

Asociación Española de
Ingenieros de Seguridad

02 Mensaje
de la Junta Directiva

03 NOTICIAS **AEINSE**
Asamblea General Ordinaria
SICUR 026

13 NOTICIAS
PATROCINADORES

28 ARTÍCULO
ESPECIALIZADO
Más allá del vídeo: del sistema
de grabación al ecosistema
cognitivo de la instalación
Juan José López Cámara

35 CONOCE A UN **SOCIO**
Cristóbal Martín Ayala

39 **AGENDA**
DEL SECTOR

43 LEÍDO, VISTO
Y OÍDO EN...



Sicur 2026

Punto de encuentro con nuestros
socios y patrocinadores

ADI

AXIS
COMMUNICATIONS

casmar

alhua
TECHNOLOGY

DESICO

DORLET

FFV
GEUTEBRÜCK

IQSIGHT

Hanwha Vision

HTD

Johnson Controls



LANACCESS

30

LEGIC

Sicuralia

SCATI

VIGI
by tp-link

La ingeniería de seguridad y el entorno cambian con el tiempo. Se requiere revisar la visión, misión y valores que hemos mantenido desde la fundación de AEINSE en 2014 para orientar nuestra actividad hacia un espacio de oportunidades para nuestros asociados: los profesionales de la ingeniería de seguridad.

Adecuarnos a los nuevos tiempos...

Damos las gracias a Juan Manuel de Diego, que ha liderado AEINSE entre 2024 y 2026 con energía, decisión y audacia, y que nos sigue apoyando en la Junta Directiva para el periodo 2026-2028.

La nueva Junta Directiva de AEINSE inicia esta etapa recordando el propósito que motivó la creación de la asociación en 2014: reunir a los profesionales de la ingeniería aplicada al sector de la seguridad y contribuir al desarrollo y reconocimiento de esta disciplina.

Desde su origen, AEINSE se creó con la finalidad de:

1. Fomentar el networking y la colaboración entre los profesionales de la ingeniería de seguridad.
2. Potenciar las capacidades de los asociados, promover la excelencia profesional y contribuir a la generación y difusión de conocimiento técnico mediante estudios especializados.
3. Actuar como foro de referencia para el intercambio de ideas en materia de formación, normativa, innovación y mejores prácticas del sector.
4. Impulsar la visibilidad y la adecuada representación de la ingeniería de seguridad dentro del ámbito profesional y empresarial.
5. Promover una visión transversal de la ingeniería de seguridad, integrando a los distintos grupos de interés: empresas de seguridad, ingenierías, fabricantes, usuarios finales, administraciones y centros de formación.

Con este espíritu, la Junta Directiva se compromete a seguir impulsando AEINSE como un espacio de encuentro para la ingeniería de seguridad, en el que los asociados puedan contrastar ideas, debatir argumentos y desarrollar actividades que contribuyan a mejorar sus conocimientos y capacidades profesionales. Aspiramos a consolidar AEINSE como un auténtico laboratorio de ingenieros de seguridad, un entorno de reflexión, aprendizaje y desarrollo profesional.

Un espacio que permita a los asociados crecer como profesionales de la ingeniería de seguridad y aplicar ese conocimiento en los distintos ámbitos del sector.

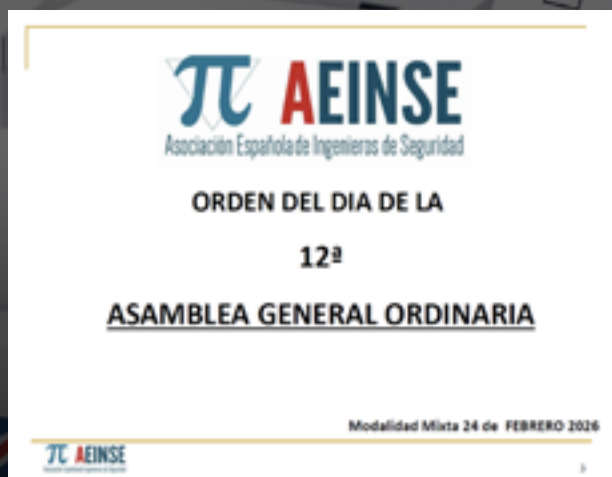
Para avanzar en esta dirección, la Junta Directiva se ha fijado los siguientes objetivos:

- Redactar y presentar para su aprobación el Plan Estratégico de AEINSE.
- Incrementar las actividades de networking de la comunidad AEINSE hasta alcanzar al menos cuatro encuentros anuales.
- Mantener el crecimiento del número de socios que compartan los valores e intereses de la asociación.
- Continuar con la redacción de los boletines de AEINSE y ampliar su difusión dentro y fuera del sector.
- Fomentar la publicación de artículos y aportaciones técnicas por parte de los socios.
- Impulsar el análisis de normas y buenas prácticas mediante la creación de un observatorio de normativa, promoviendo su debate entre los asociados.
- Mantener sesiones formativas sobre temas de actualidad en el ámbito de la ingeniería de seguridad.
- Continuar colaborando en iniciativas de formación relacionadas con la ingeniería de seguridad.
- Redactar y publicar nuevas guías técnicas de actualidad que contribuyan al desarrollo profesional de los asociados y refuercen su liderazgo en el sector.
- Establecer acuerdos con asociaciones del sector para apoyar iniciativas comunes y fomentar las relaciones institucionales.

Confiamos en que esta nueva etapa permita seguir fortaleciendo AEINSE como punto de encuentro de los profesionales de la ingeniería de seguridad y como motor de conocimiento, colaboración y progreso para todo el sector.



NOTICIAS AEINSE



Asamblea General Ordinaria Elección Junta Directiva

AEINSE

24
FEB
2026

El pasado 24 de febrero se celebró la Asamblea General Ordinaria de la Asociación Española de Ingenieros de Seguridad –AEINSE-. Este año incluía el proceso electoral de renovación de la Junta Directiva para un nuevo periodo bianual.

Este año se eligió la tarde del primer día de la **Feria SICUR** y un lugar de celebración muy próximo a la misma para facilitar la asistencia a los socios que residen fuera de Madrid. Por otra parte, se celebró en modalidad mixta, presencial y telemática.

Asistieron presencialmente más del 30% de los socios, a los que sumando la delegación de voto de otros socios se superó el tercio de socios necesario para votar y ratificar los acuerdos alcanzados. Se aprobó el acta de la asamblea de 2025, se ratificaron los socios incorporados el pasado año, se presentó el resumen de lo realizado en 2025 y se aprobaron las cuentas del ejercicio. Finalmente se pasó a la votación de la nueva candidatura para la Junta Directiva.

Especial reseña tuvo el desarrollo del **III Congreso de Ingeniería de Seguridad** celebrado en octubre con la participación de más de 130 asistentes.



NOTICIAS AEINSE



Respecto a las redes sociales, tuvimos casi 5.000 impresiones en 2025 y más de 900 seguidores. El **chat Compartech** estuvo particularmente activo, consolidándose como una herramienta de intercambio de información técnica y ayuda entre los asociados.

En cuanto a nuestros patrocinadores, se comunicó la baja de **Dormakaba** y la incorporación de **ADI** y **VIGI by tp-link**.

Por último, se llevó a cabo la votación para elegir la nueva Junta directiva, en la que fue respaldada por la totalidad de participantes la única candidatura presentada que lidera **Iván Ballesteros** como presidente, seguido de **Juan Manuel de Diego** como vicepresidente. Iván presentó seguidamente la propuesta de organización, objetivos y acciones para esta nueva etapa.

Finalmente, la jornada concluyó con una cena a la que se incorporaron nuestros patrocinadores. Cena informal que nos permitió dialogar, conocernos mejor y hablar de proyectos futuros.

ELECCION JUNTA DIRECTIVA

La nueva Junta Directiva mantiene algunos de los socios de la etapa anterior, en el mismo o en otro puesto, e incorpora nuevos, quedando constituida por:

Presidente:	Iván Ballesteros
Vicepresidente:	Juan Manuel de Diego
Secretario y Cumplimiento:	Pedro de la Hoz
Tesorera:	María del Carmen Sánchez
Vocal de Publicaciones:	Carlos Martínez
Vocal de Marketing y Comunicación:	Juan José Hernández
Vocal para Socios y Ciber:	Raúl Aguilera
Vocal de Buenas prácticas y Normas	Antonio Manzanares
Vocal de Patrocinadores:	José Luís Fernández Pallarés
Vocal de Relaciones institucionales:	Enrique Bilbao
Vocal de Formación:	Ramón Segarra

NOTICIAS AEINSE

Damos la bienvenida
a nuestro grupo de patrocinadores
a **VIGI by tp Link**



VIGI by TP-Link nuevo patrocinador de AEINSE

VIGI by TP-Link se caracteriza por la integración nativa de sus soluciones de video IP en la plataforma profesional de TP-Link para la gestión de infraestructuras de red. Lo que permite diseñar soluciones de videovigilancia altamente fiables, escalables y eficientes, donde red y seguridad trabajan de forma conjunta para garantizar el rendimiento necesario en cada proyecto.

