



Entrevista socio

Gianluca Ciuchi Davie

*Cena y Premios
ADSI
2026*

"Martes con ..."

Instituto de Medicina
Legal y Ciencias Forenses
de Cataluña

Junta Directiva

Presidente

Eduard Zamora

Vicepresidenta

Elvira Márquez

Secretario

David Sanmartín

Tesorero

Emilio Herrero

Vocales

Lourdes Castellsaguer

Francesc Chía

Joan Figuera

Isabel García

Oscar Molins

Míriam Pérez

Macarena Ramisa

Joan Roda

Jordi Silvestre

Oriol Verdura

Defensor del Socio

Miguel E. Arredonda

En este número ...

3

PATROCINADORES ADSI

4

CENA INSTITUCIONAL

5

ARTÍCULO DE OPINIÓN

- La preservación inmutable: La nueva categoría que la ciberseguridad no vio venir

7

ENTREVISTA A UN SOCIO

11

ARTÍCULO

- Entrenar el control neuromuscular
- Principales Objetivos del Robo de Tecnología por Estados Competidores: La Nueva Carrera por el Conocimiento

15

NOTICIAS ADSI

- "Martes con..." Instituto de Medicina Legal y Ciencias Forenses de Cataluña
- Vanesa Berlanga, nueva embajadora de la Marca Ejército

- COREWEAVE, nuevo patrocinador de ADSI
- ExpoProtection 2026
- ExpoSecurity 2026
- TECNOSEC dronexpo
- Jornada TAPA: protegiendo la cadena de suministro

23

ACTUALIZACIÓN DE DATOS

34

NUESTROS PATROCINADORES

- COREWEAVE
- GONBER
- MKV MEDIALAB
- ARMATURA
- IMAN SEGURIDAD
- INTERNATIONAL SOS
- SCATI
- TARGET TECNOLOGIA
- VIGI BY TP-LINK

47

FORMACIÓN

55

REVISTAS Y ENLACES DE INTERÉS

56

LECTURA RECOMENDADA

La opinión manifestada por los autores de los artículos publicados a título personal que se publican en este medio informativo no necesariamente se corresponde con la de ADSI como Asociación.

Esta comunicación se le envía a partir de los datos de contacto que nos ha facilitado. Si desea cambiar su dirección de correo electrónico dirija su petición por correo postal a "ADSI -Asociación de Directivos de Seguridad Integral", Gran Vía de Les Corts Catalanes, 373 – 385, 4ª planta, local B2, Centro Comercial "Arenas de Barcelona", 08015 -Barcelona, o mediante e-mail a vicepresidente@adsi.pro

Si o no desea recibir nuestros mensajes informativos utilice los mismos medios, haciendo constar como asunto "DAR DE BAJA". Su petición será efectiva en un máximo de diez días hábiles.



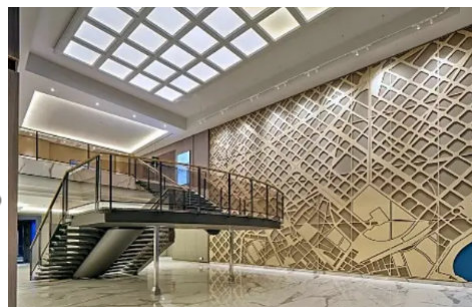
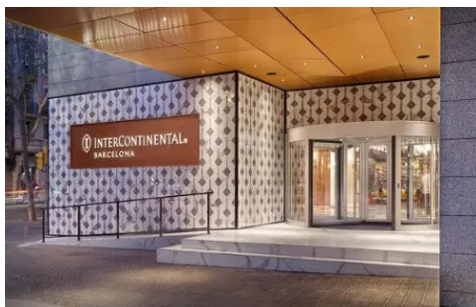
Cena Institucional y premios ADSI 2026

Jueves 15 de octubre de 2026

Hotel Intercontinental Barcelona

Avda. Rius y Taulet, 1 de Barcelona

¡¡ Inscripciones abiertas - Reserva tu plaza !!



Reserva en tu agenda la tarde del jueves 15 de octubre de 2026 para asistir a la Cena Institucional y entrega de los Premios ADSI 2026, en el Hotel Intercontinental de Barcelona.

Este año la haremos coincidir con la fecha exacta en que hace 30 años ADSI se inscribió en el Registro de Asociaciones del Ministerio del Interior y comenzó su singladura como asociación de ámbito nacional.

En esta especial celebración esperamos contar con la presencia de Socios, Patrocinadores, Autoridades y Amigos de ADSI, en el que es uno de los actos más relevantes e importantes del año, en el que se contaremos con una numerosa y muy selecta representación del sector, con unos 400 asistentes.

Ya se han abierto las inscripciones, como habrás podido ver en la nota informativa que hemos remitido al sector y que reproducimos en el siguiente enlace:

VER NOTA INFORMATIVA



La preservación inmutable: La nueva categoría que la ciberseguridad no vio venir

Por **Oriol Verdura**, Vocal de ADSI

Durante décadas, la industria de la seguridad de la información ha operado bajo una premisa casi dogmática: para proteger los activos de una organización, basta con blindar el perímetro digital. Hemos invertido fortunas en cortafuegos de última generación, arquitecturas Zero Trust, cifrado de extremo a extremo y copias de seguridad en la nube con redundancia geográfica. Sin embargo, a medida que las amenazas cibernéticas se vuelven más complejas, un riesgo estructural profundo sigue pasando desapercibido para los comités de dirección y los responsables de ciberseguridad.

Existe un error de base en la gestión de activos estratégicos: **confundimos digitalizar con preservar**. La digitalización es una solución para el presente, pero no está concebida para que prevalezca en el futuro debido a su fragilidad. Los discos duros fallan, los centros de datos consumen ingentes cantidades de energía, los formatos informáticos caducan y el software con el que hoy leemos un documento puede desaparecer en pocas décadas.

Además, en el entorno cibernético actual, las amenazas no se limitan al robo de datos; el *ransomware* masivo, la degradación silenciosa (*bit rot*) y el sabotaje informático han demostrado que cualquier sistema conectado a la red es vulnerable.

A esta fragilidad sistémica se le suma hoy la increíble disrupción de la inteligencia artificial. La IA no solo sintetiza información, sino que rompe la cadena de procedencia al entregar respuestas sin devolver al usuario a la fuente original. En un mundo donde el contenido sintético puede alterar la realidad digital, surge una pregunta crítica para directores de ciberseguridad, responsables de riesgos y custodios de la información: ¿dónde reside la prueba irrefutable de la verdad?. ¿Cómo aseguramos que los datos críticos de un

negocio, las patentes de una corporación, los archivos judiciales o el patrimonio cultural de un Estado no han sido alterados, modificados con quién sabe qué fines o borrados para siempre?.

Es en este punto donde nace una nueva categoría conceptual e industrial dentro del ecosistema de la seguridad: la **Seguridad basada en la Preservación Inmutable**.

Esta categoría no pretende competir con las soluciones de ciberseguridad activa ni sustituir el almacenamiento operativo en la nube. Se concibe como un complemento a todo ello. Representa una vuelta de tuerca al concepto clásico de conservación: un nivel extra de protección física y lógica diseñado a prueba de hackers, inmune a los ataques informáticos e independiente de las obsolescencias tecnológicas.

Hasta ahora, la seguridad de la información se ha planteado casi exclusivamente como un problema de código, algoritmos y conectividad. La Seguridad basada en la Preservación rompe esta dependencia al anclar la información en una referencia inmutable sobre un soporte óptico analógico en película fotográfica de 35 milímetros en poliéster de alta estabilidad. Esta tecnología, desarrollada e implementada en infraestructuras como el Centro Integral de Preservación Audiovisual (CIPA) en Málaga de la empresa Preservación 35 (P35), pionera en España, permite convertir cualquier activo digital —datos informáticos, código fuente, archivos audiovisuales o documentos históricos— en un máster analógico inalterable.





¿Por qué esta aproximación constituye un cambio de paradigma para la ciberseguridad global? La respuesta radica en tres pilares fundamentales que ninguna solución puramente digital puede ofrecer simultáneamente:

En primer lugar, superficie de ataque cero y aislamiento absoluto (*air-gap* real). Al convertir los paquetes de datos digitales en un soporte físico fotográfico almacenado en frío (*offline*), el activo queda totalmente desconectado de cualquier red. No existe puerto de entrada, no hay código malicioso que pueda ejecutar instrucciones sobre la película ni *ransomware* capaz de secuestrar la información. Frente a la amenaza de un ciberataque destructivo o un pulso electromagnético, el dato preservado permanece intacto e inaccesible para los atacantes.

En segundo lugar, independencia tecnológica y eliminación de la obsolescencia. Las soluciones de almacenamiento digital tradicionales obligan a realizar migraciones periódicas de datos cada pocos años, lo que genera costes desorbitados, riesgos de migración y degradación silenciosa. El máster analógico de poliéster en 35mm ofrece una vida útil verificable de hasta 500

años sin necesidad de mantenimiento activo, sin consumo energético continuo y con la garantía de ser siempre re-digitalizable en la resolución del futuro sin pérdida de calidad.

En tercer lugar, garantía de autenticidad y soberanía documental. Frente a las trampas de la inteligencia artificial y la falsificación digital, la preservación analógica actúa como el ancla de verdad inmodificable. Ante cualquier litigio legal, auditoría o intento de manipulación en la red, el máster físico se erige en la prueba definitiva contra la que contrastar el dato operativo.

Los directores de seguridad, gestores de riesgos y administraciones públicas no pueden seguir confiando la permanencia de sus activos más críticos a la misma capa digital que está bajo fuego cibernético constante. **Digitalizar produce el presente, pero solo la preservación inmutable garantiza el mañana.** Incorporar este nivel extra de seguridad a prueba de hackers no es un lujo nostálgico, sino el estándar imprescindible para proteger hoy lo que seguirá teniendo valor dentro de quinientos años. ■



Gianluca Ciuchi Davie

CEO -ID & Fraud Consultant - Int. Police ToT ARIKI y SIGMA

¿En qué campos de la seguridad se centra tu día a día y que función desempeñas?

Actualmente mi actividad se concentra en tres grandes áreas. La primera es la recuperación internacional de activos en el ámbito de la automoción, para multinacionales del sector asegurador, financiero y renting/leasing. La segunda es el desarrollo de soluciones tecnológicas aplicadas a la seguridad, especialmente destinadas a prevenir y combatir delitos como la falsedad documental que están directamente vinculados con la financiación del terrorismo, el tráfico de seres humanos y el blanqueo de capitales. Y la tercera es la formación y asesoramiento a Fuerzas y Cuerpos de Seguridad a nivel internacional, colaborando también con organismos como Naciones Unidas.

Son tres actividades diferentes, pero todas tienen un denominador común: inteligencia, tecnología y prevención.

¿Principales retos o proyectos relacionados con la seguridad en tu empresa?

Nuestro principal reto es intentar desarrollar soluciones para problemas que todavía no tienen una respuesta adecuada o que evolucionan más rápido que las herramientas disponibles para combatirlos. La inseguridad es cada vez más dinámica: cambian los métodos delictivos, la tecnología y los escenarios internacionales. Por ello, nuestro objetivo es anticiparnos, identificar nuevas vulnerabilidades y crear soluciones capaces de adaptarse rápidamente a un entorno en continua transformación.

¿Cuál es tu formación académica?

Mi formación combina estudios universitarios con una especialización posterior en seguridad empresarial. Tras establecerme en España cursé la formación superior en Dirección y Gestión de Seguridad Empresarial en la Universidad de Barcelona, que me permitió obtener posteriormente la habilitación profesional como Director y Jefe de Seguridad.

A esa formación académica se suma una parte muy importante de formación operativa y experiencia práctica

adquirida también durante toda mi trayectoria profesional.

¿Cómo accediste al mundo de la Seguridad y en qué empresas / responsabilidades has ido avanzando desde entonces?

Mi entrada en la seguridad fue eminentemente operativa.

Procedo del ámbito militar - donde serví en Italia como oficial de unidades especiales - y posteriormente de la investigación y la seguridad privada, trabajando también en apoyo de investigaciones relacionadas con crimen organizado. Mi trayectoria fue evolucionando hacia la gestión empresarial de la seguridad.

Cuando llegué a España completé mi formación como Director y Jefe de Seguridad y posteriormente tuve la oportunidad de incorporarme a Abertis, donde asumí responsabilidades relacionadas con la protección de infraestructuras, instalaciones, personal directivo, gestión de crisis y coordinación con Fuerzas y Cuerpos de Seguridad.

Más adelante decidí recuperar mi vertiente investigadora y emprendedora, creando una estructura propia que hoy opera internacionalmente en recuperación de activos, tecnología, prevención del fraude y formación policial.

En el año 1998 me incorporo en Telefónica Móviles España SAU, como responsable de proyectos de seguridad y servicios de vigilancia en Catalunya y Baleares hasta el año 2006, en el que tiene lugar la convergencia con Telefónica de España SAU, incorporándome a su Departamento de Seguridad en Barcelona, hasta la actualidad.

¿Cómo crees que ha evolucionado la Seguridad desde tus inicios hasta ahora?

Ha evolucionado enormemente, sobre todo por el impacto de la tecnología. Hace años asociábamos muchos riesgos de seguridad a amenazas principalmente físicas.



Hoy un ordenador e internet tienen seguramente una capacidad de daño muy superior a la de muchas amenazas tradicionales.

La protección de infraestructuras críticas, empresas o instituciones ya no puede limitarse a impedir una intrusión física. Un ataque tecnológico puede afectar a servicios esenciales o incluso a la estabilidad económica de un país sin necesidad de grandes capacidades materiales. Por eso, uno de los grandes retos actuales consiste en identificar vulnerabilidades que hace pocos años ni siquiera existían.

¿Cómo ves la profesión de director de seguridad en el medio/largo plazo, qué cambiarías de la misma y como crees que evolucionará?

Creo que avanzará necesariamente hacia una mayor profesionalización y especialización. La tecnología, la inteligencia (humana y artificial), la ciberseguridad y el análisis de riesgos tendrán cada vez más peso.

Pero también considero importante que la formación teórica se complemente con experiencia práctica. Mi trayectoria previa en entornos militares, investigación, seguridad privada y posteriormente seguridad corporativa me ha demostrado que los libros proporcionan herramientas fundamentales, pero no siempre enseñan a reaccionar frente a situaciones reales.

Un buen Director de Seguridad necesita conocimiento, pero también capacidad de análisis, imaginación y cierta mentalidad investigadora: ser capaz de ponerse en la posición de quien pretende vulnerar nuestro sistema para poder anticiparse a él.

¿Exigirías Departamento de Seguridad a las empresas en función del nº de empleados, nº de centros de trabajo, nº de ocupantes, de sus riesgos específicos, etc., o consideras que debe ser de libre creación en todo caso?

No creo que el criterio principal deba ser simplemente el número de empleados o de centros de trabajo. Para mí, el elemento determinante debería ser el nivel de riesgo asociado a la actividad.

Una empresa con cientos de empleados puede desarrollar una actividad relativamente poco sensible, mientras que una empresa de tres personas puede desarrollar tecnología cuya utilización indebida podría generar riesgos muy importantes.

