El programa de esta quinta edición, abarca la actualidad y el futuro del sector en diferentes formatos, como ponencias de comunicaciones, exposiciones de proyectos de edificios inteligentes, mesas redondas y ponencias magistrales.

https://www.congreso-edificiosinteligentes.es/programa/

AES, Asociación Española de Empresas de Seguridad, es socio fundador de UAS (Unión de Asociaciones de Seguridad)

Agradecemos las colaboraciones que hacen posible esta edición trimestral y animamos a nuestros lectores a que nos remitan informaciones o artículos de opinión para su publicación en el boletín. AES no se hace responsable de las opiniones vertidas en este boletín.