La combinación de **VIGI** y **Omada** facilita una gestión unificada de la videovigilancia y la red desde una única plataforma, simplificando la operación, el mantenimiento y la supervisión de las instalaciones aportando un valor diferencial clave para ingenierías, integradores y responsables de seguridad.

A través de esta colaboración, **VIGI by TP-Link** y **AEINSE** trabajarán conjuntamente en acciones de divulgación técnica, formación y comunicación, así como en la participación en jornadas, eventos y contenidos especializados.

Confiamos en que su presencia en **AEINSE** facilite la comunicación con nuestros socios ingenieros y reafirme su apuesta a largo plazo por el mercado de la seguridad profesional, poniendo al servicio de ingenierías, integradores y empresas su experiencia tecnológica y la innovación de **VIGI**, una gama de soluciones de videovigilancia IP pensadas para responder a las necesidades reales del entorno empresarial actual.

Desde estas páginas queremos agradecer el apoyo, confianza y colaboración manifestadas hacia nuestra Asociación.

[+Conocer más de VIGI by TP-Link](#) 

ADI Global se incorpora
a nuestro grupo de patrocinadores.
Conste aquí nuestro agradecimiento y bienvenida.



ADI nuevo patrocinador de AEINSE

ADI es un distribuidor líder en nuestro mercado por sus soluciones probadas y los años de experiencia en el sector, lo que permite a los integradores operar de forma más eficiente y ofrecer servicios fiables a sus clientes.

ADI ofrece el mayor catálogo del mercado en productos de seguridad y bajo voltaje, disponible para recogida en almacén o entrega en las instalaciones del cliente. También cuenta con página web para gestionar todas las compras, pudiendo navegar y entre más de 6.000 productos, de más de 700 proveedores y fabricantes.

El personal de ADI es experto en el producto y soluciones que comercializan, con más de cuarenta años de experiencia en el sector; y están disponibles para ofrecer asesoramiento on line y ayudar en el diseño de sistemas, la selección de productos y el soporte técnico.

A través del acuerdo de colaboración ADI y AEINSE lograremos contribuir a la divulgación de los productos, formación y difusión de conocimiento, así en la participación en jornadas, eventos y contenidos especializados.

Desde estas páginas agradecemos su colaboración, confiando en que su presencia en nuestra Asociación sea fructífera para la difusión y consolidación de su imagen e intereses y, también para nuestros socios.

[+Conocer más de ADI](#) 



NOTICIAS AEINSE

Como en la anterior edición de SICUR, Aeinse estuvo presente en el espacio SICUR Cyber, organizado por las revistas Seguritecnia y Red Seguridad en colaboración con la Fundación Borrerdá. Una vez más resultó un éxito en asistencia de profesionales, calidad de los ponentes y contenidos



Presencia de AEINSE en SICUR Cyber

A lo largo de tres jornadas, 24, 25 y 26 de febrero, más de treinta ponentes, del sector público y privado, en ponencias y mesas redondas abordaron y debatieron asuntos relacionados con la convergencia de las segundades y la ciberseguridad en los aspectos de las comunicaciones, normativa, videovigilancia, control de accesos, detección de intrusión, centralización y gestión, cibercrimen, etc.

En la primera jornada intervinieron nuestros socios **Patricio Delorme, Raúl Aguilera y Alfonso Bilbao**.

NOTICIAS AEINSE



Patricio Delorme presentó la ponencia “**Ciberseguridad en las Credenciales: Un Pilar Estratégico para la Gestión de Identidades Seguras**”

La tecnología de credenciales ha experimentado una evolución radical en las últimas cinco décadas. Reflejando la convergencia entre seguridad física, seguridad electrónica y ciberseguridad. Durante la última década, la industria ha incorporado tecnologías que elevan los niveles de protección de las credenciales:

- Encriptación avanzada para resguardar los datos almacenados y transmitidos.
- Mecanismos de firma digital, que garantizan la autenticidad y evitan la manipulación de la información.
- Vinculación criptográfica entre hardware y software, lo que dificulta la clonación y asegura que la credencial solo funcione con dispositivos autorizados.
- Ante amenazas cada vez más sofisticadas hay que priorizar soluciones que garanticen confidencialidad, integridad y disponibilidad tanto del sistema de control como de los datos asociados a la identidad del usuario.

La ciberseguridad aplicada a credenciales es un requisito indispensable para mitigar riesgos, cumplir con normativas emergentes y garantizar operaciones confiables.



Raúl Aguilera disertó sobre “**Las empresas necesitan una resiliencia híbrida**”.

La ponencia de Raúl Aguilera explora cómo la seguridad puede evolucionar de un coste operativo tradicional a una auténtica palanca estratégica para las organizaciones. A través del concepto de seguridad híbrida, plantea optimizar la presencia física mediante supervisión remota, tecnología inteligente y mayor integración con la ciberseguridad. Este enfoque permite liberar recursos del modelo presencial intensivo para invertir en innovación, resiliencia y cumplimiento normativo, especialmente ante nuevos marcos regulatorios como la directiva NIS2. El resultado es un modelo de seguridad más eficiente, escalable y preparado para los retos digitales actuales.



La segunda jornada fue especialmente atendida por miembros de nuestra Asociación: **Antonio Manzanares, Raúl Porras y Alfonso Bilbao**.

La sesión Comenzó por la ponencia “**Ciberseguridad e integración IoT. ¿Cómo influye?**” de **Antonio Manzanares** que ofreció una ponencia centrada en los retos que plantea la incorporación masiva de dispositivos conectados en entornos industriales.

Durante la sesión se analizó cómo el crecimiento del Internet de las Cosas, que superará los 40.000 millones de dispositivos en la próxima década, está ampliando

NOTICIAS AEINSE

la superficie de ataque y transformando el modelo tradicional de seguridad.

La exposición abordó los nuevos vectores de riesgo en infraestructuras IT/OT, la importancia de la segmentación y la monitorización de redes industriales, y el impacto del nuevo marco regulatorio europeo, destacando la necesidad de aplicar principios de “seguridad por diseño” para garantizar sistemas industriales más resilientes.



Raúl Porras disertó sobre el “**Nuevo enfoque de la ciberseguridad aplicado a los equipos de seguridad física**”.

Comenzó con una rotunda afirmación: “*La seguridad física ya no es segura sin ciberseguridad*”. Con esta idea, explicó cómo la integración de tecnologías IT, OT e IoT ha transformado los sistemas de seguridad en ecosistemas ciberfísicos interconectados, expuestos a amenazas híbridas que combinan ataques físicos y cibernéticos.

Durante su intervención, destacó la necesidad de romper la tradicional separación entre seguridad física y ciberseguridad mediante un enfoque unificado de gestión de riesgos. Además, subrayó que el nuevo marco regulatorio —como ENS, NIS2 o la Cyber Resilience Act— exige incorporar la ciberseguridad desde el diseño y durante todo el ciclo de vida de las soluciones.

Finalmente, y para cerrar la jornada matinal, se celebró la mesa redonda del Foro de Ciberseguridad Nacional en torno a la recientemente publicada “**Guía sobre la gestión de la ciberseguridad de los sistemas de seguridad física. Recomendaciones y casos de uso**”.



La mesa estuvo constituida por **Mónica Mateos** (Departamento de Seguridad Nacional), **Estefanía Linares** (Centro Criptológico Nacional, del CNI) y tres expertos redactores de la Guía: **Mariano Benito**, **Ricardo López** y **Alfonso Bilbao**.

La mesa, moderada por **Enrique González** de la Fundación Borredá, comentó desde distintos puntos de vista los trabajos que llevaron a la elaboración de la Guía, sus características y los futuros trabajos a desarrollar próximamente en esa línea.

Alfonso Bilbao comentó especialmente la oportunidad de comunicación fructífera que se dio entre especialistas de Seguridad Física y Ciberseguridad, el hallazgo de un lenguaje común, y la forma práctica de su utilización por los ingenieros de Seguridad Física.

Durante la tercera jornada, tuvieron lugar dos mesas redondas en las que participaron nuestros socios **Iván Ballesteros** y **Enrique Bilbao** (ambos en representación de ASIS).

NOTICIAS AEINSE

Mesa “**Biometría ¿es una medida de ciberseguridad?**”, moderada por **Cesar Álvarez** y constituida por **Alberto Tovar, Iván Ballesteros, Íñigo Ugalde y Carlos Vazquez**.



La Mesa tuvo el propósito de introducir la Biometría con Fines de Seguridad como una propuesta complementaria a iniciativa de AES, y respaldada por CEUSS, FORO EFITEC, AEINSE y ASIS.