Por eso creo que sería más lógico establecer categorías de riesgo, valorando la actividad, los activos que se protegen, la información que se maneja, las consecuencias potenciales de un incidente y su impacto sobre terceros. A partir de ahí debería determinarse qué estructura, responsable o medidas de seguridad resultan necesarias. La seguridad debería dimensionarse por el riesgo, no únicamente por el tamaño de la empresa.

¿Te parece correcto disponer de dos vías formativas tan diferenciadas para obtener la habilitación como Director de Seguridad (curso de habilitación TIP de un año, o grado universitario de 4 años) y que cambiarías?

Creo que existe una cierta desproporción entre una vía formativa de un año y otra universitaria de cuatro años para acceder a una misma habilitación. Probablemente cuatro años puedan resultar excesivos si una parte importante de esa formación no se traduce en experiencia práctica, pero un año me parece insuficiente para asumir responsabilidades que pueden ser muy relevantes, incluso desde el punto de vista penal y patrimonial.

Como ya he compartido anteriormente, creo que el concepto de "seguridad" no se pueda aprender únicamente en los libros. La formación teórica es imprescindible, pero después hay que saber aplicarla en entornos reales, y cada empresa - incluso dentro del mismo sector - presenta riesgos y necesidades diferentes. Por eso considero fundamental incorporar más experiencia práctica supervisada, trabajando junto a profesionales con experiencia antes de asumir determinadas responsabilidades.

Además, para mí hay un aspecto incluso más importante que la duración inicial de la formación: la formación continuada obligatoria. Las amenazas, la tecnología y los modelos delictivos evolucionan demasiado rápido como para considerar suficiente una titulación obtenida veinte años atrás sin ningún tipo de actualización posterior.

En otros entornos profesionales internacionales existen certificaciones que obligan a actualizar conocimientos periódicamente para poder mantenerlas. Creo que sería razonable avanzar hacia un modelo similar: una formación inicial sólida, una etapa práctica real y una actualización profesional obligatoria cada cierto número de años.



¿En la formación para ejercer como director de Seguridad, que materias o aspectos deberían potenciarse, que no se traten en profundidad ahora?

Creo que los programas formativos tienen que evolucionar prácticamente al mismo ritmo que las amenazas. No podemos mantener durante años temarios concebidos para escenarios de seguridad que ya han cambiado.

Potenciaría especialmente el análisis de nuevas amenazas, la protección de infraestructuras críticas, la inteligencia aplicada a la seguridad, el acceso a los recursos OSINT, la gestión de crisis, los movimientos migratorios descontrolados y sus implicaciones para la seguridad, la falsedad documental, la delincuencia transnacional y, naturalmente, la ciberseguridad.

Ahora bien, creo que debemos diferenciar claramente entre la responsabilidad global del Director de Seguridad y las especialidades técnicas.

Veo con cierta frecuencia ofertas para plazas de Directores de Seguridad que pretenden encontrar en una sola figura a un Director de Seguridad (titulado y con TIP), un ingeniero informático, un especialista en redes, un experto en ciberseguridad y, además, un responsable de seguridad física.

Eso, en mi opinión, demuestra una comprensión bastante equivocada de la función.

El Director de Seguridad (los que en inglés sería el Security General Manager) debe tener conocimientos suficientes para entender, coordinar y dirigir la seguridad integral de la organización, pero debe apoyarse en especialistas cuando el nivel técnico lo requiera. En una estructura madura, por ejemplo, la seguridad informática debería estar perfectamente coordinada con la seguridad corporativa, pero dirigida técnicamente por profesionales específicamente preparados para ello.

La seguridad moderna requiere precisamente eso: integración de especialidades, no acumulación artificial de profesiones en una sola persona.

¿Ventajas de integrarse en una asociación de profesionales de la seguridad?

La principal ventaja es poder compartir experiencias con profesionales que trabajan en ámbitos distintos al propio. Eso amplía la visión, permite conocer otros

enfoques y, muchas veces, encontrar soluciones a problemas que quizá uno no habría planteado de la misma manera.

Creo que una asociación no debe servir únicamente para socializar, sino sobre todo para compartir conocimiento y experiencia. Esto es útil tanto para quienes empiezan en la profesión como para quienes llevamos muchos años en ella. Siempre hay algo que aprender de otros profesionales y esa capacidad de seguir formándose es fundamental en un sector que cambia constantemente.

¿Qué te ha llevado a afiliarte a ADSI en concreto?

Me incorporé a ADSI hace aproximadamente 18 años, coincidiendo con mi etapa profesional en Abertis. Muchos de los directores de seguridad con los que trabajaba allí pertenecían a la asociación y eso me permitió conocerla desde dentro.

Desde entonces he seguido vinculado porque siempre he encontrado profesionales procedentes de ámbitos muy diferentes, cada uno con experiencias y conocimientos que aportan valor. Para mí, precisamente esa diversidad es uno de los grandes activos de ADSI: permite crecer no solamente como profesional, sino también como persona.

¿Qué debe mejorar ADSI en relación con la prestación a sus asociados?

Considero que la evolución de los últimos años ha sido muy positiva. La actual dirección ha sabido interpretar bien las necesidades de los asociados, promoviendo actividades formativas, visitas profesionales e iniciativas con contenidos de verdadero interés.

Un buen ejemplo fue la reciente visita al Instituto de Medicina Legal de Cataluña: conocer desde dentro ámbitos relacionados con nuestro trabajo siempre resulta enriquecedor. El crecimiento tanto de asociados como de patrocinadores creo que demuestra que se está trabajando en la dirección adecuada.

Si tuviera que plantear una línea adicional de mejora, apostaría por reforzar todavía más las relaciones con otras asociaciones profesionales, nacionales e internacionales. Cuando distintas organizaciones del sector comparten objetivos comunes, también aumenta su capacidad para impulsar iniciativas, defender intereses profesionales y colaborar con universidades, instituciones y administraciones



¿Cómo podría incrementarse la colaboración entre directores de seguridad de ámbitos/sectores/empresas diferentes de nuestro país?

Creo que habría que generar más espacios de intercambio práctico. No solamente jornadas o conferencias, sino foros donde profesionales de distintos sectores puedan compartir problemas reales, experiencias y soluciones.

Muchas veces una problemática que hoy aparece en una empresa energética, logística o financiera (inclusive de otro País) terminará afectando mañana a otro sector. Conocer cómo otros profesionales están afrontando esas amenazas permite anticiparse.

También sería interesante fomentar proyectos conjuntos entre asociaciones, universidades, empresas y Fuerzas y Cuerpos de Seguridad. Cuanto mayor sea la interacción entre estos mundos, mayor será nuestra capacidad de entender las amenazas y desarrollar respuestas eficaces.

En un mundo cada vez más globalizado y por tu experiencia, ¿destacarías algún país en la gestión de la seguridad y cómo mejorarías el intercambio de experiencias y conocimiento entre países?

Por mi trabajo he tenido la oportunidad de colaborar con profesionales y Fuerzas y Cuerpos de Seguridad en

numerosos países de Europa, Norte de África y Oriente Medio, y una de las conclusiones que he extraído es que nadie tiene todas las respuestas.

Más que señalar un país concreto como modelo, creo que lo verdaderamente importante es conocer lo que otros están haciendo bien y aprender de ello. Una amenaza que hoy está apareciendo en Alemania, Turquía o Letonia puede terminar afectándonos mañana en España (y viceversa).

Por eso creo que deberíamos impulsar mucho más el intercambio internacional entre directores de seguridad, asociaciones profesionales y cuerpos policiales.

Incluso me parecería muy interesante que ADSI promoviera en algún momento un foro europeo de dirección de seguridad, reuniendo a profesionales de diferentes países y a representantes de las Fuerzas y Cuerpos de Seguridad.

Hay numerosos congresos especializados, pero echo de menos un espacio europeo claramente orientado a la dirección integral de seguridad, donde podamos analizar conjuntamente la seguridad global, las nuevas amenazas y los riesgos emergentes que afectan a nuestras empresas. ■

🚴 Un hobby: Uno de mis hobbies es frecuentar el campo de práctica del golf: esta actividad me obliga a mantener la concentración y la disciplina mental, habilidades que valoro mucho y que también aplico en mi vida profesional. Me ayuda a gestionar la presión, a mantener la calma en momento decisivos y a pensar con precisión. Sin embargo, debido a mis responsabilidades profesionales y la gestión de varios negocios, no siempre puedo dedicarle todo el tiempo que me gustaría.

📖 Un libro: Encuentro inspiración en textos que moldean valores y criterio. En mi caso, la Biblia es sin lugar a duda mi referencia constante. Más allá de un mero argumento de fe, me aporta principios que aplico tanto a mi vida personal como profesional.

🎵 Una canción: Where The Streets Have No Name del grupo "U2". Habla del deseo de escapar de las etiquetas, divisiones y barreras que nos separan, buscando un lugar en el cual lo que somos importe más que de dónde venimos. Es una

búsqueda de libertad, unidad y esperanza, aunque ese lugar ideal quizás haya que buscarlo más allá de esta vida.

🏠 Un lugar para desconectar: Sin duda, la Val Badia en los Alpes del norte de Italia. Es probablemente el único lugar donde realmente no echo de menos ni el móvil ni el portátil, y para mí esa es la mejor señal de que he conseguido desconectar de verdad. Es un entorno que me permite bajar el ritmo, cambiar completamente de perspectiva y volver con las pilas cargadas.

🕒 Un momento de la historia: Me hubiera gustado vivir en una época de grandes transformaciones sociales porque me apasiona observar cómo los valores y el liderazgo inspiran cambios reales en la gente. A nivel personal me inspira analizar y entender como figuras históricas movían multitudes de personas y cómo esos principios, coherencia, ética y servicio pueden ser aplicables también hoy en mi propia vida para hacer de mí una mejor persona y un mejor profesional.



Entrenar el control neuromuscular. Equilibrio, coordinación, aterrizajes, desaceleración, cambios de dirección y estabilidad dinámica como barreras preventivas de lesiones.

Por **Francesc Sanahuja**, Coordinador SECOT- Técnico en seguridad CEPREVEN y socio de ADSI

Adjuntamos la sexta parte de la serie de artículos sobre prevención y seguridad en los deportes de naturaleza que se publicarán sucesivamente en la revista ADSI.

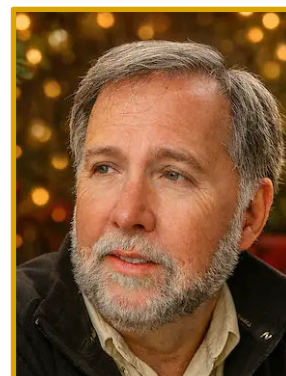
Muchas lesiones no aparecen únicamente por falta de fuerza o resistencia. Surgen cuando el deportista aterriza sin control, frena tarde, pierde estabilidad o no coordina con suficiente precisión el tronco y las extremidades. En ese momento, el problema no es solo muscular: es neuromuscular.

El control neuromuscular es la capacidad de organizar el cuerpo y responder con eficacia ante cambios rápidos. Integra equilibrio, propiocepción, coordinación, fuerza, control del tronco, desaceleración y capacidad de corregir el movimiento. Todo ello cobra especial importancia

cuando aumenta la velocidad, aparece la fatiga o el entorno se vuelve imprevisible.

La prevención no consiste en acumular ejercicios difíciles ni en trabajar siempre sobre superficies inestables. Consiste en progresar desde tareas simples y bien controladas hacia aterrizajes, frenadas, cambios de dirección y situaciones cada vez más próximas al deporte real. Primero debe dominarse el gesto; después se añade velocidad e incertidumbre.

Para clubes y entidades, la ventaja es clara: este trabajo puede integrarse en el calentamiento habitual, con poco material y sin necesidad de tecnología sofisticada. Lo decisivo es la continuidad, la calidad de ejecución y la adaptación a la edad, al nivel y a la modalidad deportiva.



IDEA CENTRAL

cuando llega el gesto crítico ya no hay tiempo para aprender; el cuerpo solo puede utilizar aquello que ha entrenado.

[ENLACE ARTÍCULO 6](#)



Principales Objetivos del Robo de Tecnología por Estados Competidores: La Nueva Carrera por el Conocimiento

Por **Pedro Sebastián**, CEO, Founder & Owner ESRM Consulting Global S.L

En el siglo XXI, la tecnología ha sustituido en gran medida a las materias primas como principal factor de poder. Quien domina las tecnologías críticas no solo obtiene ventajas económicas, sino también superioridad militar, capacidad de influencia geopolítica y resiliencia industrial.

Diversos informes públicos de agencias gubernamentales y organismos de seguridad de Europa, Estados Unidos y otras democracias advierten de que algunos Estados desarrollan campañas de espionaje económico, industrial y ciberespionaje con el objetivo de acelerar su desarrollo tecnológico, reducir costes de investigación y obtener ventajas estratégicas frente a sus competidores.

Estas actividades pueden dirigirse contra empresas, universidades, centros de investigación, organismos públicos, laboratorios, startups y cualquier organización que desarrolle conocimiento de alto valor.

¿Qué tecnologías son las más buscadas?

1 Electrónica y semiconductores

Los semiconductores constituyen el recurso estratégico más importante de la economía digital.

- Sin microprocesadores no existirían:
- Inteligencia Artificial
- Computación de alto rendimiento
- Centros de datos
- Vehículos autónomos
- Redes 5G y futuras 6G
- Sistemas militares inteligentes
- Satélites y tecnología espacial

El conocimiento relacionado con el diseño de chips, litografía, encapsulado, materiales y procesos de fabricación representa uno de los principales objetivos de las operaciones de inteligencia tecnológica.

2 Informática, software e Inteligencia Artificial

El software se ha convertido en el auténtico multiplicador de capacidades.

Los Estados buscan acceder a:

- Algoritmos de IA
- Modelos de aprendizaje automático
- Computación cuántica
- Sistemas operativos
- Plataformas cloud
- Criptografía
- Herramientas de análisis masivo de datos
- Software industrial
- Gemelos digitales
- Automatización avanzada

En muchos casos el verdadero valor ya no reside únicamente en el hardware, sino en el conocimiento acumulado durante años de desarrollo.

3 Aeronáutica y espacio

La industria aeroespacial continúa siendo una de las más protegidas del mundo.

Las tecnologías de interés incluyen:

- Motores aeronáuticos
- Materiales ultraligeros
- Aviónica
- Sistemas de navegación
- Satélites
- Observación terrestre
- Lanzadores espaciales
- Comunicaciones espaciales
- Vehículos hipersónicos



Muchas de estas capacidades poseen aplicaciones tanto civiles como militares, lo que las convierte en tecnologías de doble uso especialmente sensibles.

4 Tecnologías militares y de defensa

Los sistemas de defensa modernos integran electrónica, software, inteligencia artificial y comunicaciones avanzadas.

Entre las capacidades más sensibles destacan:

- Guerra electrónica
- Sistemas de radar
- Sensores avanzados
- Comunicaciones seguras
- Sistemas de mando y control
- Tecnologías navales
- Defensa aérea
- Drones
- Vehículos autónomos
- Sistemas espaciales
- Ciberdefensa

La superioridad tecnológica en este ámbito puede marcar diferencias estratégicas durante décadas.

5 Equipos de fabricación industrial

La capacidad de fabricar tecnología avanzada resulta tan importante como diseñarla.

Por ello existe un enorme interés en:

- Robótica industrial
- Automatización
- Fabricación inteligente
- Máquinas CNC
- Litografía
- Fabricación aditiva
- Impresión 3D industrial
- Metrología de precisión
- Automatización de procesos
- Industria 4.0

Controlar estas tecnologías significa controlar la producción futura.

6 Materiales avanzados

Los nuevos materiales son la base de prácticamente todas las industrias tecnológicas.

Los desarrollos más buscados incluyen:

- Nanotecnología
- Grafeno
- Aleaciones especiales
- Materiales compuestos
- Fibra de carbono
- Cerámicos avanzados
- Materiales inteligentes
- Materiales para baterías
- Superconductores
- Materiales resistentes a altas temperaturas

Su aplicación afecta directamente a sectores como la aviación, la energía, el espacio, la medicina, la automoción y la defensa.

¿Cómo se obtiene esta información?

Los informes públicos de organismos de seguridad describen un amplio abanico de métodos empleados para intentar acceder a tecnología estratégica, entre ellos:

- Ciberespionaje mediante campañas dirigidas.
- Robo de propiedad intelectual.
- Compromiso de cadenas de suministro.
- Captación de personal con acceso privilegiado.
- Uso de empresas pantalla o intermediarios para adquirir tecnología restringida.
- Colaboraciones de investigación utilizadas de forma indebida.
- Explotación de vulnerabilidades en proveedores y contratistas.

En muchos casos estas actividades combinan operaciones técnicas con inteligencia humana y análisis de información disponible públicamente.

La protección del conocimiento: una prioridad estratégica

La ciberseguridad ya no consiste únicamente en proteger redes o sistemas informáticos.

Hoy implica proteger el conocimiento.

La propiedad intelectual, los diseños industriales, los



Por ello, las empresas deben adoptar una estrategia integral basada en:

- ▶ Protección de la propiedad intelectual.
- ▶ Gestión del riesgo de terceros y cadena de suministro.
- ▶ Inteligencia de amenazas.
- ▶ Seguridad en investigación y desarrollo (I+D).
- ▶ Formación y concienciación del personal.
- ▶ Protección frente a amenazas internas.
- ▶ Clasificación y control de la información sensible.
- ▶ Ciberseguridad industrial (OT/ICS).
- ▶ Monitorización continua de riesgos tecnológicos.

La competencia tecnológica entre Estados continuará intensificándose durante la próxima década. La inteligencia artificial, los semiconductores, la computación cuántica, la biotecnología, la industria espacial y los materiales avanzados marcarán la diferencia entre las economías que lideren la innovación y aquellas que dependan de terceros.

En este escenario, proteger el conocimiento no es únicamente una cuestión de seguridad informática; es una decisión estratégica que afecta a la soberanía tecnológica, la competitividad empresarial y la resiliencia nacional.

La pregunta ya no es si una organización puede convertirse en objetivo de una campaña de espionaje tecnológico, sino si está preparada para proteger aquello que la hace verdaderamente competitiva.

¿Está su organización preparada para proteger su activo más valioso: el conocimiento? ■



"Martes con..." en Hostpitalet de Llobregat, 15 de septiembre Instituto de Medicina Legal y Ciencias Forenses de Cataluña



Generalitat de Catalunya
Departament de Justícia
i Qualitat Democràtica
**Institut de Medicina Legal
i Ciències Forenses de Catalunya**

El pasado día 15 de septiembre, ADSI celebró su segunda edición y último "Martes con..." en el Instituto de Medicina Legal y Ciencias Forenses de Cataluña. La anterior edición fue el pasado 26 de mayo.

El Instituto de Medicina Legal y Ciencias Forenses de Cataluña (IMLCFC), se puso en marcha el 3 de junio de 2002. Se define como un órgano técnico al servicio de la Administración de justicia, adscrito al Departamento y dependiente de la Secretaría de Relaciones con la Administración.

Desde su creación, el IMLCFC ha comportado un cambio sustancial en la organización y gestión de la medicina forense en nuestro país. Durante estos años, el IMLCFC ha llevado a cabo el despliegue orgánico y funcional y ha seguido una línea de consolidación del desarrollo e impulso de la investigación. El IMLCFC mantiene una estrecha colaboración con las instituciones sanitarias de Cataluña, así como con las universidades y otros organismos del ámbito científico.

Recibidos por Yobanka Toledo, Coordinadora Técnica y de Patología Forense de Cataluña.

Tras el saludo inicial de bienvenida por parte del Presidente de ADSI, D. Eduard Zamora, dió comienzo la actividad.

Yobanka Toledo, lidera y gestiona la investigación médico-legal de muertes violentas o sospechosas, además de actuar como representante y ponente institucional en jornadas especializadas del sector.

El Instituto de Medicina Legal y Ciencias Forenses de Catalunya (IMLCFC) está integrado por un equipo multidisciplinar de profesionales relacionados con las ciencias forenses. Aunque la mayor parte de este personal está integrado por médicos especializados en la medicina forense, también trabajan químicos, biólogos, psicólogos, técnicos especialistas en patología y personal de enfermería. Además, en el IMLCFC encontramos personal funcionario administrativo, documentalistas, informáticos y personal de mantenimiento, entre otros.

Las funciones que corresponden al Instituto de Medicina Legal y Ciencias Forenses de Cataluña (IMLCFC) son periciales, docentes y de investigación.

El IMLCFC auxilia a los juzgados, tribunales, fiscalías y oficinas del registro civil mediante la práctica de pruebas periciales médicas, tanto tanatológicas como clínicas y de laboratorio, previstas en la normativa vigente de medicina forense, y por otro lado, realiza actividades de docencia e investigación relacionadas con la medicina forense en colaboración con las instituciones sanitarias de Cataluña.

Estas funciones se materializan en los siguientes servicios principales:

- Servicio de Patología Forense. Práctica autopsias médico-legales y demás actividades relacionadas, incluyendo los estudios antropológicos, identificaciones odontológicas.
- Servicio de Clínica Médico Forense. Realiza peritajes médico-legales, que comprende la valoración genérica de toda patología clínica desde el punto de vista médico-



forense (valoración de daño corporal, exploraciones psiquiátricas y psicológicas), así como la asistencia facultativa médica a detenidos.

Las funciones que corresponden a estos dos servicios se llevan a cabo mediante las seis divisiones que conforman la estructura territorial del IMLCFC (Barcelona Ciudad y Hospitalet de Llobregat, Barcelona Comarcas, Girona, Lleida, Tarragona y Terres de l'Ebre), al frente de las cuales existe un subdirector.

- Servicio de Laboratorio Forense. Realiza análisis biológicos y toxicológicos de casos de interés judicial para investigar la presencia de drogas, alcohol, fármacos o tóxicos en muestras obtenidas durante la autopsia o en la exploración de personas vivas (detenidos, víctimas de violencia de género, etc.). Asimismo, investiga biológicamente casos de agresión sexual.

- Formación, docencia e investigación. Mediante la Sección de Formación, Docencia e Investigación Forense, así como la Comisión de Docencia e Investigación se elabora la propuesta de programa anual de formación continuada, y los programas de investigación y desarrollo realizados por los profesionales del IMLCFC o en colaboración con otros profesionales externos.

Finalizada la ponencia, arrancamos con la visita a los siguientes espacios:

Área de registro: Es el punto de control de acceso y recepción administrativa, donde se gestiona la documentación judicial, el ingreso de oficios, expediente o cadáver.

Sala de neveras (Morgue): Espacio refrigerado con temperatura controladas para la conservación del cadáver a disposición judicial.



Servicio de patología forense: Unidad dedicada a la investigación de muertes violentas. Incluye las salas de autopsias.

Salas de reconocimiento forense: Áreas destinadas a la exploración clínica de personas vivas (clínica médico-forense).

Salas de exploraciones forenses: Espacios anexos o integrados en la clínica médico-forense, donde se realizan los peritajes específicos.

Laboratorios de anatomía patológica: Instalaciones donde se procesan las muestras de tejidos extraídas en las autopsias.

Finalizada la visita, pasamos al encuentro final y esperado, donde pudimos degustar de un cocktail-networking, en compañía de todos los asistentes que nos pudieron acompañar, Socios y Patrocinadores. Gracias a todos!!!

Especialmente unas palabras de agradecimiento y gratitud a Yobanka Toledo, por concedernos esta segunda edición y su entrega con ADSI para llevar a cabo esta exitosa jornada. ■

Elvira Márquez
Vicepresidenta de ADSI



Vanessa Berlanga, nueva embajadora de la Marca Ejército



Uno de sus retos será "que las nuevas generaciones puedan conocer qué hace el Ejército, escuchar a las personas que hay detrás del uniforme y formarse una opinión propia".

El pasado 22 de septiembre recibió las credenciales correspondientes de manos del teniente general Raimundo Rodríguez Roca, en el Palacio de Capitanía en Barcelona. ■

Vanessa Berlanga, socia de ADSI, ha sido nombrada embajadora de la Marca Ejército, que implica la tarea de dar a conocer a la ciudadanía la labor de los integrantes de las Fuerzas Armadas.

[Enlace a la noticia](#)



COREWEAVE, nuevo patrocinador de ADSI

ADSI ha incorporado a COREWEAVE a su notorio grupo de empresas patrocinadoras de su proyecto asociativo.

COREWEAVE es una empresa norte-americana, fundada en 2017, dedicada a cubrir la alta demanda de centros de datos, con especialización en infraestructura de computación en la nube para Inteligencia Artificial, alquilando una enorme potencia de cálculo para que empresas y laboratorios puedan entrenar y ejecutar sistemas de IA.

Dispone en todo el mundo de grandes centros de datos que permiten a sus clientes una alta capacidad para entrenar modelos de IA de gran volumen.

ADSI agradece a COREWEAVE su confianza y colaboración con nuestra Asociación, en la que estamos convencidos será una larga y fructífera relación para ambas partes.

En las imágenes diversos momentos del acto formal de firma del acuerdo de colaboración ADSI-COREWEAVE, realizado en Barcelona aprovechando la presencia en nuestro país de los máximos responsables de seguridad de COREWEAVE.

En la foto de grupo, de izquierda a derecha, Brett N. , Security Manager EMEA; Charles Lieberman, Global Manager Security Operations; Eduard Zamora, Presidente de ADSI; Adrián Sánchez, Data Center Security Specialist Spain y Alberto Peláez, Data Center Security Specialist Spain. ■



ExpoProtection 2026



En su 30.ª edición, EXPOPROTECTION, el salón internacional de la prevención y el control de riesgos, cita a los profesionales en París. En un contexto de policrisis, el evento reunirá a profesionales del sector bajo un eje estratégico: **"Descompartimentar la gestión de riesgos frente a la convergencia de las amenazas y las tecnologías"**, en la que será una plataforma europea de intercambio, influencia y soluciones al servicio de la resiliencia sostenible de las organizaciones.

EXPOPROTECTION se articulada en torno a 2 universos de referencia

La feria se organiza en dos universos de referencia, que permite a los actores de la prevención, expertos y decisores, acceder a una visión de 360° de la cadena de valor del riesgo de manera fluida y exhaustiva:

El Universo Riesgos Profesionales e Industriales: reúne los sectores Salud y Seguridad en el Trabajo, Prevención y Calidad de Vida, Condiciones de Trabajo, Salud y Seguridad en el Trabajo, Protección, Intervenciones y Socorro, y Riesgos Climáticos e Industriales.

El Universo Riesgos de Actos Malintencionados e Incendio: agrupa los sectores Seguridad y Protección, e Incendio.

En un contexto de rápidas transformaciones, la edición 2026 refleja una prevención en la que los desafíos de la seguridad física, los incendios y la salud en el trabajo se cruzan con la intensificación de los riesgos cibernéticos, climáticos y operativos. Esta dinámica está impulsada por

la inteligencia artificial, la robótica y los sistemas conectados, que refuerzan la capacidad de anticipación, al mismo tiempo que plantean nuevos retos en materia de regulación.

Acerca de EXPOPROTECTION

Fundado en la década de 1960, **Expoprotection** celebra en 2026 su 30.ª edición. Esta cita bienal de la prevención y el control de riesgos reúne a cerca de 660 expositores y alrededor de 15.000 visitantes.

El salón ofrece una visión de 360° del mercado de la prevención de riesgos, ya sean profesionales, industriales, climáticos o vinculados a actos malintencionados.

En el evento se presentan las últimas innovaciones del sector, facilita reunirse con expertos de alto nivel y contactar con proveedores de soluciones eficaces para proteger a las personas y a las organizaciones frente al conjunto de amenazas a las que están expuestas.

Enlace e inscripciones gratuitas: ■



ExpoSecurity 2026



EXPOSESECURITY

¡NOS VEMOS EN LA FERIA INTERNACIONAL DE SEGURIDAD, POLICIAL Y TECNOLOGÍA.

 **5 · 6 · 7 DE NOVIEMBRE 2026**
9 CAJA MÁGICA - MADRID
info@exposecurity.net

exposecurity.net +34 611 853 757 expo_security2026



**PERSONAS
TECNOLOGÍA
UN MUNDO MÁS SEGURO**

5 - 6 - 7 de Noviembre
HORARIO: - 10:00h - 18:00h

 **ENTRADA GRATUITA
CON REGISTRO**

+34 611 853 757 expo_security2026 info@exposecurity.net

**Tecnología, equipamiento, innovación y profesionales
reunidos en un mismo lugar.**

GUARDIA CIVIL

INNOVACIÓN
AL SERVICIO
DE LA SOCIEDAD





La Feria de Altas Tecnologías de la Seguridad e Inteligencia, Drones y Antidrones, TECNOSSEC DRONExpo celebra su V edición los próximos 5 y 6 de noviembre en el Madrid Arena.

Acudirán organismos públicos, Fuerzas y Cuerpos de Seguridad nacionales, autonómicos y locales, y empresas de infraestructuras críticas estarán presentes junto con los protagonistas de la industria.



TECNOSSEC DRONExpo será una ocasión para presentar novedades del sector,

Encontrar oportunidades de colaboración entre empresas y con las administraciones, además de promover proyectos y negocios.

Esta V edición de la feria se consolida como un escaparate de la industria nacional con participación internacional, mostrando la cohesión de los actores del sector ante los retos y novedades de la seguridad global y los drones.

TECNOSSEC es un ecosistema de nuevos desarrollos de seguridad, inteligencia, ciberseguridad y emergencias, que tendrá lugar junto con DRONExpo , un espacio centrado en tecnología de drones, sistemas antidrón y aplicaciones para seguridad.

LISTA DE EXPOSITORES

REGISTRO GRATUITO





TAPA EN ACCIÓN: PROTEGIENDOLA CADENA DE SUMINISTRO

TAPA EMEA CONFERENCE- 21 DE OCTUBRE DE 2026 – MADRID

España sufre una de las tasas más altas de delincuencia contra el transporte de mercancías en Europa.

Durante los dos años hasta finales de junio de 2026, la Transported Asset Protection Association (TAPA) registró más de 4.200 ataques contra camiones, almacenes y otros tipos de instalaciones y modos de transporte. El 13% de estos delitos relacionados con la carga, en los que se notificó el valor de las pérdidas, contribuyó a unas pérdidas totales de mercancías en España superiores a 197 millones de euros.