Se formularon a debate dos preguntas. ¿Cuál fue el impacto de la Guía de la AEDP de 23/11/23 Guía sobre tratamiento de control de presencia mediante sistemas biométricos, AEPD el 23 de Noviembre de 2023 y ¿Cómo se gestionaron las consultas sobre la Guía? ¿Es necesaria la biometría?

Ivan enfatizó en la necesidad de hacer coincidir las definiciones jurídicas y las técnicas. Por ejemplo; el marco de la protección de datos emplea una única definición “dato biométrico” la norma UNE-EN ISO IEC 2382-17 emplea 198 definiciones. También explicó los principales términos empleados en biometría; los atributos biométricos, la plantilla biométrica cifrada, la comparación cifrada para el reconocimiento, entre otros términos.

La mesa concluyó con una apuesta por la colaboración público privada.

Ivan Ballesteros propuso un *think tank* de biometría que apoye el desarrollo del sector y que aporte garantías en la protección de datos.



Finalmente, la Mesa de Ingeniería de Seguridad “**La convergencia físico digital. Del riesgo al control**” con la participación de **Enrique Bilbao**, en representación de ASIS, **Jorge Noguerales** responsable del área de Ciberseguridad de AES y **Juan Carlos Fúnez** Responsable IT de ACAES.

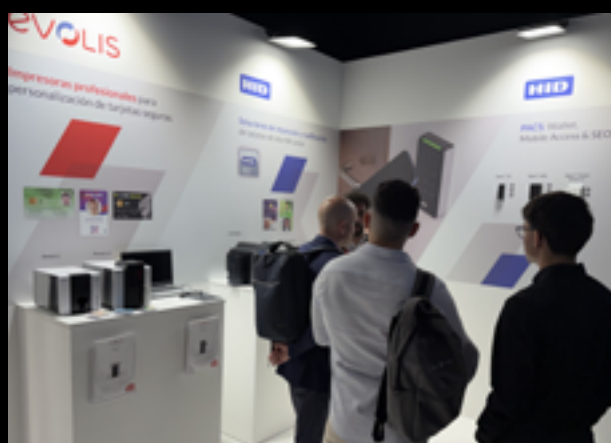
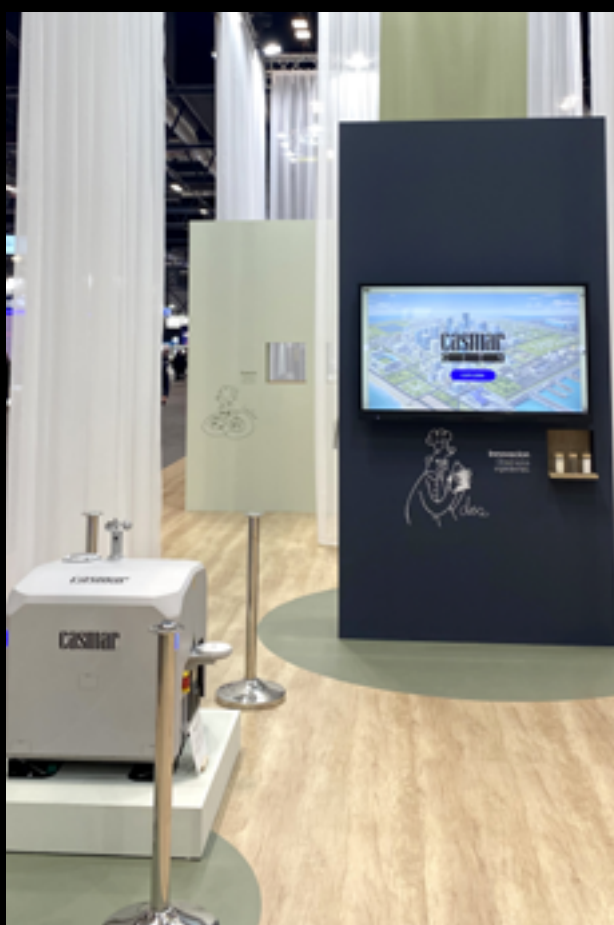
Enrique defendió la importancia de que los ingenieros se basen en estándares internacionales y en mejores prácticas (como las de las guías de AEINSE), para que la ingeniería colabore en una mejor gestión de los riesgos.

Tanto **Jorge** como presentaron la visión de AES y de ACAES, respectivamente, sobre qué activos, amenazas y controles de ciberseguridad serían más adecuados para la gestión de los riesgos físico-digitales.

NOTICIAS AEINSE



2026 en imágenes...



NOTICIAS AEINSE



ADI

AXIS
COMMUNICATIONS

Casmar
Comunidad en la Seguridad

alhua
TECHNOLOGY

DESICO®

DORLET

ff VIDEOSISTEMAS
FFV
GEUTEBRÜCK

HID

IQSIGHT

Hanwha Vision

Johnson
Controls

LANACCESS 30

LEGIC

Sicuralia
Sistemas

VIGI
by tp-link

SCATI

AEINSE
Asociación Española de
Ingenieros de Seguridad



SICUR 2026

IQSIGHT refuerza su apuesta por la seguridad inteligente

IQSIGHT

La compañía tecnológica IQSIGHT, evolución de Bosch Video Systems, ha tenido una destacada participación en SICUR 2026, , donde presentó sus últimas soluciones orientadas a impulsar la gestión de video basada en inteligencia y datos.

El equipo de la compañía mostró a clientes y socios del mercado ibérico varias de sus innovaciones tecnológicas. Entre ellas **IVA Pro Context**, una solución de analítica de vídeo impulsada por inteligencia artificial generativa, diseñada para transformar grandes volúmenes de datos visuales en información útil para la toma de decisiones.

Asimismo, **IQSIGHT** contó con el socio tecnológico Genetec. Conjuntamente mostraron soluciones para entornos de alto riesgo, desarrolladas específicamente para infraestructuras críticas y escenarios operativos complejos. **Genetec** presentó sus soluciones que permiten crear flujos de trabajo de seguridad unificados y más eficientes dentro de los sistemas de gestión de seguridad.

Otro de los focos de la participación de la empresa fue su **nuevo portafolio de cámaras**, compuesto por sensores de video de última generación en cumplimiento de los últimos estándares de ciberseguridad NDAA, y fabricados en Europa, como cámaras multisensor con PTZ, cámara dual y el nuevo rango CPP16.

En palabras de Laura Alcázar (Directora Comercial de España y Portugal) *“Con IQSIGHT abrimos una nueva era dentro de la inteligencia visual de la mano de las tecnologías de futuro y SICUR ha sido la plataforma de lanzamiento perfecta para nuestras nuevas aportaciones a la industria”.*

[+información](#) 



British Airways refuerza la seguridad de su base de Heathrow

con una solución integrada de Johnson Controls Security Products

British Airways Engineering ha completado una transformación integral de seguridad en su base de mantenimiento en Heathrow mediante una solución avanzada diseñada e integrada por Johnson Controls Security Products.

El proyecto unifica inteligencia artificial, detección por radar y el sistema de control de accesos aeroportuario **CEM Systems AC2000**, líder en el sector con más de 35 años de despliegue en infraestructuras críticas.

La nueva plataforma combina más de 200 cámaras Illustra con analítica de IA, radares perimetrales integrados con cámaras PTZ y el renovado AC2000 Airport. Todo gestionado desde el software unificado Victor y los grabadores VideoEdge. Esta integración permite supervisión en tiempo real de zonas aire-tierra, hangares, viales y perímetros, mejorando la precisión en la detección de amenazas y reduciendo falsas alarmas.

El proyecto incluye uno de los primeros centros de control aeroportuarios del Reino Unido con IA integrada, que aporta búsqueda forense avanzada, verificación inteligente de personal y una operativa más eficiente y preventiva.

Con esta implementación, British Airways Engineering adopta un modelo de seguridad más inteligente, sostenible y preparado para el futuro, impulsado por la tecnología de **Johnson Controls Security Products**.



Lanaccess presentó en SICUR 2026 una tecnología de videovigilancia más cibersegura y resiliente

Durante su participación en la feria, Lanaccess mostró sus últimos avances en seguridad y puso en valor las certificaciones que reafirman su compromiso con la ciberseguridad, como la ENS Categoría Alta, la ISO 27001 y la NIS 2, expedidas por Adok (acreditado por la ENAC) o el CCN, así como el cumplimiento de normativas como DORA, NDAA y C-TPAT. Además, este año dará un paso más para alcanzar la certificación LINCE.

Este posicionamiento se sustenta en una infraestructura y procesos preparados para entornos altamente exigentes, donde la resiliencia, la trazabilidad y la protección de los datos son requisitos imprescindibles.

La compañía presentó la nueva familia de videograbadores NXT, una nueva gama que duplica la capacidad del modelo anterior, ofrece más potencia, mayor capacidad de procesamiento, una arquitectura más resiliente y permite gestionar hasta 100 cámaras.

Los nuevos equipos incorporan un sistema operativo a medida, firmware desarrollado íntegramente por su equipo de I+D+i y hardware específico para la gestión de vídeo.

SICUR 2026 fue, además, el escenario elegido para celebrar el **30 aniversario de Lanaccess**, una trayectoria que refuerza su posicionamiento en el desarrollo y la fabricación en Europa de soluciones de videovigilancia para sectores críticos y entornos exigentes.

[+información](#) 



SM 6300

El Módulo de Seguridad Interoperable para Lectores de Control de Acceso

El SM-6300 es compatible con Bluetooth Low Energy y comunicación de campo cercano (NFC) y cumple con altos requisitos de seguridad gracias a su Elemento Secreto (SE) integrado y certificado como ancla de seguridad. El SE a prueba de manipulaciones se utiliza para ejecutar código crítico para la seguridad y almacenar claves de aplicación específicas del cliente.

Sistema-en-paquete

Construido como un sistema en paquete, integra diversos componentes electrónicos, como condensadores, resistencias y cristales, además del SE y los componentes para la comunicación a través de NFC y Bluetooth. De este modo, el **SM-6300** puede reducir hasta en un 25% los componentes necesarios para una placa lectora.

Ventajas

- **Lee todos los estándares RFID relevantes a nivel mundial, incluidos advant, prime, neon, NXP MIFARE, HID iCLASS, LEGIC MTSC, Inside Secure, Sony Felica y la serie ST SR. Compatible con los licenciarios de Apple que implementan ECP 2.0 para leer credenciales NFC en Apple Wallet.**
- **Elemento seguro EAL5+ para requisitos de seguridad elevados.**
- **Preparado para el futuro gracias a las actualizaciones de firmware OTA y la compatibilidad con versiones anteriores.**
- **Consumo muy bajo, óptimo para funcionamiento con batería, detección de tapa y activación RFID.**

SCATI Protege las Pirámides de Guiza, el Templo de Luxor y el Gran Museo Egipcio con seguridad inteligente

Egipto ha reforzado la seguridad de algunos de sus enclaves patrimoniales más emblemáticos con soluciones inteligentes desarrolladas por SCATI. Entre ellos figuran las Pirámides de Guiza y el Templo de Luxor, donde se ha desplegado una avanzada infraestructura de videovigilancia para proteger perímetros, accesos, recorridos turísticos y zonas interiores sensibles en entornos arqueológicos sometidos a altas temperaturas, polvo y grandes flujos de visitantes.

En **Guiza**, la solución cubre perímetro, accesos y recorridos turísticos, así como zonas sensibles del interior de las pirámides, mediante distintas tipologías de cámaras y supervisión centralizada 24/7.

En **Luxor**, la modernización ha incluido 232 cámaras térmicas y de espectro dual, además de la migración de tecnología analógica a IP para mejorar la calidad de imagen, la trazabilidad y la gestión operativa.

A estos proyectos se suma la protección del **edificio Solar Boat del Gran Museo Egipcio**, donde SCATI

ha implantado una solución integral con 216 cámaras, 96 terminales de control de accesos y una plataforma centralizada de integración para salvaguardar el **barco funerario de Khufu de 4600 años de antigüedad** y otras zonas críticas del edificio con una respuesta rápida ante cualquier incidente.

[+información Guiza y Luxor](#)

[+información Khufu](#)





InvisiFence Plus:

Cable enterrado con sensores sísmicos inteligentes

Sicuralia presenta InvisiFence Plus, el primer y único sistema de cable sensor enterrado totalmente digital para seguridad perimetral. Esta solución avanzada crea un anillo de protección invisible mediante sensores sísmicos inteligentes enterrados a 40 cm, resultando imposible de saltar o sobrepasar mediante excavación sin ser detectado.

A diferencia de las tecnologías analógicas, **InvisiFence Plus** ofrece procesamiento distribuido donde cada sensor incluye un procesador DSP para el análisis local de señales. Gracias a sus algoritmos de auto-aprendizaje adaptativo, el sistema clasifica con precisión amenazas como pasos, vehículos o excavaciones, garantizando una detección fiable y libre de falsas alarmas. Cabe destacar que el sistema puede cubrir hasta 400 m de perímetro desde un único punto de control y ubicar al intruso con una precisión de hasta 3 metros.

Diseñado bajo estándares militares con certificación IP68, opera fiablemente entre -40°C y 85°C, siendo inmune a condiciones climáticas extremas e interferencias de vallas cercanas. Su diseño modular facilita la integración con sistemas de alarma y software VMS.

Optimice la protección de sus infraestructuras críticas con tecnología de vanguardia. Le invitamos a conectar con la web de Sicuralia para conocer más sobre InvisiFence Plus y otras soluciones de seguridad perimetral.

[+información](#) 

NOTICIAS PATROCINADORES



VIGI by tp-link lleva la Gestión Unificada de las Redes y Seguridad a SICUR 2026

TP-Link presenta en SICUR 2026 su solución VIGI by TP-Link, concebida como un sistema que trasciende la videovigilancia tradicional para convertirse en una auténtica herramienta de gestión operativa. Gracias a su analítica basada en Inteligencia Artificial, no solo registra eventos: los interpreta, prioriza y contextualiza, transformando datos en información accionable que facilita la toma de decisiones en tiempo real y mejora la eficiencia de los equipos de seguridad.

Entre sus funciones destacan la detección de intrusiones, objetos abandonados, cruces de línea y comportamientos anómalos, incorporando mecanismos avanzados de filtrado que reducen de forma significativa las falsas alarmas.

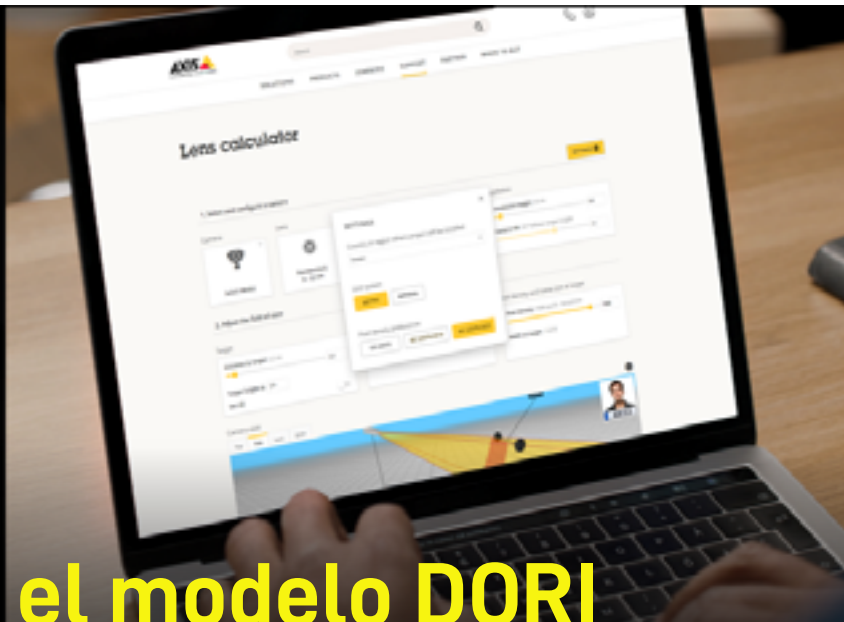
El sistema permite búsquedas rápidas e inteligentes de datos, definición de zonas de interés y configuración granular de reglas de alerta, adaptándose a entornos operativos diversos y exigentes.

Compatible con ONVIF y conforme a la normativa NDAA, su catálogo incluye cámaras Bullet, Turret, Dome, PTZ, Fisheye y panorámicas, así como opcio-

nes con alimentación solar o conectividad 4G para ubicaciones remotas.

La compañía mostró también Omada Central, su plataforma cloud de gestión unificada para redes y videovigilancia. Diseñada para entornos distribuidos y de misión crítica, permite supervisar, configurar y optimizar infraestructuras desde una única interfaz, aportando visibilidad en tiempo real, trazabilidad completa del estado de la red y reducción de los tiempos de respuesta ante cualquier incidencia operativa.

[+información](#) 



IEC 62676 4 y el modelo DORI

cómo Axis impulsa un diseño de videovigilancia más preciso

La norma IEC 62676 4 sigue siendo una referencia clave para diseñar sistemas de videovigilancia basados en niveles de detalle visual. Su conocido modelo DORI —Detección, Observación, Reconocimiento e Identificación— ha servido durante años para definir expectativas realistas de imagen y asegurar que cada cámara cumple una función concreta.