Las pérdidas importantes (más de 100.000 €) derivadas de ataques a la cadena de suministro en España alcanzaron una media de 1.336.836 € por incidente.

En la actualidad, prácticamente todo tipo de mercancías son objetivo de los delincuentes, tanto en almacenamiento como durante el transporte, entre ellas:

- Metales
- Dinero en efectivo
- Herramientas y materiales de construcción
- Alimentos y bebidas
- Joyas y metales preciosos
- Productos electrónicos
- Ropa y calzado
- Cosméticos e higiene personal
- Teléfonos móviles
- Piezas de automoción
- Tabaco
- Maquinaria agrícola
- Bicicletas
- Muebles y electrodomésticos
- Neumáticos
- Equipamiento deportivo y de fitness
- Ordenadores y portátiles
- Juguetes y juegos
- Productos farmacéuticos

¿Qué más pueden hacer los fabricantes y los proveedores de servicios logísticos para proteger sus operaciones de la cadena de suministro en España frente a los ataques de grupos delictivos organizados y otros delincuentes?

El 21 de octubre de 2026, en Madrid, TAPA reunirá a líderes de la industria y a profesionales de las fuerzas y cuerpos de seguridad para analizar las causas de la delincuencia contra el transporte de mercancías en España, así como las actuaciones policiales destinadas a desarticular a los grupos criminales. El evento también presentará soluciones de seguridad ya probadas que protegen cadenas de suministro en toda Europa, además de la inteligencia sobre incidentes de robo de carga que impulsa la respuesta del sector.

La asistencia a la conferencia es gratuita, pero las plazas para los asistentes son limitadas y se asignarán por riguroso orden de inscripción.

Le invitamos a acompañarnos en Madrid para conocer mejor cómo proteger su cadena de suministro en España y prevenir el impacto financiero y reputacional de un ataque criminal.

¡INSCRÍBASE AHORA!



Actualización de datos de socios y amigos de ADSI

Estimado/a Socio/a, Amigo/a,

En su momento, nos aportasteis vuestros datos profesionales y personales, pero en muchas ocasiones estos han cambiado y nos dificulta el contacto con vosotros cuando nos es preciso.

Por ello, te agradeceríamos que:



Nos escribas un correo a:

- Elvira Márquez vicepresidente@adsi.pro
- Eduard Zamora presidente@adsi.pro

Si eres socio de ADSI

Indicando:

*Nombre y apellidos
Empresa y cargo
Domicilio profesional
E-mail profesional
Teléfono de contacto*

*Domicilio particular
E-mail particular
Teléfono de contacto*

Si eres amigo de ADSI

¿Deseas recibir nuestras comunicaciones? Facilitanos tus datos, remarcando que no eres socio.

Gracias por vuestra colaboración!



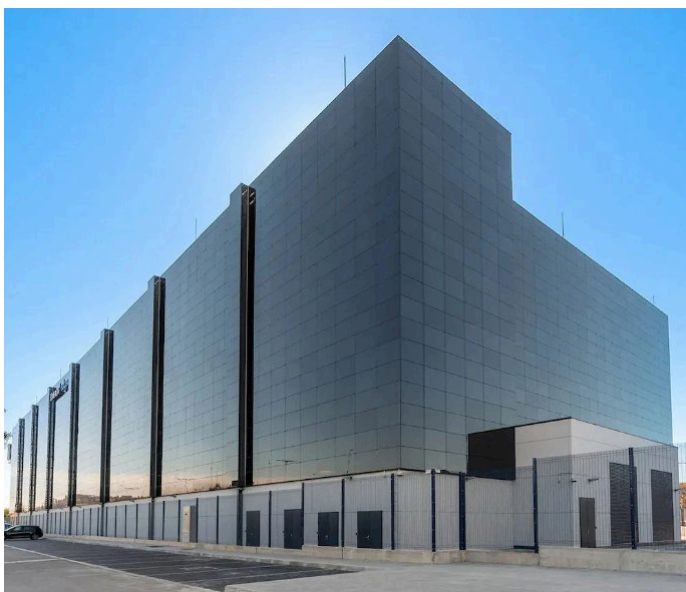


Estimados miembros de la Asociación de Directivos de Seguridad Integral (ADSI).

Nuevo patrocinador

En CoreWeave nos ilusiona dirigirnos a vosotros para presentarnos y compartir quiénes somos, qué hacemos y por qué nos hemos convertido en una de las infraestructuras de referencia para la inteligencia artificial a escala mundial. Lo hacemos convencidos de que la IA y la seguridad integral están cada vez más unidas, y de que tenemos mucho que aportar a los profesionales que protegen cada día a las personas, los activos y las infraestructuras críticas.

Vivimos un momento en el que la inteligencia artificial ha dejado de ser un experimento para convertirse en el motor de los sistemas que millones de personas y organizaciones utilizan cada día. En el ámbito de la seguridad, esa transformación es especialmente evidente: el videoanálisis inteligente, la detección de amenazas, la ciberseguridad o la protección de infraestructuras críticas se apoyan ya en modelos de IA que exigen una potencia de cómputo enorme, fiable y disponible sin interrupciones. Ese es, precisamente, el problema que resolvemos.



Por eso nos ilusiona sumarnos a ADSI: para aportar nuestro conocimiento sobre la infraestructura que hace posible la nueva generación de tecnologías de seguridad y para colaborar con una comunidad que comparte con nosotros un mismo principio: cuando se trata de proteger lo que importa, la fiabilidad no es opcional.

¿Quiénes somos?

CoreWeave (Nasdaq: CRWV) es The Essential Cloud for AI™: un hiperescalador nativo de inteligencia artificial que ofrece infraestructura de computación acelerada de nueva generación para entrenar, ajustar y desplegar modelos de IA a escala. A diferencia de las nubes de propósito general, nuestra plataforma se ha diseñado desde cero para la IA, integrando en un único sistema el cómputo con GPU, las redes de alto rendimiento, el almacenamiento, la orquestación y las herramientas para desarrolladores.

Con sede central en Livingston (Nueva Jersey, EE. UU.) y sede europea en Londres, damos servicio a los principales laboratorios de IA, hiperescaladores y grandes empresas del mundo: nueve de los diez mayores proveedores de modelos de IA confían hoy en CoreWeave. En 2025 alcanzamos unos ingresos de 5.130 millones de dólares —un crecimiento del 168 % interanual— y operamos 43 centros de datos con más de 850 MW de potencia activa y más de 250.000 GPU. Más que capacidad, ofrecemos ejecución fiable a una escala que muy pocos son capaces de igualar.

Nuestra historia

CoreWeave nació en 2017 de la mano de Michael Intrator, Brian Venturo y Brannin McBee. La compañía comenzó su andadura bajo el nombre de Atlantic Crypto, adquiriendo



GPU de NVIDIA para tareas de computación intensiva. Aquella primera etapa nos enseñó, mejor que a nadie, a exprimir el rendimiento de la computación acelerada: la economía de las GPU, la gestión térmica y los despliegues de alta densidad.

Hacia 2019 dimos un giro decisivo: pasamos a ofrecer computación en la nube basada en GPU y adoptamos el nombre de CoreWeave. Cuando, poco después, la IA generativa irrumpió con fuerza, nuestra apuesta temprana por la computación acelerada se reveló profundamente estratégica. En marzo de 2025 dimos otro paso histórico al salir a bolsa en el Nasdaq (CRWV), en la mayor oferta pública de una empresa tecnológica estadounidense desde 2021.

Nuestro crecimiento se apoya en una relación privilegiada con NVIDIA —accionista y socio tecnológico— que nos sitúa, de forma recurrente, entre los primeros proveedores en desplegar sus chips más avanzados. Además, hemos ampliado nuestras capacidades con adquisiciones estratégicas como Weights & Biases (seguimiento de experimentos e iteración de modelos) u OpenPipe (aprendizaje por refuerzo), y con CoreWeave Ventures, que respalda con capital y cómputo a la próxima generación de fundadores de IA.

En Europa hemos establecido nuestra sede en Londres e invertido en centros de datos en el Reino Unido y en Europa continental —incluida España—, alimentados con energía 100 % renovable y concebidos para ofrecer una nube soberana a los clientes europeos.

Soluciones y servicios

1. Cómputo con GPU: acceso a las GPU de NVIDIA más avanzadas (GB200 NVL72, HGX B200/B300, H100/H200, entre otras), en configuraciones flexibles y sobre infraestructura bare metal para obtener el máximo rendimiento en entrenamiento e inferencia.

2. Cómputo con CPU y bare metal: procesadores AMD,

Intel y NVIDIA Grace para preprocesado, orquestación y servicios de apoyo, con acceso directo al hardware y sin capas de virtualización que resten rendimiento.

3. Almacenamiento nativo de IA: CoreWeave AI Object Storage, junto con almacenamiento local y de ficheros distribuido, con rendimiento sostenido a gran escala y sin comisiones de egress ni de peticiones.

4. Redes de alto rendimiento: InfiniBand de NVIDIA, nubes privadas virtuales (VPC) y Direct Connect para mantener las GPU alimentadas de datos con baja latencia y máxima fiabilidad.

5. Servicios gestionados: Kubernetes gestionado (CKS) y Slurm sobre Kubernetes (SUNK), para desplegar y escalar clústeres sin necesidad de construir ni mantener la infraestructura subyacente.

6. Inferencia, IA agéntica y orquestación: inferencia serverless y dedicada, entrenamiento de modelos, renderizado y VFX, y CoreWeave Mission Control, que aporta visibilidad de extremo a extremo, seguridad y automatización operativa.

Por qué elegir CoreWeave

1. Una plataforma nativa de IA, de extremo a extremo. No adaptamos una nube genérica: integramos cómputo, red, almacenamiento, orquestación y herramientas en un único sistema pensado para la IA, lo que simplifica las operaciones y acelera el paso a producción.



2. Rendimiento y fiabilidad a escala. Operamos algunos de los sistemas más complejos de la industria coordinando hardware, red y software en cuasi perfecta sincronía, para que las cargas críticas funcionen sin interrupciones.

3. Acceso temprano a la mejor tecnología. Nuestra estrecha relación con NVIDIA nos convierte, con frecuencia, en el primer proveedor en ofrecer sus arquitecturas más recientes, dando a nuestros clientes una ventaja competitiva real.

4. Escalabilidad y visibilidad total. Con Mission Control, nuestros clientes obtienen una visión completa de GPU, red y almacenamiento en tiempo real, detectan incidencias antes de que ocurran y escalan con costes y rendimiento previsibles.

5. Costes transparentes y alineados con el uso. Modelos de precios flexibles para capacidad reservada y bajo demanda, con facturación por uso y sin comisiones ocultas de egress ni de transferencia de datos.

6. Presencia global y soberanía de datos. Infraestructura en Norteamérica y Europa —incluida España— con energía renovable en nuestros centros europeos, para operar cerca de los datos y cumplir los requisitos de soberanía de cada región.

Agradecimiento

En CoreWeave creemos que la infraestructura adecuada es lo que permite que las mejores ideas de IA lleguen a producción y generen impacto real, también en el ámbito de la seguridad. Por eso queremos agradecer a ADSI la oportunidad de presentarnos y de compartir nuestra visión sobre el papel de la infraestructura de IA en el futuro de la seguridad integral. Es un privilegio formar parte de un entorno que impulsa la colaboración, el intercambio de conocimiento y el desarrollo de soluciones que refuerzan la protección de personas, activos e infraestructuras.

Esperamos seguir trabajando junto a los miembros de la asociación, aportando nuestra experiencia y explorando nuevas oportunidades para acompañar al sector en su adopción de la inteligencia artificial con la máxima fiabilidad. Os invitamos a conocer más sobre CoreWeave y a descubrir cómo podemos ayudaros en vuestros retos presentes y futuros. ■

Contacta con nosotros

Sitio web: coreweave.com

Contacto comercial: coreweave.com/contact

Sede central: 290 W Mt Pleasant Ave, Suite 4100, Livingston, NJ 07039 (EE. UU.)





Una trayectoria de crecimiento, seguridad y compromiso

Nuevo patrocinador

El Grupo Gonber se une al proyecto asociativo de ADSI como NUEVO PATROCINADOR.

El Grupo Gonber ha construido su trayectoria desde una visión clara: ofrecer servicios profesionales, cercanos y adaptados a las necesidades de cada cliente. Lo que comenzó como una iniciativa vinculada a los servicios auxiliares ha evolucionado hasta convertirse en un grupo con presencia en distintos territorios y una actividad consolidada en el ámbito de la seguridad privada, los servicios auxiliares, el control de accesos y los grandes eventos.

La historia del grupo está marcada por una evolución progresiva, basada en la experiencia, la profesionalización y la capacidad de adaptarse a las nuevas exigencias del sector.

2015 | Los comienzos

Se crea Gonber Events, inicialmente como empresa especializada en la prestación de servicios de auxiliares y

control de accesos. Este es el punto de partida de una trayectoria empresarial que, con el paso de los años, irá ampliando sus servicios y su presencia territorial.

2019 | La entrada en la seguridad privada

La compañía da un paso decisivo en su evolución al obtener la habilitación como empresa de seguridad privada, inscrita en la Dirección General de la Policía (DGP) con el número 4452. Este momento supone la incorporación de la actividad de seguridad privada a la trayectoria del grupo y abre una nueva etapa de crecimiento y especialización.

2020 | Nace Gonber Control

Con el objetivo de ampliar y diversificar su actividad, nace Gonber Control como empresa especializada en servicios de auxiliares, control de accesos y servicios de apoyo. Esta nueva estructura permite reforzar la capacidad operativa del grupo y sentar nuevas bases para su crecimiento.



2022 | Expansión territorial

El crecimiento continúa con la apertura de una delegación en Castilla y León. La expansión permite al Grupo Gonber ampliar su presencia territorial y acercar sus servicios a nuevos mercados, avanzando en su estrategia de crecimiento más allá de Cataluña.

2023 | Consolidación en grandes eventos

La compañía alcanza una nueva etapa de crecimiento y se consolida en el ámbito de los grandes eventos, participando en operativos que requieren una elevada capacidad de organización, coordinación y respuesta. La experiencia acumulada permite al grupo reforzar su posicionamiento en servicios de seguridad, control y apoyo para eventos de gran afluencia.

2024 | Gonber Seguridad, la identidad de una nueva etapa

Gonber Events adopta Gonber Seguridad como nombre comercial, marca registrada ante la Oficina Española de Patentes y Marcas (OEPM). Esta evolución de la identidad comercial refleja la especialización y el crecimiento de la compañía dentro del sector de la seguridad privada,

aportando una imagen de marca más reconocible y directamente vinculada a sus servicios. Gonber Events continúa siendo la denominación fiscal de la sociedad.

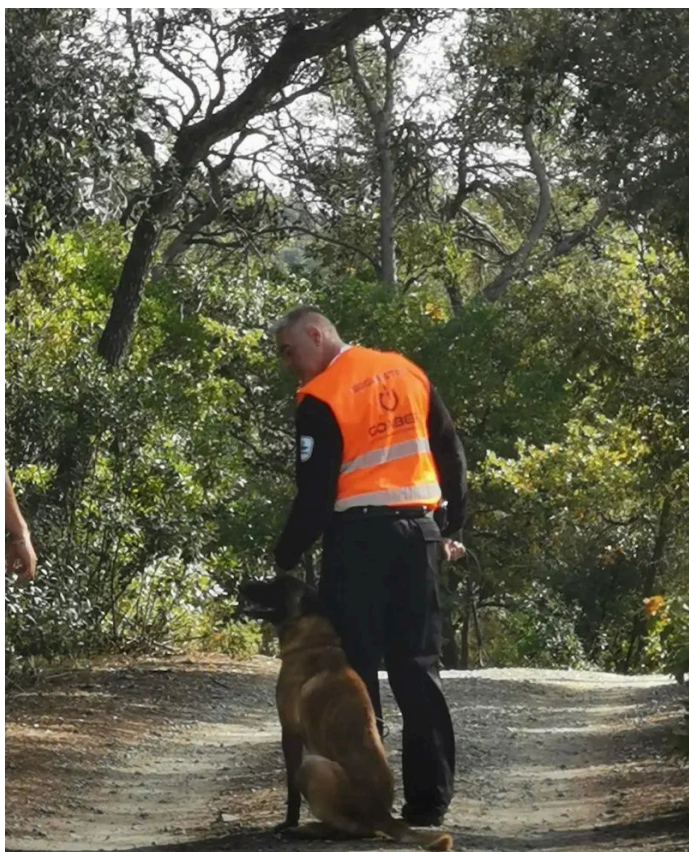
2025-2026 | Consolidación y crecimiento

En la actualidad, el Grupo Gonber continúa su proceso de consolidación en Cataluña y gana fuerza progresivamente en Castilla León y Aragón. El grupo afronta esta nueva etapa con una estrategia de crecimiento sostenible, apoyada en la experiencia adquirida en seguridad privada, servicios auxiliares, control de accesos y grandes eventos.

Una mirada hacia el futuro

Hoy, el Grupo Gonber afronta el futuro con la experiencia de más de una década de trayectoria y con la voluntad de seguir creciendo de forma sólida y responsable. La prioridad continúa siendo ofrecer un servicio profesional y de calidad, reforzar la confianza de sus clientes y consolidar su presencia en los territorios donde desarrolla su actividad.

Desde sus primeros servicios auxiliares en 2015 hasta su actual expansión territorial, la evolución del Grupo Gonber representa una apuesta constante por la profesionalización, la adaptación y el compromiso con el sector de la seguridad. ■





Expertos en sistemas de seguridad

Nuevo patrocinador

Los últimos años, el mundo evoluciona a una velocidad vertiginosa. Nuestra seguridad se ve afectada por nuevos factores a tener en cuenta:

- Las amenazas se renuevan
- La tecnología alcanza un grado de complejidad que la hace difícilmente comprensible
- Los recursos disponibles son limitados
- La exigencia de la normativa se incrementa
- Los ciberataques se multiplican y se sofistican
- Las directivas europeas son cada vez más restrictivas para hacer frente a los desafíos globales

Muchas de los retos que presenta esta coyuntura no se afrontan con un incremento del número de vigilantes. Para garantizar la seguridad en muchos casos, es necesario acudir empresas líderes en tecnología que cuenten con:

- Fabricantes de primer orden mundial
- Integración de sistemas (arquitecturas de red, federación...)
- Analíticas avanzadas de vídeo
- Inteligencia artificial aplicada a flujos de vídeo
- Ciberseguridad

MKV MEDIALAB somos una ingeniería especializada en sistemas de seguridad. Nuestros alcances incluyen el diseño, la arquitectura de red, la instalación, la puesta en marcha, el mantenimiento y la integración de CCTV, analíticas de vídeo, controles de accesos e intrusión en una única plataforma.

Nuestros orígenes como ingeniería de IT hacen que compaginemos las necesidades de los responsables de seguridad con las posibilidades de los equipos de IT de las organizaciones. Estamos homologados por el Ministerio del Interior como empresa de seguridad privada con el número 4548.



A la vanguardia en sistemas contra intrusión



Videovigilancia IP de última generación en entornos urbanos e infraestructuras críticas



El dinamismo con el que se desarrolla el sector de la seguridad obliga a que los proyectos más emblemáticos solo puedan ser acometidos por integradores con amplia experiencia. Para la realización de estos proyectos, en MKV MEDIALAB trabajamos exclusivamente con marcas de primer nivel mundial, fundamentalmente europeas y americanas:

- MILESTONE Systems: Premier Partner
 - Configuración de 50+ MILESTONE CORPORATE
 - Integración de 10.000+ dispositivos en MILESTONE
- AXIS Communications: Gold Partner
- 2N: Elite Partner
- AJAX: 50+ instalaciones
- Honeywell, Synology, D-Link, HPE y Fortinet
- BriefCam, Hafnia e IntellexVision: Partner certificado

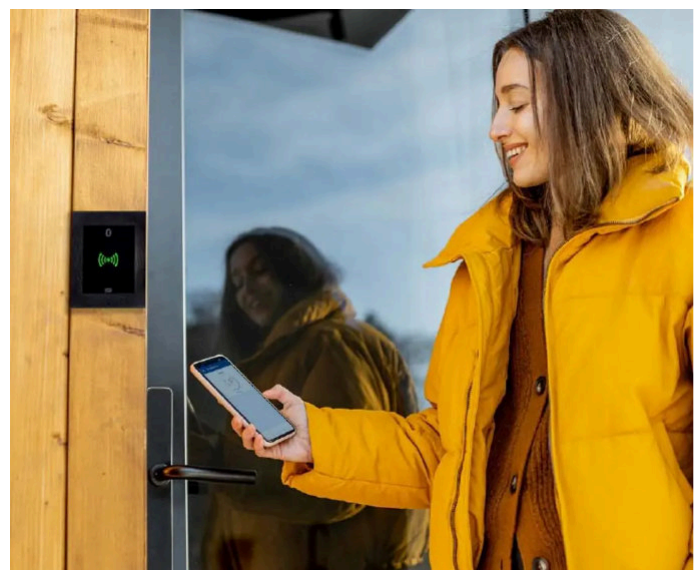
Nuestro equipo cuenta con formación certificada por los fabricantes y experiencia en el uso de las plataformas más avanzadas del mercado. La calidad de nuestro trabajo nos ha llevado a ser recomendados por estos fabricantes para proyectos de gran envergadura.

MKV MEDIALAB presta servicio ofreciendo soluciones integrales de seguridad, fiables y con tecnología de vanguardia en sectores tan diversos como:

- Infraestructuras: aeropuertos, puertos, vertederos, aparcamientos.
- Movilidad y transporte: autopistas, ferrocarril, metro, plataformas logísticas.
- Industria: siderurgia, automóvil, petroquímica, agroalimentaria, minería.
- Energía: centrales nucleares, fotovoltaicas, eólicas, subestaciones.
- Administraciones públicas: smart cities, museos, recintos deportivos, espacios de eventos.
- Servicios de emergencia: cuerpos de seguridad, bomberos, equipos de emergencia.
- Servicios: retail, centros comerciales, hoteles.
- Educación: campus universitarios, institutos, colegios, bibliotecas.
- Sanidad: hospitales, ambulatorios, centros de salud, laboratorios. ■



Técnicos homologados de MKV Medialab durante una instalación



Control de accesos: soluciones integradas para empresas, edificios y áreas sensibles



ARMATURA

Entrevista al Equipo de Seguridad de ZKTeco ARMATURA



Encuentro con el equipo de desarrollo de negocio de Armatura en España:

- Francisco Javier Boter PMM Security Solutions
- Manuel David Gonzalez Presales Security Solutions
- Roberto Suárez BDM Security Solutions

¿Qué importancia tiene para ustedes formar parte de una asociación especializada en seguridad?

ADSI nos permite compartir experiencias con directivos y profesionales del sector, conocer mejor las necesidades reales del mercado y contribuir al desarrollo de una cultura de seguridad más profesionalizada

Para ZKTeco Europe es importante porque Armatura está orientada a proyectos de alta seguridad, infraestructuras críticas y entornos regulados, donde la prescripción técnica y el conocimiento especializado son esenciales. Para ello disponemos en Europa con un equipo específico de producto, desarrollo de negocio y preventa para

acompañar este tipo de proyectos desde la fase de diseño hasta su implantación.

¿Qué es Armatura?

Armatura es una empresa especializada en soluciones avanzadas de control de accesos e identificación segura, orientada especialmente a proyectos de alta seguridad y entornos de elevada exigencia.).

Su propuesta combina hardware, software y tecnologías biométricas avanzadas dentro de un ecosistema diseñado para ofrecer una gestión de accesos segura, escalable y flexible, con capacidad de integración con sistemas y plataformas de terceros.)

Con fabricación en Tailandia la plataforma en si consta de una certificación en **Grado IV** en control de accesos (bajo normativas como la EN 60839) es el nivel máximo de seguridad electrónica diseñado para **infraestructuras críticas, instalaciones militares y entornos de riesgo muy alto** donde las amenazas son graves y complejas.



¿A quién va dirigido?

Armatura está dirigida principalmente a empresas de seguridad, integradores e ingenierías que trabajan en proyectos de mediana y gran escala con elevados requisitos de seguridad.

Por un lado, se orienta a empresas de seguridad con experiencia en infraestructuras críticas, complejos industriales y otros entornos donde el control de accesos forma parte de una arquitectura de seguridad más amplia.

También tiene un papel especialmente relevante para ingenierías y empresas de consultoría responsables de la prescripción, diseño y dirección de proyectos de seguridad en instalaciones como CPDs, plantas industriales, centros logísticos, instalaciones químicas o farmacéuticas e infraestructuras críticas.

En cuanto al cliente final, Armatura está pensada para organismos públicos y grandes empresas que necesitan soluciones avanzadas de identificación, control de accesos y gestión de credenciales.

Por ello, encontramos su aplicación en sectores como transporte, banca, químicas, farmacéuticas, gas, sanidad, industria, entre otros. Especialmente en proyectos donde la seguridad, la integración y el cumplimiento de determinados requisitos técnicos o normativos y certificación en Grado IV son factores clave.

¿Trabajáis directamente con el cliente final o a través del canal?

El modelo de comercialización de Armatura se basa en un canal especializado y certificado, aunque su estructura puede variar en función del país.

En algunos mercados trabajamos a través de distribuidores o mayoristas con acuerdos específicos, como es el caso de Iberia con Casmar. En otros países, como Reino Unido, Polonia o Grecia, contamos con partners e integradores certificados que disponen de la formación, experiencia y capacidad técnica necesarias para comercializar, instalar y dar soporte posventa a este tipo de proyectos.

En todos los casos, Armatura apuesta por un modelo de canal certificado, ya que se trata de soluciones que requieren un conocimiento técnico elevado tanto en la fase de diseño como en la implantación y el mantenimiento posterior.

¿Cómo se está incorporando esta solución a los proyectos y qué papel juegan los distintos agentes que intervienen en su definición y especificación? Entiendo que tiene un componente importante de prescripción, ¿es así?

Sí. Armatura está especialmente pensada para proyectos en los que existe una fase previa de ingeniería y prescripción.



Por el tipo de entornos en los que se implanta, es importante analizar previamente los requisitos del cliente, la arquitectura de seguridad, las integraciones necesarias y las condiciones específicas de cada instalación.

Esta labor de prescripción permite definir la solución más adecuada desde el inicio del proyecto y adaptar Armatura a las necesidades concretas de cada cliente, tanto desde el punto de vista técnico como operativo.

¿Qué características o capacidades diferenciales aporta vuestra solución respecto a otras plataformas o soluciones existentes?

Principalmente destacaremos cuatro:

- **Integración unificada.** Armatura permite integrar en una misma arquitectura sistemas de control de accesos y presencia, intrusión, VMS, ascensores y plataformas de gestión de edificios, además de tecnologías y protocolos como BACnet o MQTT. Esto facilita una gestión más centralizada y evita trabajar con sistemas aislados.

- **Escalabilidad enterprise.** La plataforma está preparada para proyectos de gran tamaño, con capacidad para gestionar hasta 1 millón de usuarios, 10.000 puertas y 5.000 clientes simultáneos, trabajando sobre bases de datos PostgreSQL o MS SQL Server.

- Tecnología propia y flexibilidad de identificación.

Armatura combina biometría avanzada, como reconocimiento facial y de palma, con un amplio abanico de tecnologías RFID, credenciales móviles mediante Bluetooth, códigos QR y funcionalidades como autenticación multifactor o anti-passback. Esta variedad permite adaptar la solución a diferentes requisitos de seguridad y operativa.

- **Seguridad y certificaciones.** Armatura dispone de soluciones certificadas en Grado IV para control de accesos y incorpora mecanismos de protección como cifrado AES-256, comunicaciones TLS y diferentes capacidades orientadas a reforzar la seguridad de la plataforma.

¿Qué proyectos o experiencias destacarías como especialmente relevantes para mostrar cómo vuestra solución responde a necesidades de seguridad complejas? ¿Podéis compartir algunos casos de éxito?

Contamos con diferentes proyectos de referencia, aunque en muchos casos, por tratarse de organismos, infraestructuras críticas o empresas con elevados requisitos de seguridad, no estamos autorizados a identificar públicamente al cliente.

- **Transporte público.** Uno de los casos más representativos es la implantación de un sistema de pago



biométrico mediante reconocimiento de palma para ATTO, desarrollado junto con el integrador y utilizando el lector AMT-PVR-10.

- **Sector público e infraestructuras.** Hemos participado en proyectos para centros de control y organismos públicos, incluyendo despliegues con Armatura One, servidores redundantes, controladoras y lectores biométricos y de proximidad. También se han desarrollado soluciones para el control de accesos, señales técnicas y vídeo en infraestructuras como túneles, integrando la plataforma con sistemas BMS, CCTV y LPR.

- **Industria y entornos regulados.** Armatura también está presente en instalaciones donde existen requisitos específicos de alta seguridad y cumplimiento normativo, como empresas del sector alimentario sujetas a criterios de Food Defense, CPDs y otras instalaciones críticas.

- **Telecomunicaciones.** Otro ejemplo es un proyecto multisede para un gran operador de telecomunicaciones en Chipre, donde Armatura se integra con el sistema de intrusión de Risco para centralizar y reforzar la seguridad

de diferentes instalaciones distribuidas por todo el país.

Además, actualmente se están desarrollando nuevas integraciones con plataformas de otros fabricantes, sistemas BMS y diferentes soluciones PSIM, ampliando progresivamente las capacidades de interoperabilidad del ecosistema Armatura.

¿Qué evoluciones tenéis previstas en los próximos años?

El roadmap de Armatura seguirá centrado en ampliar y evolucionar el ecosistema de soluciones, tanto a nivel de hardware como de capacidades de integración con otros sistemas y plataformas.

Veremos nuevas propuestas en el ámbito de la intercomunicación, evoluciones de los dispositivos actuales y nuevas soluciones Stand Alone con mayores opciones de conectividad e integración.