Aunque la nueva versión de la norma evoluciona hacia un enfoque más amplio de “tareas visuales”, DORI continúa siendo la base conceptual para proyectos que requieren simplicidad, claridad y resultados medibles.

En este contexto, **Axis Communications** juega un papel protagonista. La compañía no solo incorpora DORI y la nueva IEC 62676 4:2025 en su filosofía de diseño, sino que ofrece herramientas que permiten aplicarlo de forma precisa.

Su **Lens Calculator** es el primer configurador capaz de alternar entre la norma antigua y la nueva, facilitando la selección de la lente y la densidad de píxeles adecuada para cada objetivo operativo.

Además, soluciones como **AXIS Site Designer** permiten introducir requisitos específicos de pixelado y traducirlos en configuraciones técnicas coherentes para integradores y clientes.

Gracias a este soporte, **Axis** ayuda a garantizar que los proyectos de videovigilancia se diseñen con criterios sólidos, datos verificables y una alineación total con los estándares internacionales.

Diseña tu sistema conforme a la IEC 62676-4 con las herramientas de **Axis**. Calcula la densidad de píxeles adecuada y elige la óptica perfecta con **Axis Lens Calculator**.

[+información](#) 



Casnova brilla en SICUR: uniendo legado y futuro

En SICUR, el Grupo Casnova hizo su gran presentación, mostrando la unión de Casmar y Desico bajo un mismo proyecto. La puesta en escena reflejó la identidad y la ambición del grupo, y su stand marcó el inicio de la feria con fuerza, recibiendo una gran acogida y transmitiendo la ilusión de reencontrarse con clientes y profesionales del sector.

Casnova nace de la experiencia y los valores de la familia Castro, referente en seguridad en España durante más de 45 años, combinando un sólido legado con una visión de innovación, atrevimiento y compromiso con el futuro. El proyecto busca impulsar iniciativas colaborativas y fomentar un crecimiento equilibrado, independiente y sostenible de sus dos empresas, **Casmar** y **Desico**, cada una con más de cuatro décadas de excelencia.

Como su nombre sugiere, **Casnova** representa el equilibrio perfecto entre tradición y transformación.

En SICUR quedó claro que esta unión es mucho más que una fusión: es un nuevo camino lleno de oportunidades y un debut que ya puede considerarse todo un éxito.



Dahua Technology participa en SICUR 2026 junto a sus distribuidores



Dahua Technology participó en la feria SICUR 2026 a través de varios de sus distribuidores en España y Portugal, donde se presentaron algunas de sus soluciones más innovadoras en el ámbito de la seguridad electrónica y el vídeo inteligente.

Durante el evento se mostraron diferentes tecnologías y productos, entre ellos la solución Xinghan, sistemas de alarma, la tecnología de imagen WizColor, así como soluciones para la gestión del tráfico y la movilidad inteligente.

Los visitantes pudieron conocer de cerca distintas aplicaciones orientadas a mejorar la seguridad y la gestión eficiente de entornos urbanos, infraestructuras críticas y espacios comerciales.

Además, se presentaron soluciones basadas en inteligencia artificial que permiten optimizar la monitorización, el análisis de vídeo y la toma de decisiones en tiempo real, contribuyendo a aumentar la eficiencia operativa y reducir los tiempos de respuesta ante posibles incidentes.

La presencia en SICUR permitió a Dahua y a sus partners compartir con clientes e integradores las últimas innovaciones tecnológicas y seguir reforzando su compromiso con el desarrollo del sector de la seguridad en el mercado ibérico.



Desico – Grupo CASNOVA

ha presentado en esta edición de SICUR
sus últimas novedades y desarrollos



VIGIPLUS PSIM 11. Nueva versión de la suite PSIM Vigiplus que incorpora los requisitos avanzados de ciberseguridad que requieren nuestros clientes y que permiten cumplir con las certificaciones más exigentes. Esta solución se encuentra en fase de ensayos de laboratorio para obtener la certificación LINCE del Centro Criptológico Nacional (CCN).

Módulo de mantenimiento:

Nuevo módulo que facilita la gestión del mantenimiento desde un único interfaz, aportando eficacia y permitiendo la digitalización de un proceso tan crítico como el mantenimiento.

Cientes web:

Cientes web que permiten conectarse al sistema **Vigiplus** desde cualquier punto, utilizando solo un navegador. Se dispone de un cliente web **Vigiplus Alarmas** y de un Cliente Web **Vigiplus accesos**, diseñados para el uso desde terminales móviles y desde PC's.

Servicios avanzados de ciberseguridad:

Desico también ha anunciado el lanzamiento de nuevos servicios de soporte que permitirán la implantación de instalaciones que cumplan con las normativas de ciberseguridad (ENS, NIS2, CRA, etc.).

Los nuevos sistemas de Seguridad contarán desde ahora con el soporte de un equipo de gestión de vulnerabilidades que permitirá la operación segura en todo el ciclo de vida.

Muchas gracias a todos los clientes y visitantes que os habéis acercado a conocer de primera mano todas estas novedades.



DORLET refuerza en SICUR su liderazgo en Seguridad Integral Certificada



DORLET cierra la última edición de SICUR con un balance muy positivo. Durante el evento, la compañía tuvo la oportunidad de compartir su visión tecnológica y su apuesta por soluciones cada vez más integradas, capaces de responder a los nuevos retos de las infraestructuras críticas.

Uno de los hitos más relevantes fue la presentación de **SHeld**, primera y única solución de control de accesos cibersegura incluida en el Catálogo de Productos y Servicios TIC (CPSTIC), herramienta avalada por el Centro Criptológico Nacional (CCN). La incorporación de la solución SHeld en el catálogo no solo demuestra un óptimo desempeño incluso en situaciones complejas, sino que también otorga garantías en procesos de licitación y auditorías.

Además, SICUR fue el escenario elegido para presentar oficialmente **ODISEE, el nuevo Open Physical Security Software de DORLET**. Esta plataforma abierta de seguridad suscitó un notable interés entre los profesionales del sector por su capacidad para integrar diferentes tecnologías y simplificar la gestión operativa de los sistemas de seguridad en entornos cada vez más complejos.

En definitiva, SICUR 2026 ha sido clave para reforzar la confianza de clientes y partners, presentar innovaciones tecnológicas y abrir nuevas oportunidades de colaboración... Y esto no es sino una muestra de que **DORLET** avanza en la dirección correcta.



Sistemas de Grabación GEUTEBRÜCK

Los sistemas de grabación Geutebrück obtienen la certificación ISO 27001:Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información

En un entorno donde la ciberseguridad es un requisito estratégico, tenemos el orgullo de informarles que nuestros sistemas de grabación han alcanzado un hito clave al certificarse bajo la norma ISO 27001, referente internacional en gestión de la seguridad de la información.

Esta certificación no solo valida procesos, sino que es un compromiso integral con la protección de datos frente a accesos no autorizados, sabotaje o espionaje.

La seguridad está integrada desde el diseño, mediante un Ciclo de Vida de Desarrollo Seguro (SDL) que contempla análisis de amenazas, pruebas de penetración, codificación segura y gestión sistemática de parches.

A nivel técnico, los sistemas incorporan cifrado avanzado AES-256, comunicaciones seguras TLS/HTTPS y protección robusta de contraseñas mediante algoritmos como SHA-256 y PBKDF2. Además, su base de datos propietaria y las opciones de cifrado de disco refuerzan la protección de la información en reposo y en tránsito.

Para nuestros clientes, esta certificación representa una garantía adicional de fiabilidad, resiliencia y cumplimiento normativo.

En un mercado altamente competitivo, contar con soluciones certificadas ISO 27001 supone una ventaja diferencial clara y un respaldo sólido para proyectos en entornos críticos e infraestructuras sensibles.

[+información](#) 





Hanwha Vision

Por qué puede confiar en nuestra Inteligencia Artificial

En Hanwha Vision creemos que la innovación sin responsabilidad se convierte en un riesgo. Por ello, nos enorgullece anunciar la obtención de la Certificación ISO/IEC 42001, el primer estándar internacional certificable para un Sistema de Gestión de Inteligencia Artificial (AIMS).

La comunidad internacional avanza para garantizar que la Inteligencia Artificial sea una fuerza positiva. Con la entrada en vigor del Reglamento Europeo de Inteligencia Artificial, la primera normativa integral sobre esta tecnología, el vacío regulatorio está desapareciendo.

Para mantener este alto estándar, hemos institucionalizado el Consejo de Inteligencia Artificial Responsable.

Este órgano establece normas internas de cumplimiento y supervisa el rendimiento de la Inteligencia Artificial, asegurando que cada innovación esté basada en principios éticos fundamentales:

- Seguridad y fiabilidad.
- Privacidad y dignidad humana.
- Transparencia y equidad

De los principios a la práctica

En **Hanwha Vision**, nuestro marco de gestión de la Inteligencia Artificial se traduce en requisitos estrictos que guían su desarrollo e implementación.