El objetivo es seguir ampliando la flexibilidad de la plataforma y ofrecer soluciones cada vez más adaptables a diferentes arquitecturas de seguridad y necesidades de proyecto. ■





IMAN Seguridad: la evolución hacia una seguridad inteligente

Por **Javier Montes González**, Director Servicios Híbridos y Nuevas Tecnologías IMAN Services

El sector de la seguridad está viviendo una profunda transformación. La evolución de la inteligencia artificial, la analítica avanzada, la automatización, los sistemas autónomos y la capacidad de integrar diferentes tecnologías están permitiendo evolucionar desde modelos tradicionalmente reactivos hacia una seguridad cada vez más conectada, eficiente y orientada a la anticipación.

En IMAN Seguridad entendemos esta evolución como una oportunidad para desarrollar una nueva generación de servicios en los que tecnología y personas trabajan de manera coordinada.

Nuestro objetivo no es sustituir el factor humano por tecnología, sino utilizarla para ampliar sus capacidades, mejorar la información disponible y conseguir que cada recurso intervenga donde realmente aporta mayor valor.

Esta transformación también está impulsando una evolución en el perfil de nuestros Vigilantes de Seguridad. El profesional de seguridad incorpora progresivamente nuevas competencias tecnológicas y una mayor cualificación para operar plataformas, interpretar información procedente de diferentes sistemas y gestionar servicios cada vez más digitalizados.

El Vigilante de Seguridad evoluciona así hacia un perfil más tecnológico, especializado y conectado, en el que su experiencia y criterio profesional se complementan con nuevas herramientas que amplían su capacidad de actuación.

Global SOC: el centro de nuestro modelo de seguridad

En el centro de esta estrategia se encuentra nuestro Global SOC (Security Operations Center), concebido como mucho más que un centro receptor y gestor de señales.

El Global SOC constituye una plataforma tecnológica y operativa desde la que integramos, supervisamos y

gestionamos en tiempo real los diferentes sistemas y servicios de seguridad de nuestros clientes.

Videovigilancia, analítica de vídeo mediante inteligencia artificial, control de accesos, sistemas de intrusión, comunicaciones, plataformas de integración, sensores IoT y nuevas tecnologías convergen en un entorno común que permite disponer de una visión global de cada instalación.

Esta arquitectura facilita la correlación de eventos procedentes de diferentes sistemas, la verificación de situaciones y la aplicación de procedimientos operativos, permitiendo transformar múltiples fuentes de información en una respuesta coordinada.

El Global SOC se convierte así en el núcleo tecnológico y operativo que conecta instalaciones, sistemas, operadores y profesionales de seguridad.

Servicios Híbridos: tecnología y vigilancia trabajando conjuntamente

Uno de los principales ejemplos de esta evolución son nuestros Servicios Híbridos de Seguridad.

Este modelo combina tecnología avanzada, supervisión desde el Global SOC y, como elemento diferencial, ponemos a disposición del cliente Vigilantes de Seguridad en exclusiva para la gestión remota de sus instalaciones.

Estos profesionales, con un perfil cada vez más tecnológico y especializado, pueden gestionar de manera remota los diferentes emplazamientos del cliente desde nuestro Global SOC, apoyándose en sistemas de videovigilancia inteligente, analítica mediante IA, control



de accesos, intrusión, sensores IoT y otras tecnologías integradas.

Entre las funciones desarrolladas se encuentran las videorondas, la verificación de eventos y alarmas, la gestión remota de los sistemas de seguridad y la inspección y supervisión del estado de los diferentes sensores y dispositivos IoT desplegados en las instalaciones.

Esto permite que una ronda de seguridad evolucione desde una comprobación exclusivamente visual hacia una supervisión mucho más completa del estado de las instalaciones y de sus diferentes sistemas.

Ante una alarma, anomalía o evento, el Vigilante de Seguridad asignado al cliente dispone de información en tiempo real para verificar la situación, aplicar los procedimientos establecidos y coordinar, cuando sea necesario, los recursos presenciales disponibles.

Este modelo permite además que el Vigilante de Seguridad conozca en profundidad las instalaciones, procedimientos, operativa y particularidades del cliente,

manteniendo una continuidad en la prestación del servicio a pesar de realizarse de forma remota.

La tecnología amplía así la capacidad de supervisión del profesional de seguridad, permitiéndole gestionar diferentes instalaciones desde un entorno tecnológico avanzado y desarrollar funciones de mayor valor añadido.

El resultado es una combinación de dedicación exclusiva, capacidad tecnológica y criterio profesional, manteniendo al Vigilante de Seguridad como una pieza fundamental dentro del servicio.

Drones: seguridad, inspección y supervisión desde una nueva perspectiva

La incorporación de drones dentro de los servicios de seguridad abre nuevas posibilidades especialmente interesantes en instalaciones con grandes extensiones o con zonas complejas de supervisar.

Instalaciones industriales, centros logísticos, infraestructuras críticas, instalaciones energéticas,

TECNOLOGÍA + INTELIGENCIA + PERSONAS

IMAN SEGURIDAD

GLOBAL SOC

SEGURIDAD SIN LÍMITES

Integramos, supervisamos y gestionamos en tiempo real los sistemas de seguridad de nuestros clientes.

- VIDEOVIGILANCIA INTELIGENTE
- CONTROL DE ACCESOS
- SENSORES IoT
- IA Y ANALÍTICA
- DRONES
- CONSERJERÍA REMOTA
- INTELIGENCIA DE DATOS
- PERSONAS MÁS SEGURAS

PREVENIR
DETECTAR
ANALIZAR
RESPONDER

IMAN SEGURIDAD

PROTEGEMOS HOY LOS ENTORNOS DEL MAÑANA

UNA SEGURIDAD MÁS AVANZADA



plantas fotovoltaicas, parques eólicos, plantas de tratamiento y gestión de residuos, explotaciones agrícolas y otras grandes superficies pueden beneficiarse especialmente de este tipo de soluciones.

Desde IMAN Seguridad trabajamos en la integración de estos dispositivos dentro de la operativa de seguridad y su conexión con nuestro Global SOC.

Los drones pueden complementar las rondas tradicionales, realizar recorridos, verificar alarmas o inspeccionar zonas de difícil acceso. La incorporación de cámaras visibles, térmicas y sistemas de analítica permite ampliar además sus aplicaciones más allá de la vigilancia convencional.

Entre ellas se encuentran las inspecciones visuales de instalaciones e infraestructuras, apoyo a tareas de mantenimiento, supervisión de elementos críticos o detección temprana de anomalías térmicas, posibles conatos e incendios.

Estas capacidades adquieren especial relevancia en instalaciones industriales, energéticas o de tratamiento de residuos, donde una detección temprana puede proporcionar información de gran valor para la gestión de una incidencia.

De esta forma, una misma plataforma tecnológica puede generar información de utilidad tanto para seguridad como para otras áreas operativas del cliente.

Pero el verdadero valor no está únicamente en el dron. Está en su integración dentro del ecosistema global de seguridad, donde la información obtenida puede ser analizada, correlacionada con otros sistemas y gestionada desde un entorno operativo común.

Consejería Remota: atención, control y gestión a distancia

La transformación tecnológica también permite evolucionar servicios tradicionalmente presenciales mediante nuestro modelo de Consejería Remota.

La solución permite gestionar funciones como atención a usuarios y proveedores, control y autorización de accesos, apertura remota de puertas, gestión de incidencias, videointerfonía bidireccional y supervisión de instalaciones.

Uno de sus elementos diferenciales es la interacción

directa entre el usuario y el profesional que presta el servicio.

A través de una pantalla de comunicación bidireccional instalada en el emplazamiento, usuario y Vigilante de Seguridad pueden verse y hablar en tiempo real. Esta interacción audiovisual permite ofrecer una atención cercana y directa mientras el profesional dispone simultáneamente de acceso a los sistemas necesarios para verificar autorizaciones, gestionar accesos o resolver incidencias.

El modelo permite ampliar horarios, centralizar la atención de diferentes ubicaciones y combinar la prestación remota con recursos presenciales cuando las necesidades del cliente así lo requieran.

Global Intelligence Center: transformar información en inteligencia

La evolución natural de un ecosistema cada vez más conectado es nuestro Global Intelligence Center (GIC).

Actualmente, los sistemas de seguridad generan enormes cantidades de información. Cámaras, controles de acceso, sensores, alarmas, sistemas de gestión y fuentes externas proporcionan continuamente datos sobre lo que sucede en las instalaciones.

A estas fuentes incorporamos además un elemento especialmente importante: nuestros propios Vigilantes de Seguridad.

Su presencia sobre el terreno, conocimiento de las instalaciones y contacto directo con la operativa del cliente los convierte también en una fuente de información de gran valor. Incidencias, observaciones, situaciones anómalas o cambios detectados durante el servicio pueden incorporarse al ecosistema de información.

El reto consiste en transformar todos estos datos en conocimiento útil.

El GIC nace con esta filosofía: recopilar, integrar, analizar y contextualizar información procedente tanto de fuentes tecnológicas como humanas para identificar patrones, tendencias, riesgos o situaciones que puedan afectar a nuestros clientes.

La combinación de inteligencia artificial, analítica



avanzada, fuentes de información y conocimiento operativo permite avanzar progresivamente desde modelos basados principalmente en la detección hacia una seguridad con una mayor capacidad de anticipación y prevención.

De la tecnología al servicio: un modelo integral

Servicios Híbridos, Drones, Conserjería Remota, Global Intelligence Center y otros nuevos servicios y soluciones tecnológicas representan diferentes líneas de innovación, pero todas responden a una misma estrategia: integrar personas, tecnología e inteligencia dentro de un único ecosistema de seguridad.

El Global SOC actúa como elemento vertebrador de este modelo, conectando sistemas, operadores, Vigilantes de Seguridad e información para ofrecer una respuesta coordinada ante cada situación.

Pero para que esta transformación sea posible es necesario algo más que tecnología.

La participación conjunta de nuestro Departamento de Tecnología e Innovación, Ingeniería e Instalaciones nos permite abordar todo el ciclo de vida de cada solución: desde el análisis de las necesidades y el diseño de la

arquitectura tecnológica hasta la integración, instalación, puesta en marcha y posterior operación del servicio.

Esta capacidad nos permite no solo identificar nuevas tecnologías, sino convertirlas en soluciones reales, integradas y adaptadas a las necesidades de cada cliente.

Y en este proceso las personas siguen siendo fundamentales. La evolución tecnológica implica también una evolución de nuestros profesionales hacia perfiles cada vez más cualificados, tecnológicos y especializados, capaces de interactuar con sistemas de inteligencia artificial, plataformas integradas, sensores IoT, videovigilancia inteligente, drones y nuevas herramientas que continuarán incorporándose al sector.

En IMAN Seguridad entendemos que el futuro no estará definido únicamente por disponer de más tecnología, sino por nuestra capacidad para integrar con las personas, transformar la información en inteligencia y convertir todo ello en nuevos servicios de seguridad.

Porque innovar en seguridad no significa únicamente incorporar nuevas herramientas. Significa evolucionar nuestra forma de proteger. ■





Lecciones para fortalecer la resiliencia organizativa. Cumplimiento normativo a la preparación ante crisis

Oriente Medio 2026: lecciones para fortalecer la resiliencia organizativa.

La escalada del conflicto en Oriente Medio durante 2026 puso a prueba la capacidad de respuesta de las organizaciones ante una crisis geopolítica de rápida evolución. En pocos días, las interrupciones afectaron a los viajes internacionales, la seguridad de los empleados, las cadenas de suministro y la continuidad de las operaciones, evidenciando la importancia de una preparación sólida y una gestión de crisis eficaz.

Las experiencias vividas durante este periodo muestran que la resiliencia organizativa depende, en gran medida, de cuatro factores clave: una visibilidad precisa de la plantilla, una comunicación rápida y fiable, estructuras de gobernanza claras y una preparación continua. Las organizaciones que habían desarrollado estas capacidades respondieron con mayor agilidad ante un entorno cambiante y altamente incierto.

Uno de los mayores desafíos fue la gestión de evacuaciones y movimientos de personal en un contexto

marcado por restricciones de transporte, cambios regulatorios y necesidades de apoyo a empleados y familiares. Esta situación puso de manifiesto la necesidad de contar con planes de contingencia flexibles y regularmente testados mediante ejercicios y escenarios realistas.

Este documento analiza las lecciones aprendidas durante la crisis y ofrece recomendaciones prácticas para reforzar la preparación ante futuras escaladas. Su objetivo es ayudar a las organizaciones a construir una resiliencia más sólida, mejorar la toma de decisiones y proteger tanto a las personas como a las operaciones en un entorno global cada vez más volátil.

No espere a la próxima escalada para identificar vulnerabilidades. Descargue ahora el informe y descubra acciones prácticas para fortalecer la resiliencia de su organización: [Conflicto en Oriente Medio 2026 | International SOS](#).

Directiva CER: del cumplimiento normativo a la preparación ante crisis



La Directiva de Resiliencia de las Entidades Críticas (CER) supone un cambio significativo para las organizaciones que prestan servicios esenciales en Europa. Más allá del cumplimiento normativo, exige demostrar que existen capacidades reales para responder a crisis, interrupciones y amenazas cada vez más complejas.

Aplicable a sectores como energía, transporte, salud, banca e infraestructuras digitales, la directiva refuerza los requisitos en materia de evaluación de riesgos, gobernanza, gestión de crisis y continuidad de negocio. También promueve un enfoque integral que contempla dependencias críticas, proveedores estratégicos y procesos esenciales.

Además, su alineación con marcos como NIS2 y DORA brinda a las organizaciones la oportunidad de desarrollar un modelo más sólido e integrado de resiliencia.

Este informe ofrece una guía práctica para comprender los requisitos de la CER, evaluar el nivel de preparación de la organización y convertir el cumplimiento regulatorio en una ventaja estratégica para proteger operaciones esenciales y afrontar futuras crisis

CTA

¿Está preparada su organización para cumplir con la Directiva CER y responder eficazmente ante una crisis? Descargue el informe completo y descubra cómo convertir las exigencias regulatorias en una verdadera capacidad de resiliencia, continuidad y gestión de crisis.

[Directiva de resiliencia de Entidades Críticas \(CER\): Del cumplimiento normativo a la preparación de la crisis.](#) ■





SCATI recibe el Premio Marketing Internacional de la Cámara de Comercio de Zaragoza

El galardón reconoce la estrategia de la compañía para impulsar una marca tecnológica española en más de 35 países, adaptando su propuesta de valor a cada mercado.

SCATI, fabricante español de soluciones inteligentes de seguridad, ha recibido el **Premio Marketing Internacional** en el marco de los Premios a la Internacionalización de Aragón 2026, un reconocimiento a la estrategia desarrollada por la compañía para posicionar su marca y su propuesta tecnológica en mercados internacionales.

Con más de 25 años de trayectoria y presencia en más de 35 países, SCATI ha construido su crecimiento internacional sobre una idea clave: mantener una identidad de marca global y, al mismo tiempo, adaptar su propuesta de valor a las características, necesidades y particularidades de cada mercado.

Esta filosofía se refleja también en una estrategia de marketing que ha evolucionado al ritmo de los cambios en la forma de informarse, comunicar y tomar decisiones. El desarrollo de contenidos especializados, el posicionamiento digital, la participación en ferias y eventos, las relaciones con medios y las acciones desarrolladas localmente permiten acercar la tecnología de SCATI a las necesidades concretas de cada sector y cliente.