- Privacidad desde el diseño
- Eliminación de sesgos algorítmicos, evitando resultados discriminatorios
- Integridad y seguridad de los datos.
- Transparencia y capacidad de explicación.

Nuestro marco asegura procesos auditables y transparentes

El sector de la videovigilancia entra en una nueva etapa en la que las especificaciones técnicas ya no son el único indicador de excelencia. A medida que la Inteligencia Artificial adquiere mayor autonomía, la verdadera ventaja competitiva reside en la responsabilidad.

Hanwha Vision es un partner en el que puede confiar.

NOTICIAS PATROCINADORES



Transparent Gateway HID® M1™

¿Qué tal si pudiera cumplir con los requisitos de una arquitectura donde la seguridad esté depositada en la controladora en lugar de la lectora sin reemplazar lo que funciona?

Nuestro nuevo **HID® M1™ Transparent Gateway** funciona junto con su infraestructura de control de acceso existente. Instalado entre sus lectoras y el controlador OSDP, M1 ofrece una arquitectura modernizada y conforme a la normativa, preservando tu inversión actual, brindando cumplimiento de arquitectura transparente sin necesidad de quitar y reemplazar el equipamiento existente.

La innovación incluida en el M1, está diseñada para cumplir con estrictos estándares regulatorios, como la Certificación de Seguridad de Primer Nivel (CSPN) de la Agencia Nacional de Ciberseguridad Francesa (ANSSI), al tiempo que ofrece una integración perfecta, un rendimiento superior y una escalabilidad excepcional para entornos de alta seguridad.

El Gateway M1 provee:

- Cumple con los estándares de ANSSI CSPN. Las organizaciones mantienen control exclusivo sobre las claves de cifrado. Proporciona administración centralizada de claves con HID Linq Key Manager.
- Funciona con cualquier controlador OSDP. Conserva la infraestructura de control de acceso existente sin interrupciones ni tiempos de inactividad.
- Solución adaptativa con un procesador SEM (Sistema En Módulo) con capacidad de IA, listo para futuros casos de uso inteligente. Admite hasta ocho lectores transparentes por módulo I/O.

[+información](#) 



MÁS ALLÁ DEL VÍDEO...

DEL SISTEMA DE GRABACIÓN AL ECOSISTEMA COGNITIVO DE LA INSTALACIÓN

Juan José
López Cámara

Especialista en sistemas de vídeo IP,
arquitectura e integración
en infraestructuras críticas.

EL PARADIGMA DE LA VIDEOVIGILANCIA TRADICIONAL, BASADO EN EL REGISTRO PASIVO DE IMÁGENES PARA SU POSTERIOR REVISIÓN FORENSE, ESTÁ SIENDO SUSTITUIDO POR EL CONCEPTO DE SISTEMA COGNITIVO DE INSTALACIÓN. ESTE ARTÍCULO TÉCNICO ANALIZA CÓMO EL VÍDEO IP HA DEJADO DE SER UN SUBSISTEMA DE SEGURIDAD AISLADO PARA CONVERTIRSE EN EL EJE TRANSVERSAL DE DATOS EN INFRAESTRUCTURAS CRÍTICAS Y ENTORNOS INDUSTRIALES COMPLEJOS.

En la ingeniería de instalaciones contemporánea, la seguridad ha dejado de concebirse como un conjunto de silos independientes (control de accesos, detección de intrusión, protección contra incendios) para transformarse en un entorno interconectado. Bajo esta visión, múltiples subsistemas comparten información en tiempo real. Control de accesos, Protección Contra Incendios (PCI), climatización (HVAC), automatización e infraestructuras IT forman parte de una misma arquitectura operativa que debe diseñarse bajo criterios comunes de integración, disponibilidad y resiliencia.

Históricamente, estos sistemas funcionaban en paralelo, utilizando protocolos propietarios que dificultaban la interoperabilidad y creaban “islas tecnológicas”. Sin embargo, el escenario actual exige plataformas abiertas capaces de intercambiar información de forma segura y verificable. Como recoge la Guía de proyectos de instalaciones de protección contra incendios en establecimientos industriales (2025) del COIIM, la convergencia de información entre sistemas es hoy un requisito necesario para garantizar

la continuidad de negocio y la seguridad operativa. En este contexto, el vídeo IP se erige como una infraestructura crítica de datos, capaz de aportar el contexto visual y analítico necesario para validar eventos, automatizar procesos y respaldar decisiones estratégicas de alta responsabilidad.

El vídeo IP como eje del ecosistema de datos

Las arquitecturas modernas de seguridad no solo conectan sensores; utilizan el vídeo como fuente primaria de verificación, contexto y automatización. En el modelo actual, un evento de acceso ya no se limita a un simple registro en una base de datos; se asocia automáticamente a evidencia visual sincronizada que permite identificar quién y bajo qué circunstancias ha accedido a una zona.



Una alarma de intrusión deja de ser únicamente una señal digital ciega para convertirse en un incidente contextualizado mediante imagen, ubicación y tiempo. Cuando el sistema se diseña sobre plataformas de arquitectura abierta, el vídeo puede cumplir funciones que trascienden la seguridad física:

- **Verificación visual:** Alimentar sistemas de control de acceso mediante la asociación automática de grabaciones o reconocimiento facial.
- **Automatización operativa:** Activar cambios en iluminación, climatización o procesos operativos basados en la presencia o el flujo de personas.
- **Interoperabilidad:** Integrarse con sistemas de terceros mediante APIs, eventos y streaming seguro, permitiendo que el vídeo sea un “sensor de sensores”.
- **Cumplimiento y auditoría:** Proporcionar evidencia certificada para auditorías internas, cumplimiento normativo y análisis forense avanzado.

Diversos estudios recientes sobre AIoT (Artificial Intelligence of Things) muestran que la combinación de inteligencia artificial y dispositivos conectados permite que el vídeo asuma funciones de telemetría que anteriormente requerían múltiples sensores físicos costosos y complejos de mantener.

Seguridad aumentada por vídeo inteligente: Del análisis reactivo al proactivo

La verdadera transformación ocurre cuando el análisis de vídeo deja de ser un generador de alarmas aisladas para convertirse en un sistema de apoyo a la decisión basado en inteligencia artificial. Para aprovechar plenamente el potencial de la IA, es necesario rediseñar los procesos operativos.

La inteligencia artificial no debe entenderse como una capa cosmética, sino como un componente estructural que permite automatizar, priorizar y contextualizar los eventos masivos de una instalación.

Ante una incidencia, una plataforma moderna puede ejecutar respuestas orquestadas de forma automática:

- 1. Priorización de riesgos:**

Clasificar eventos según su contexto y nivel de criticidad.

- 2. Grabación dinámica:**

Activar grabación en alta resolución únicamente en las cámaras implicadas en el incidente, optimizando el ancho de banda.

- 3. Respuesta activa:**

Reposicionar cámaras móviles (PTZ) hacia la zona del evento de forma autónoma.

- 4. Optimización visual:**

Activar iluminación auxiliar para mejorar la visibilidad y aumentar la calidad de la prueba visual.

- 5. Reducción de fatiga operativa:**

Filtrar metadatos para eliminar falsas alarmas (diferenciando entre personas, vehículos, animales u objetos inanimados).

- 6. Este enfoque permite, por ejemplo, detectar conductas anómalas como el tail-gating (práctica en la que una persona accede siguiendo a otra autorizada sin usar credencial). Además, permite integrar flujos de trabajo mediante protocolos como MQTT, ajustando sistemas como climatización o iluminación según la ocupación real detectada por el análisis de imagen.**



IA aplicada al vídeo: Arquitectura, precisión y gobernanza



La incorporación de inteligencia artificial debe abordarse desde una perspectiva arquitectónica. Existen tres modelos principales de implementación que el ingeniero debe evaluar:

1. Analítica en el Edge (Borde)

La ejecución de algoritmos directamente en la cámara o en dispositivos cercanos a la fuente de imagen.

Este modelo permite:

- **Reducción de latencia:** Fundamental para decisiones críticas en milisegundos.
- **Eficiencia de red:** Disminuye el tráfico masivo hacia el núcleo del sistema, enviando solo metadatos.
- **Resiliencia:** Mantiene la capacidad operativa incluso ante fallos de conectividad central. Requiere hardware con capacidad de aceleración (GPU o NPU) y una estrategia robusta de actualización remota de modelos de IA.

2. Analítica centralizada

El procesamiento se realiza en servidores de alto rendimiento. Facilita el uso de modelos más complejos, el análisis histórico avanzado y la correlación entre múltiples cámaras para seguimiento de trayectorias. Diversos estudios indican que el dimensionamiento adecuado de recursos de cálculo y almacenamiento es fundamental para mantener un rendimiento estable en sistemas de gran escala.