“Competir en mercados internacionales implica entender que una misma solución no siempre se comunica de la misma manera. Nuestro trabajo consiste en identificar qué aporta realmente valor a cada cliente y trasladarlo de una forma clara, cercana y adaptada a su realidad”, señala **Miguel Ángel Gimeno, Director de Marketing y Desarrollo de Negocio de SCATI.**

El premio supone también un reconocimiento al trabajo conjunto de los equipos que participan en la construcción y proyección internacional de la marca y a una forma de trabajar basada en la evolución constante, el aprendizaje y la capacidad de adaptación.



"Este premio reconoce también una forma de trabajar basada en probar, aprender y evolucionar constantemente. El marketing ha cambiado muchísimo en los últimos años y nosotros hemos evolucionado con él, incorporando nuevos canales, nuevas formas de comunicar y, sobre todo, nuevas maneras de acercarnos a nuestros clientes", explica Raquel Elías, Marketing Manager de SCATI.

El galardón fue entregado el **29 de septiembre en el Palacio de Congresos de Zaragoza**, durante una gala organizada por las Cámaras de Comercio de Zaragoza, Huesca y Teruel y Aragón Exterior (AREX).

Miguel Ángel Gimeno, Director de Marketing y Desarrollo de Negocio de SCATI, y Raquel Elías, Marketing Manager, recogieron el premio de manos de Javier Camo, Director General de Internacionalización del Gobierno de Aragón, y Óscar Calvo, Director Comercial de JCV.

Los Premios a la Internacionalización de Aragón reconocen a las empresas aragonesas que han convertido



su presencia en mercados exteriores en un eje estratégico de crecimiento, competitividad e innovación. Junto a SCATI, en esta edición fueron galardonadas Magdalenas Lázaro (Mr. Brownie), Litera Meat, PRODESA Group y Arvensis Agro. ■





De la tecnología a la capacidad operativa: 30 años acompañando a la seguridad

En un entorno donde las amenazas evolucionan constantemente y la seguridad exige respuestas cada vez más especializadas, la tecnología ha dejado de ser un fin en sí mismo para convertirse en una herramienta al servicio de la capacidad operativa. Esa ha sido precisamente la filosofía que ha guiado la trayectoria de Target Tecnología durante los últimos 30 años.

La compañía celebra en 2026 tres décadas de actividad en las que ha pasado de acercar a España tecnologías avanzadas para la detección de amenazas a consolidarse como un socio integral en proyectos de seguridad, emergencias y protección de infraestructuras críticas. Una evolución que refleja también la transformación experimentada por el propio sector.

"Durante estos 30 años hemos comprobado que la clave no está únicamente en disponer de la mejor tecnología, sino en saber cómo integrarla para que aporte una capacidad real a quienes tienen la responsabilidad de proteger personas, instalaciones y servicios esenciales", explica Luis Rolandi, director adjunto de Target Tecnología. "Nuestra misión consiste en ayudar a

convertir la innovación tecnológica en resultados operativos tangibles".

Más allá del suministro de equipos

Hoy, un proyecto de seguridad abarca mucho más que la adquisición de un sistema. La selección de la tecnología adecuada, su adaptación al entorno operativo, la instalación, la formación de los usuarios, el mantenimiento y la capacidad de respuesta ante incidencias son factores que determinan el éxito de cualquier despliegue.

Con esa visión integral, Target Tecnología ha desarrollado un modelo basado en la comercialización, suministro, instalación, asistencia técnica, mantenimiento, consultoría y formación especializada. Su catálogo reúne soluciones de inspección por rayos X, arcos detectores de metales, sistemas de detección de explosivos y sustancias, tecnologías NRBQe, sistemas antidron, barreras de protección frente a vehículos, robótica pesada y sistemas autónomos, entre otras capacidades.

Sin embargo, el verdadero valor diferencial no reside únicamente en la amplitud de este portfolio, sino en la experiencia acumulada para adaptar cada tecnología a las necesidades específicas de administraciones públicas, Fuerzas y Cuerpos de Seguridad, infraestructuras críticas y operadores privados.

Convertir tecnología en capacidad

Para la compañía, la consultoría se ha convertido en una pieza esencial del proceso. Antes de implantar cualquier solución es necesario comprender el problema, analizar los riesgos y definir qué capacidad operativa se necesita desarrollar. Solo entonces la tecnología puede aportar todo su potencial.

"Cada organización tiene procedimientos, recursos y



necesidades diferentes", señala Luis Rolandi. "Por eso apostamos por un enfoque basado en el análisis previo y el acompañamiento continuo. La tecnología debe integrarse de forma natural en la operativa diaria y ayudar a mejorar la toma de decisiones y la capacidad de respuesta".

La formación constituye el siguiente eslabón de la cadena. Los sistemas más avanzados solo alcanzan su máximo rendimiento cuando los profesionales conocen sus posibilidades, limitaciones y procedimientos de uso. La capacitación permite que la inversión tecnológica se traduzca realmente en una mejora de la seguridad y la operatividad.

"Instalar una solución es solo el principio"

La continuidad operativa es otro de los pilares del modelo de Target Tecnología. Como destaca Mercedes Agustín Vicente, responsable de Postventa de la compañía, "instalar una solución es solo el principio".

El servicio posventa incorpora formación y entrenamiento de operadores, mantenimiento preventivo y predictivo, revisiones periódicas y un equipo técnico especializado preparado para intervenir con rapidez en cualquier punto del territorio nacional. El objetivo es minimizar riesgos, anticiparse a posibles fallos y garantizar que los equipos estén disponibles cuando realmente se necesitan.

Esta capacidad resulta especialmente relevante en entornos donde cualquier interrupción puede tener un impacto significativo sobre la seguridad de las personas o la continuidad de servicios esenciales.

Una relación basada en conocimiento y confianza

La evolución tecnológica también ha transformado la relación entre proveedores y clientes. Según Hugo González Lozano, responsable de Ventas de Target Tecnología, los proyectos actuales exigen conocer en profundidad la operativa de cada organización y mantener una colaboración a largo plazo que incluya soporte técnico, formación y actualización continua.

En palabras de Luis Rolandi, "la confianza se construye combinando conocimiento técnico, cercanía y capacidad de respuesta. Nuestro objetivo es acompañar a los profesionales de la seguridad durante todo el ciclo de vida de sus proyectos".

Treinta años después de su fundación, la trayectoria de Target Tecnología refleja la evolución de un sector que demanda cada vez más integración entre tecnología, conocimiento y personas. Un enfoque orientado a reforzar la capacidad operativa y la resiliencia de las organizaciones, y que comparte plenamente los valores de profesionalización y colaboración que promueve ADSI entre los profesionales de la seguridad. ■





TP-Link presenta Omada | VIGI Conecta Summit 2026, el encuentro de la tecnología del presente que impulsa el futuro

La segunda edición del evento, exclusiva para integradores de sistemas, instaladores y distribuidores de la compañía, reunió a más de 300 profesionales en Madrid,

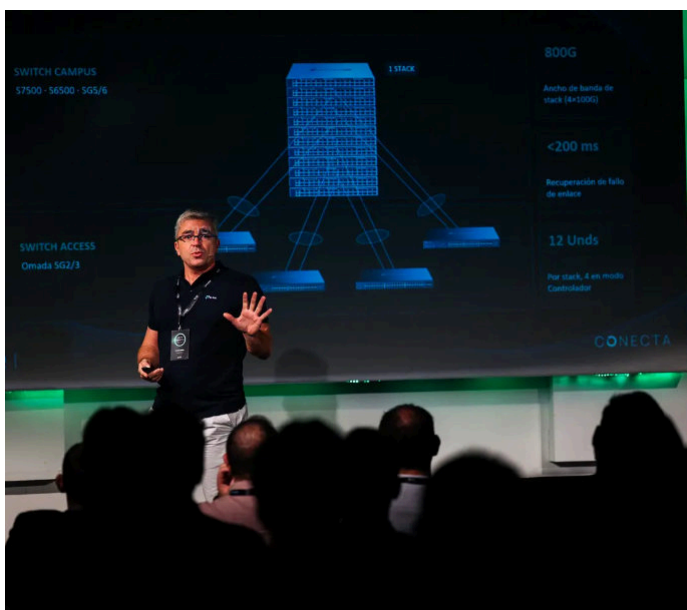
Madrid, 24 de septiembre de 2026. - TP-Link, expertos en soluciones de conectividad, videovigilancia e IoT de alta fiabilidad, ha celebrado la segunda edición del Conecta Summit. En el encuentro, Omada by TP-Link, la solución tecnológica para empresas en el ámbito del networking, y VIGI, la videovigilancia inteligente 24/7 integrada en el negocio, presentaron las tecnologías que impulsan el futuro de las empresas, especialmente en los sectores hostelería, AAPP, educación y sanidad.

El encuentro, celebrado en Madrid el 24 de septiembre, reunió a más de 300 responsables y directivos de empresas integradoras de sistemas, instaladoras, distribuidoras y partners tecnológicos de la compañía. Sirvió además para dar a conocer las últimas novedades de Omada y VIGI en los ámbitos del networking y la videovigilancia, así como para comprobar, mediante demostraciones en directo, cómo estas tecnologías

responden a los retos de sectores como hostelería, puntos de venta, sanidad y administraciones públicas.

Entre las principales novedades presentadas destacó un adelanto exclusivo de la nueva generación de puntos de acceso Wi-Fi 8, junto con la presentación de la nueva gama Omada Fusion, especialmente diseñada para pequeñas y medianas empresas y puntos de venta. Mientras que los nuevos puntos de acceso Wi-Fi 8 anticipan la evolución de la conectividad inalámbrica, Omada Fusion integra en un único equipo router, controlador y, según el modelo, NVR, facilitando la instalación y gestión de las infraestructuras de red y videovigilancia. El Summit también permitió conocer nuevas soluciones de conectividad, infraestructura de red y videovigilancia.

Además, contó con una zona de exposición en la que se mostraron, entre otras tecnologías, soluciones para entornos Enterprise, Hospitality, puntos de venta, sistemas autónomos 4G y las últimas propuestas de Omada y VIGI.



Uno de los principales atractivos de la jornada fue la puesta en marcha real de una solución Omada Campus dentro del propio espacio del evento. Los asistentes pudieron conocer de primera mano todo el proceso, desde la selección de los equipos hasta su instalación, configuración y puesta en marcha, tanto de la infraestructura de red como del sistema de videovigilancia.

TP-Link también dio protagonismo a sus partners, que compartieron con los asistentes sus experiencias y casos reales de aplicación de estas tecnologías. La jornada incluyó una mesa redonda centrada en el sector Hospitality, en la que diferentes profesionales del canal analizaron los principales retos tecnológicos del sector y cómo las soluciones de conectividad y videovigilancia pueden contribuir a mejorar su operativa y la experiencia de cliente.

Posteriormente, los asistentes tuvieron la oportunidad de conocer diferentes casos de éxito desarrollados junto a partners de TP-Link en los ámbitos de la sanidad y la administración pública. Las presentaciones contaron con los testimonios de los clientes finales, que compartieron su experiencia y mostraron cómo las soluciones Omada y VIGI han permitido responder a necesidades específicas de conectividad, gestión de redes y seguridad.

“Hoy no solo hemos presentado las nuevas soluciones que estamos llevando al mercado, sino que también hemos podido comprobar cómo nuestros partners de

todo el país ya las están convirtiendo en proyectos reales que generan valor para sus clientes. Ese es precisamente el espíritu del Omada | VIGI Conecta Summit, compartir innovación, experiencias y casos reales con los profesionales que están haciendo posible la transformación tecnológica de las empresas”, declaró Aaron Wei, Country Manager de TP-Link España, durante la clausura del evento.

Sobre TP-Link:

Con sede en EEUU, TP-Link es el proveedor número 1 mundial en venta de equipos de redes Wi-Fi para empresas y hogares según el IDC Worldwide Quarterly Wireless LAN Tracker del tercer trimestre de 2025. La compañía comercializa las soluciones profesionales Omada, VIGI y Aginet, diseñadas para cubrir las necesidades de conectividad, gestión de redes y videovigilancia de organizaciones, integradores e ISP.

TP-Link desarrolla y suministra infraestructuras de red seguras, escalables y de alto rendimiento en más de 170 países. En España, la compañía dispone de una sólida estructura que centraliza atención al cliente, logística y soporte técnico especializado, garantizando un servicio eficiente y cercano a partners y clientes.

TP-Link mantiene un firme compromiso con la innovación y la excelencia tecnológica, facilitando a empresas de cualquier tamaño el acceso a soluciones avanzadas que impulsen su competitividad y transformación digital. ■



IMMUNE
TECHNOLOGY INSTITUTE

 ADSI 30 años
 asociación de directivos conectados e
 de seguridad integral impulsando

PROGRAMA DIRIGIDO A

Profesionales

de todos los ámbitos, sectores
y responsabilidades

de la seguridad privada,

Directivos y Directores de
Seguridad, usuarios y prestatarios
de sistemas de seguridad.Miembros ADSI
descuento del

20%

Modalidad híbrida

48h. + 8h. de simulacro

Dentro del marco de colaboraciones, ADSI y IMMUNE Technology Institute a través de su área de conocimiento en ciberseguridad aplicada a entornos de vigilancia, combinando seguridad física y digital, ha desarrollado este programa formativo, que tiene como objetivo fundamental capacitar a los profesionales de la seguridad en la identificación, prevención y respuesta ante amenazas híbridas, así como en el cumplimiento normativo y la operación segura de sistemas como CCTV, controles de acceso, biometría o drones.

IMMUNE Technology Institute nos ofrece: Promover un acceso preferente de las formaciones a los Socios y Patrocinadores de ADSI, con un descuento del 20%.

DESCARGA
PROGRAMA COMPLETO

PARA MÁS INFORMACIÓN

Borja de Alarcón
Business Director

borja.alarcon@immune.institute

Resumen de los datos más relevantes de la convocatoria

Modalidad: Híbrida (online con prácticas y simulaciones).

Duración: 48 horas lectivas + 8 horas de simulacro (total estimado: 56 horas).

Nivel: Intermedio.

Dirigido a: Vigilantes de seguridad privada con funciones en CCTV, control de accesos, alarmas, drones y sistemas biométricos.

Requisitos: Certificado de Profesionalidad y tarjeta TIP en vigor.

Metodología:

- Enfoque práctico (20% teoría, 60% práctica, 20% simulacros).
- Casos reales, simulaciones de incidentes y material operativo (checklists, guías, etc.).

Evaluación:

- Prueba teórico-práctica (mínimo 70% para aprobar).
- Simulacro de incidente híbrido con evaluación por competencias.

Titulación:

- Diploma acreditativo alineado con el SEPE.
- Opcional: acreditación con sello de la AEPD.

Contenidos principales:

- Fundamentos de ciberseguridad y marco legal.
- Protección de datos en videovigilancia y control de accesos.
- Amenazas híbridas (físicas + cibernéticas).
- Sistemas biométricos y control de accesos seguros.
- Operación segura de CCTV, alarmas y drones.
- Detección de indicadores de compromiso (IoC).
- Prevención de ingeniería social y desinformación.
- Notificación de incidentes de seguridad.
- Ciberhigiene operativa y concienciación continua.

Objetivos del programa:

- Reducir riesgos de brechas por errores humanos.
- Garantizar el cumplimiento normativo.
- Mejorar la respuesta ante incidentes híbridos.
- Posicionar a las empresas de seguridad como socios estratégicos en resiliencia digital.

Certificación y renovación:

- Certificado válido por un año.
- Posibilidad de renovación mediante examen y simulacro.

Formación continua opcional:

Plataforma online con alertas de amenazas, contenidos formativos y ejercicios periódicos.

DESCARGA DOCUMENTO RESÚMEN



Condiciones especiales de matriculación para socios, adheridos y patrocinadores de ADSI en cursos de la UNIR-Universidad Internacional de La Rioja



Convocatoria Otoño 2026

Tu vocación protege, fórmate para los retos del futuro

CONSIGUE TU DESCUENTO AQUÍ



UNIR te ofrece más de 400 titulaciones con descuentos y ventajas exclusivas gracias al Convenio de Colaboración con tu organización. Además, tienes condiciones especiales en las siguientes titulaciones destacadas:

GRADOS

DESCUENTO 45% PRIMER AÑO
(20% en años sucesivos)

- Grado en Derecho
- Grado en Criminología
- Grado en Ciencias de la Seguridad
- Grado en Ciencias Políticas y Gestión Pública
- Grado en Relaciones Internacionales

Participa en **seminarios y cursos gratuitos** y **reconoce hasta 18 ECTS adicionales**.

DESCUENTO 40% PRIMER AÑO
(10% en años sucesivos)

- Grado en Psicología

MÁSTERES OFICIALES

DESCUENTO 40%

- Máster Universitario en Ciberdelincuencia
- Máster Universitario en Delincuencia Juvenil e Intervención con Menores
- Máster Universitario en Estudios Avanzados en Terrorismo: Análisis y Estrategias
- Máster Universitario en Estudios de Seguridad Internacional
- Máster Universitario en Investigación Criminal
- Máster Universitario en Seguridad Pública
- Máster Universitario en Victimología y Criminología Aplicada
- Máster Universitario en Análisis y Prevención de la Corrupción



Docencia 100% online



Clases en directo



Mentor personal

Infórmate en:

colectivos@unir.net



Delta13-UDIMA

Cátedra en Tecnología aplicada a la seguridad

CURSO DE DIRECTOR DE SEGURIDAD



**OFERTA ASOCIADOS:
70€ AL MES**

Aprende las habilidades esenciales para convertirte en un líder en seguridad. ¡No te lo pierdas!

Curso Homologado por el Ministerio del Interior y acreditado por la Universidad a Distancia de Madrid (UDIMA)



INSTITUTO
DELTA13





UNIVERSITAT DE
BARCELONA

Facultat
de Dret



ADSI

Asociación de Directivos
de Seguridad Integral

CONOCIMIENTO • NETWORKING • PROFESIÓN

MÁSTER EN DIRECCIÓN DE SEGURIDAD PRIVADA

FORMACIÓN UNIVERSITARIA DE REFERENCIA

El conocimiento, la experiencia y la visión estratégica
para liderar la seguridad de hoy y de mañana.

*Personas
Conocimiento
Seguridad*



TITULACIÓN UB

Prestigio académico
y reconocimiento
universitario.



PROFESORADO EXPERTO

Profesionales en activo
y referentes del sector.



MODALIDAD ONLINE Y PRESENCIAL

Flexibilidad para
tu desarrollo profesional.



PERSPECTIVA INTERNACIONAL

Casos, tendencias
y retos globales.

SI ERES ASOCIADO
O PATROCINADOR DE ADSI

**DISPONES DE
GRANDES VENTAJAS
EN TU MATRÍCULA**



ADSI
Asociación de Directivos
de Seguridad Integral

- ✓ Condiciones especiales de matrícula para asociados.
- ✓ Beneficios exclusivos para patrocinadores de ADSI.
- ✓ Consulta todos los detalles a través de nuestros canales de contacto.



UNA FORMACIÓN COMPLETA Y ACTUAL

DIRIGIDA A PROFESIONALES DE LA SEGURIDAD



Dirección
y gestión
de la seguridad



Marco
normativo
y compliance



Seguridad
corporativa
y riesgos



Seguridad
en sectores
estratégicos



Visión internacional
y adaptación local



MÁS INFORMACIÓN E INSCRIPCIÓN

Escanea el QR o accede a:

<https://web.ub.edu/ca/web/estudis/w/masterpropi-202511680>



+34 93 403 96 17



postgrausegur@ub.edu



postgrausegur@gmail.com

*Tu próximo paso
empieza aquí*



Si eres asociado o Patrocinador de ADSI dispones de un 15% de descuento en el importe del curso.

Formación certificada por IMQ Business school

IA Estratégica desde el Consejo

Del criterio a la ventaja competitiva, el único executive programa certificado de gobierno de la IA diseñado por y para consejeros.

La inteligencia artificial está modificando cómo se vende, cómo se atiende al cliente, cómo se calcula el riesgo, como se controla el fraude y cómo se explica una decisión ante reguladores y accionistas.

La cuestión no es si el Consejero debe aprender a programar, es si puede ejercer con rigor su función de supervisión cuando una parte creciente de la compañía decide, recomienda y automatiza mediante modelos que no siempre son visibles para el órgano de administración.

EL PRIMER PROGRAMA QUE CONVIERTE LA IA EN MATERIA DE CONSEJO

Un consejero necesita poder formular exigencias verificables, no basta con "entender la IA". Qué casos de uso existen, qué datos los alimentan, quién responde por sus decisiones, qué riesgos se han clasificado, qué controles son proporcionales, qué métricas se reportan y qué evidencia quedará en acta. Criterio estratégico: Distinguir valor real de ruido de mercado. Aprobar, pausar o exigir cambios a una iniciativa de IA con argumentos estratégicos, regulatorios y económicos. Diligencia documentada: Al Act en vigor, AESIA activa.

La formación certificada es un instrumento de trazabilidad y defensa, no un reconocimiento honorífico. Gobierno operativo: Un sistema operativo de Consejo para la IA: charter, inventario, scoring, KPIs/KRIs y hoja de ruta. Herramientas que se usan desde la siguiente reunión.

Para mayor información en el [siguiente link](#):



CiberseguridadEstratégica

Hay dos clases de Consejeros en 2026: los que ya supervisan el riesgo digital con criterio propio y los que aún confían en que el problema lo resolverá el departamento técnico.

La distancia entre ambos se mide en sanciones evitadas, brechas contenidas y reputación preservada. La transformación digital ha redefinido el mapa de riesgos del Órgano de Administración.

La ciberseguridad ha dejado de ser un asunto operativo del CIO para convertirse en una palanca estratégica que impacta directamente en la continuidad del negocio, la valoración corporativa, el cumplimiento regulatorio y la responsabilidad personal de cada Consejero.

En enero de 2026, el World Economic Forum lo formuló sin matices: la ciberseguridad ha pasado del departamento de IT a la sala del Consejo. El 94 % de los líderes mundiales identifica la Inteligencia Artificial como el principal motor de cambio del riesgo digital, y el 87 % sitúa las vulnerabilidades asociadas a IA como el riesgo de mayor crecimiento de 2025.

ESTE PROGRAMA OFRECE a

Consejeros, Consejeros Delegados, Secretarios del Consejo y miembros de Comités las claves para comprender, supervisar y decidir con criterio en materia de ciberseguridad, gestión de crisis e Inteligencia Artificial. Un itinerario construido sobre casos reales con nombre propio, herramientas inmediatamente aplicables y un claustro que vive el problema cada día. El programa contribuye al cumplimiento de DORA, NIS2 y el Reglamento Europeo de IA, y culmina con la certificación oficial de IMQ Ibérica Business School.

Para mayor información en el [siguiente link](#):

Curso de Director de seguridad integral / Modalidad Online

SOCIOS ADSI

15% OFF

POSGRADO EN DIRECCIÓN DE SEGURIDAD INTEGRAL

UVIC UNIVERSITAT DE VIC
UNIVERSITAT CENTRAL DE CATALUNYA

- Doble TIP – Director y Jefe de Seguridad
- Acreditación Oficial (30 ECTS)
- Más de 30 años formando profesionales

¡Solicita Información ahora!

www.ised.es | Contacto: 932 082 121

- Si cumples el nivel de titulación académica requerida Obtendrás el título de Posgrado por la Universidad de Vic (30ECTS)
- En caso de no contar con una titulación requerida, obtendrás el Certificado de Aprovechamiento del Curso de Dirección de Seguridad Integral (400H) expedido por Universidad de Vic.

ised

ADSI 30 años
asociación de directivos de seguridad integral



UCAV
www.ucavila.es



MÁS INFORMACIÓN



MÁSTER UNIVERSITARIO EN PROMOCIÓN PROFESIONAL PARA LA GESTIÓN DE CRISIS EN SEGURIDAD Y DEFENSA

UNIVERSIDAD CATÓLICA DE ÁVILA

DIRECTOR: Dr. Alberto Barea Vera

CODIRECTOR: Coronel José Luis Calvo Albero





LISA Institute

Becas de Excelencia para analistas de riesgos

En el siguiente enlace se detalla el [Proceso de selección de Becas de Excelencia de LISA Institute](#) para aspirar a una **Beca de 50%** de importe del curso para estos Másteres universitarios:

- [Máster Profesional de Analista de Inteligencia](#)
- [Máster Profesional de Analista Criminal y Criminología Aplicada](#)
- [Máster Profesional de Analista Internacional y Geopolítico](#)
- [Máster Profesional de Analista Estratégico y Prospectivo](#)
- [Máster Profesional en Ciberseguridad, Ciberinteligencia y Ciberdefensa](#)

¿Cómo participar?

[FORMULARIO](#)

Características de los másteres

- **100% online**, prácticos, interactivos e inmersivos.
- Duración: **9 meses** con avance **flexible**.
- **Doble titulación universitaria** emitida por LISA Institute y la Universidad a Distancia de Madrid (UDIMA), con 60 créditos ECTS.
- **Requisitos:** NO hace falta titulación universitaria previa.
- **100% de profesores son profesionales en activo** en empresas e instituciones públicas.
- **Prácticas reales** en unidades de análisis mentorizadas por profesionales en activo.
- Bolsa de Trabajo



Programa formativo en ciberseguridad de Policía Nacional y Universidad de Salamanca

[INFORMACIÓN](#)

**CIBER
WALL**

— ACADEMY —

2026

¡Fórmate con los mejores
cursos en ciberseguridad!

Programa Formativo Gratuito

- Programa formativo de la Policía Nacional en colaboración por la Universidad de Salamanca.
- Plazas limitadas, hasta completar aforo.



UNIVERSIDAD
DE SALAMANCA

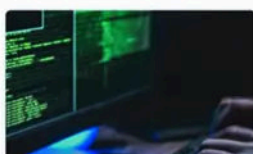


¡Síguenos vía web!



FORMACIÓN ESPECIALIZADA

con la colaboración y el respaldo del
Instituto Universitario Gutiérrez Mellado-UNED



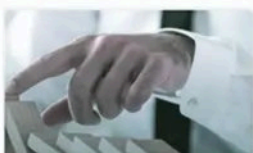
Curso de Ciberseguridad
y preparación del Director
de Seguridad – CISO



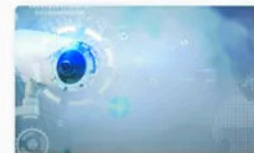
Curso de Seguridad
en Infraestructuras Críticas (DSICE)



Curso de Continuidad de Negocio,
herramienta para la
sostenibilidad de la empresa



Curso de Gestión del Riesgo:
Sistemática y Metodología



Curso de Técnico
en Sistemas de Seguridad

20% descuento
para
asociados
ADSI

**DESCARGAR
INFORMACIÓN**

Más información - formacion@getseguridad.com - 915 001 724

Cursos bonificables para empresas. Desde GET realizan la consulta del crédito disponible, así como la tramitación de la bonificación en caso de realizar algún curso



Curso de Especialista en Seguridad
en Infraestructuras Críticas y
Estratégicas

[Enlace](#)



Curso Superior de Dirección y Gestión
de Seguridad Integral

[Enlace](#)



Master de Formación Permanente en
Cibersecurity Management

[Enlace](#)



Grado en Prevención y Seguridad
Integral (100% a distancia)

[Enlace](#)



Grado de Criminología y Dirección de
Seguridad

[Enlace](#)





Cuadernos de Seguridad
N° 387 Jul/Sep 2026

[Enlace](#)



Revista Seguritecnia
N° 520 Jul/Ago 2026

[Enlace](#)



La Unión Europea quiere ser más.

[Enlace](#)



Hazte socio de ADSI

¿Quieres ser Socio de ADSI – Asociación de Directivos de Seguridad Integral?

Para iniciar el proceso de alta como Asociado, envíe un email a vicepresidente@adsi.pro, indicando nombre y apellidos, una dirección de correo y un teléfono de contacto.

En cuanto recibamos su solicitud le enviaremos el formulario de Solicitud de Admisión.

¿Quién puede ser socio de ADSI?

- Quien esté en posesión de la titulación profesional de Seguridad Privada reconocida por el Ministerio del Interior (T.I.P. de Director de Seguridad, Jefe de Seguridad, Detective Privado o Acreditación de Profesor de Seguridad Privada).
- Todo Directivo de Seguridad que posea, a criterio de la Junta Directiva de la Asociación, una reconocida y meritoria trayectoria dentro del sector.



L'altra veu



SOBRE LA AUTORA

Nacida en el barrio barcelonés del Poble-sec, aunque gerundense de corazón y de raíces, forma parte de esa generación pionera de mujeres que, en la promoción de 1985-1986, cruzaron por primera vez las puertas del Cuerpo de Mossos d'Esquadra. Desde entonces ha recorrido un camino profesional de cuatro décadas, en el que ha ocupado responsabilidades como la jefatura de la Oficina del Portavoz de los Mossos en la Región Policial de Girona o el cargo de subinspectora de la Policía Municipal de Girona.

Más allá de la vida policial, Irene ha cultivado también una faceta humanista y creativa: es graduada en Humanidades por la Universitat Oberta de Catalunya, maestra de reiki e instructora de Qigong. Su vocación literaria le ha valido reconocimientos como el Primer Concurso de Relato Breve Policial Ramon Martí, el

Primer Premio Picasso en Letra (2012), además de quedar finalista en el V Concurso de Cuentos de la Policía de la Generalitat. ■

Autora: Irene Alcalde

A través de la mirada de su protagonista, la novela recorre momentos clave de la Cataluña reciente —como el incendio de Montserrat de 1986, Hipercor, las Ramblas y los Juegos Olímpicos de 1992— junto al reto íntimo de las mujeres que abrieron camino en una profesión diseñada por y para hombres. La historia refleja la tensión entre una exigente carrera masculina y la vida familiar, en plena transformación social e institucional.

L'altra veu no es una crónica, sino un homenaje al legado de aquellas pioneras que rompieron moldes. Fruto del trabajo de siete mossos d'esquadra, la obra visibiliza una perspectiva esencial para modernizar la policía catalana y redefinir la seguridad pública. Como afirma su autora: «Las mujeres no son necesarias en la policía, son la policía».





ADSI

30
auto

**CONECTANDO E
IMPULSANDO**