3. Arquitectura híbrida

Combina la detección inicial en el borde con la validación o enriquecimiento en el núcleo. Los modelos distribuidos jerárquicos permiten que el sistema decida en milisegundos qué información procesar localmente y qué datos enviar al servidor central, optimizando tanto la red como los recursos de cómputo globales.

Más allá de la ubicación, el diseño debe contemplar políticas de actualización de modelos, evaluación periódica de tasas de falsos positivos y la trazabilidad de las decisiones automatizadas para evitar sesgos algorítmicos.

Optimización energética y operativa: El impacto térmico

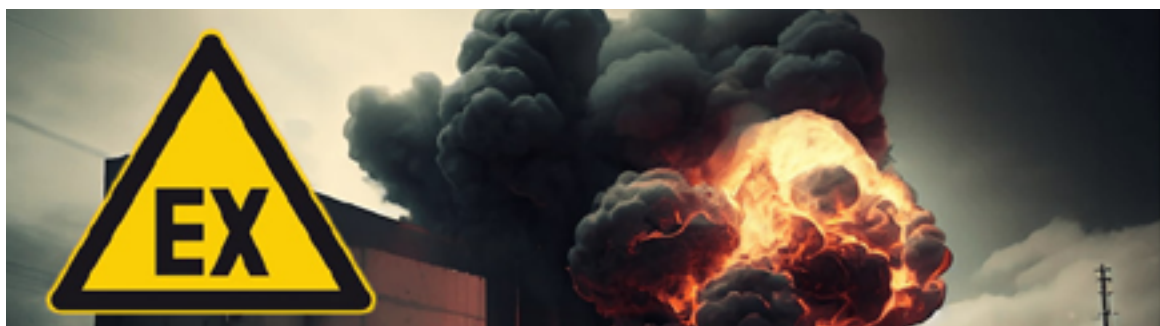
En instalaciones críticas 24/7-365, el diseño del sistema de vídeo IP no es neutro energéticamente. Cada cámara, grabador, switch PoE o servidor incrementa el consumo eléctrico y la carga térmica sobre la infraestructura de climatización.

En centros de datos y centros de control, este impacto afecta directamente al indicador PUE. Cuanto más cercano a 1,0 sea el valor del PUE, mayor será la eficiencia.

Cada equipo genera calor que debe ser disipado, lo que implica:

- Mayor carga térmica expresada en BTU/h que el sistema de HVAC debe eliminar.
- Mayor caudal de aire requerido (CFM), incrementando el consumo de ventiladores.
- Necesidad de sistemas de respaldo (SAI/UPS) más grandes y costosos.

Reducir el consumo individual de los equipos tiene un efecto multiplicador. Una arquitectura optimizada térmicamente mejora la estabilidad global del sistema y aumenta el MTBF, disminuyendo la probabilidad de fallos por sobrecalentamiento. La eficiencia energética deja de ser un objetivo ambiental para convertirse en un criterio técnico de diseño en sistemas de misión crítica.



Cumplimiento normativo y seguridad industrial (PRL y ATEX)

En entornos industriales y logísticos, el sistema de vídeo IP con IA se convierte en una herramienta activa de Prevención de Riesgos Laborales (PRL). La integración del vídeo con protocolos de seguridad permite verificar en tiempo real si el personal cumple los requisitos antes de acceder a zonas peligrosas.

Control de EPP / EPIs

El sistema puede verificar visualmente el uso correcto de Equipos de Protección Personal, como cascos, chalecos de alta visibilidad, gafas o botas de seguridad. Si el sistema detecta que un operario no porta el equipo requerido, puede denegar el acceso o bloquear la operación de maquinaria peligrosa, generando un registro verificable de la infracción para auditoría.

Aplicaciones en zonas ATEX

En atmósferas explosivas (gases o polvos combustibles), la monitorización mediante cámaras térmicas permite supervisar condiciones críticas sin exposición humana. El sistema puede detectar de forma temprana anomalías térmicas basadas en el análisis de emisividad, identificando sobrecalentamientos en cuadros eléctricos o rozamientos mecánicos antes de que se produzca un incendio o explosión.

Integración con Protección Contra Incendios (PCI)

La integración entre los sistemas de PCI y el vídeo IP añade una capa esencial de verificación remota. Cuando una central de incendios genera una alarma, el vídeo permite confirmar visualmente la situación en segundos.

Un sistema correctamente integrado puede:

- **Verificar alarmas en tiempo real:** Diferenciando un conato real de una falsa alarma.
- **Guiado automático:** Orientar cámaras PTZ hacia el detector exacto que ha saltado.
- **Gestión de emergencias:** Mostrar vídeo contextual al responsable de emergencias para coordinar la evacuación.
- **Detección temprana:** Utilizar analítica para detectar humo o llama en áreas donde los sensores convencionales pueden tardar en reaccionar debido a la altura de los techos o corrientes de aire.

Hacia plataformas unificadas: El VMS como núcleo

La fragmentación tecnológica está evolucionando hacia arquitecturas unificadas. Las soluciones modernas de gestión de vídeo (VMS) actúan como el núcleo de esta convergencia. Una plataforma abierta facilita la integración de dispositivos de múltiples fabricantes, reduciendo la dependencia de proveedores únicos y permitiendo una escalabilidad progresiva.

Las funciones operativas avanzadas de los VMS modernos incluyen:

- **Interfaces gráficas georreferenciadas:** Visualización mediante planos o mapas interactivos.
- **Controles contextuales:** Sugerir procedimientos de actuación (SOP) al operador ante cada tipo de evento.
- **Búsqueda forense basada en metadatos:** Encontrar en segundos a una persona con “chaqueta roja” o un vehículo de “marca específica” en grabaciones de semanas.
- **Audio bidireccional:** Comunicación directa con personal en campo a través de las propias cámaras.

Desde la ingeniería de seguridad, el diseño debe alinearse con marcos internacionales de referencia: IEC 62443 para ciberseguridad industrial, ISO 27001 para seguridad de la información e ISO 22301 para la continuidad de negocio.



Conclusión:

El reto para el ingeniero de seguridad ya no consiste únicamente en instalar cámaras, sino en diseñar una arquitectura capaz de integrar identidad, evento, contexto y confiabilidad. El vídeo IP ha dejado de ser un sistema auxiliar para consolidarse como el eje transversal que conecta la seguridad física con la operación técnica y la gestión de riesgos.

En un ecosistema cognitivo, el vídeo actúa simultáneamente como fuente de contexto, motor de automatización, herramienta de cumplimiento normativo y pieza fundamental de la resiliencia operativa. Al integrar estos elementos, las organizaciones no solo protegen sus activos, sino que optimizan sus procesos, garantizan la seguridad de las personas y aseguran la continuidad de servicio en infraestructuras modernas de misión crítica.

Referencias bibliográficas

- (2025). Guía de proyectos de instalaciones de protección contra incendios en establecimientos industriales. COIIM (Colegio Oficial de Ingenieros Industriales de Madrid).
- Pazho, A. D., Neff, C., Noghre, G. A., Ardabili, B. R., Yao, S., Baharani, M. & Tabkhi, H. (2023). Ancilia: Vigilancia Inteligente de Video Escalable para la Inteligencia Artificial de las Cosas. arXiv:2301.03561.
- Reglamento General de Protección de Datos (RGPD). Normativa europea sobre tratamiento de datos personales y privacidad.
- Normas Internacionales ISO/IEC 27001, 22301 y 62443 aplicadas a la seguridad industrial y la información.

Glosario técnico

- **AIoT:** Artificial Intelligence of Things (Inteligencia Artificial de las cosas)
- **ATEX:** Atmosphères Explosives (Atmósferas explosivas)
- **BTU/h:** Unidad Térmica Británica por hora (capacidad de calor/frío).
- **CFM:** Pies cúbicos por minuto (medida de caudal de aire).
- **COIIM:** Colegio de Ingenieros Industriales de Madrid
- **EPP / EPI:** Equipos de Protección Personal / Individual.
- **HVAC:** Heating, Ventilation and Air Conditioning
- **MTBF:** Mean Time Between Fails (Tiempo medio entre fallos). Indicador de fiabilidad.
- **MQTT:** Protocolo ligero de mensajería para comunicaciones M2M y sensores IoT.
- **PUE:** Power Usage Effectiveness (métrica de eficiencia energética en CPDs).
- **SOP:** Standard Operating Procedure (Procedimiento Operativo Estándar)
- **VMS:** Video Management System (software de gestión de vídeo).



CONOCE A UN **SOCIO**

**Cristóbal
Martín
Ayala**

SOCIO Nº 177



Buenos días Cristobal. Para comenzar, por favor, preséntate y dinos algo de ti para empezar a conocerte.

Buenos días, antes de nada agradecer el interés por entrevistarme y dar a conocer mi actividad, así como visibilizar al mercado de de la tecnología de video e inteligencia artificial. Nací en Sevilla hace 46 años y desde el 1998, coincidiendo con el inicio de la carrera universitaria, resido en Málaga, donde vivo con mi mujer y tengo un hijo de 8 años. Actualmente trabajo en Motorola Solutions donde me responsabilizo del negocio de video en Corporate Accounts en España, y también lidero el área de Relaciones Institucionales y empresa en el colegio Oficial de Graduados en Ingeniería de Telecomunicación de Andalucía.

¿Cuál es tu formación académica?

Soy Ingeniero Técnico de Telecomunicación por la Universidad de Málaga complementando mi formación técnica con un Executive MBA en la Escuela de Organización Industrial y posteriormente un posgrado en Big Data y Bussines Analytics también en la EOI.

Además de la ingeniería creo que te interesó desde joven la gestión empresarial ¿cuál fue el motivo?

Desde el inicio de mi actividad laboral he estado ligado al ámbito de ventas, considero necesario y pienso, de forma muy acertada, adquirir destrezas transversales en la gestión empresarial y de personas, con el



objeto de tener una visión completa de la empresa y complementar la formación eminentemente técnica que proporcionan las carreras técnicas.

¿Qué otros estudios no académicos, o reglados, has realizado?

Además de la formación reglada, siempre me ha resultado muy interesante potenciar la oratoria y comunicación en público, al fin y al cabo es esencial transmitir y hacer llegar el mensaje, bien sea con carácter personal o a un grupo de personas con eficiencia, en este sentido he realizado cursos de oratoria en el Marco de la Programación Neurolingüística (Escuela Europea de Oratoria), y Comunicación Científica no Verbal Aplicada a la Negociación (Escuela de Comunicación No Verbal Científica).

¿Cómo te han ayudado en tu desarrollo profesional?

Pienso que es muy necesario en perfiles técnicos con formación en ingeniería potenciar las soft skills o habilidades blandas: competencias personales y sociales como inteligencia emocional, flexibilidad, empatía, liderazgo, creatividad y resiliencia. Este tipo de habilidades ayudan mucho y son esenciales para el trabajo en equipo y para una colaboración efectiva en entornos híbridos o presenciales.

¿En qué empresas has desarrollado tu actividad profesional y en qué puestos? ¿cuáles son, o eran, sus sectores?

Tras finalizar los estudios universitarios inicié mi andadura laboral en una empresa de seguridad local en Málaga (Seguripur), me resultó muy interesante porque aterricé los conocimientos técnicos de la carrera al mundo real y comercial, y vi mucho potencial de crecimiento en el sector.

De Seguripur salte a Gunnebo responsabilizándome del área de ventas en Málaga, fue una gran escuela en materia de elaboración de grandes proyectos y licitaciones públicas, trabajábamos mayoritariamente con las Administraciones Públicas (AAPP). En 2008 inmersos en la crisis de las subprime me incorporé a Seguriber donde me responsabilicé del área de ventas de grandes proyectos en zona Sur, también trabajando mucho con las AAPP y clientes Institucionales. Estando en Seguriber surgió la oportunidad y me incorporé a Grupo Eulen, responsabilizándome del área comercial y técnica en Andalucía Oriental. Es una gran empresa donde aprendí muchísimo y coincidí con grandísimos profesionales, aprendiendo mucho sobre la gestión de equipos.

En esta época decidí incrementar mi formación con el objeto de llegar a puestos de mayor responsabilidad, y tras mi paso por Grupo Eulen me incorporé como Director Comercial a Grupo Control (donde lideré todo el equipo comercial de sistemas). También fue una enriquecedora experiencia en una gran empresa en pleno proceso de crecimiento y expansión que se ha consolidado de forma extraordinaria a nivel nacional.

Estando en Grupo Control surgió la oportunidad en Avigilon - Motorola Solutions, una grandísima oportunidad porque complementa toda la experiencia laboral en el área de ventas de integradores con un fabricante de primer nivel y cierra todo el círculo con los actores involucrados en el proceso de ventas. Actualmente desde Motorola Solutions estamos involucrados en grandes proyectos de video en Smart Cities, Administración Pública, Defensa, Transporte, Retail, Energía, etc. ayudando a nuestros partners (corporate accounts) a generar negocio con nuestras soluciones. Lo cual es muy satisfactorio.

Tras tu paso por Seguripur ¿viste que la seguridad era tu camino?

Como comentaba anteriormente tras mi paso por Seguripur vi mucho potencial de crecimiento en tecnologías aplicadas a seguridad, inicié la andadura trabajando en la Costa del Sol que ha sido siempre nicho de grandes proyectos de seguridad electrónica, y posteriormente en Gunnebo donde trabajábamos mucho con Administración Pública y también corroboré las grandes posibilidades de crecimiento en este sector. Llegando finalmente al área de ventas en Motorola Solutions donde enlazo todas las áreas anteriores (relación con integradores (partners) y Administración Pública).

Por lo que nos dices, tu trabajo de ingeniero se ha encaminado a las ventas y trato con el cliente. Supongo que es un aspecto de la empresa en el que te sientes cómodo ¿Qué te mantiene en él?

Desde que inicié mi andadura laboral he estado ligado a departamentos de ventas. Desde mi punto de vista es el área más importante y atractivo de la empresa, es esencial poder llegar al cliente final con un producto, un proyecto o un servicio y materializarlo e implantarlo.

Es muy importante saber comunicar y hacer llegar la parte técnica del producto al cliente y cerrar el ciclo, de hecho son perfiles muy demandados en el mer-

cado y más difíciles de encontrar (perfiles técnicos transversales en área de ventas). Pienso se deberían potenciar estas habilidades durante la formación técnica como complemento. Me mantengo en ventas en Motorola Solutions porque me siento muy cómodo, me apasionan las relaciones interpersonales y el poder hacer llegar la parte tecnológica a las personas. Para mi es la simbiosis ideal: tecnología-ventas.

En todo este tiempo ¿Qué cambios destacarías en las estrategias de venta? ¿cómo han cambiado los clientes?

Desde mi punto de vista las ventas han evolucionado hacia una venta mucho mas consultiva con perfiles cada vez más formados y especializados. Pienso es la evolución natural de la tecnología que ha cambiado y está evolucionando a pasos agigantados.

El mercado requiere perfiles con gran solvencia técnica y capaces de adaptarse a los cambios, reciclarse y formarse de forma continua.

Los clientes igualmente han evolucionado en las demandas tecnológicas y en general requieren proyectos de mayor complejidad tecnológica e innovación.

En casos muy recientes desde Motorola Solutions estamos trabajando en compras públicas innovadoras Europeas, donde se requieren los últimos avances en inteligencia artificial y analítica de video y adaptarlos a casos de usos concretos. Son proyectos muy apasionantes pero que requieren una gran solvencia técnica.

¿Entre tus competencias y capacidades personales cuales destacarías?

Desatacaría el trabajo en equipo, pienso que es esencial la colaboración y enriquecimiento entre todos los miembros de un equipo de trabajo, y me preocupo por fomentarlo y armonizar en todos los equipos de trabajo a los que pertenezco. En cuanto a lo personal la honestidad y generar relaciones fuertes de confianza a largo plazo es también muy importante para mi.

Desde tu puesto actual ¿cómo valorarías el estado y desarrollo de la transformación digital en las empresas, incluyendo a ingenieros de proyectos y a instaladores?

Con carácter general actualmente las compañías están en continuo proceso de transformación tecnológica, en los últimos años se ha acentuado el uso de nuevas herramientas de inteligencia artificial y bigda-

ta y se han incorporado como herramientas habituales e indispensables en el día a día.

Es muy habitual para los ingenieros de proyectos actuales usar herramientas de inteligencia artificial como ayuda para la elaboración de proyectos, licitaciones, etc. Esto supone un salto cualitativo en la gestión y optimización del tiempo en el día a día, pero también implica hacer un uso responsable de las mismas.

Sé que perteneces a varias asociaciones y eres una persona colaboradora. Háblanos de esta faceta de tu vida profesional.

Actualmente pertenezco a la directiva del Colegio Oficial de Graduados en Ingeniería de Telecomunicación de Andalucía, donde lidero el área de relaciones Institucionales y empresa, y también soy asociado de AEINSE. Para mi es muy enriquecedora la interrelación con personas y grupos que comparten un objetivo o actividad común, y la posibilidad de ayudarse y complementarse entre si.

Desde el COITTA en Andalucía tenemos distintos grupos de trabajo y potenciamos la tecnología en la región, haciendo de paraguas entre Administración Pública, empresas tecnológicas y asociados- colegiados, esta actividad es muy beneficiosas para la sociedad y para los asociados en particular porque ayuda a visibilizar oportunidades, a dinamizar proyectos, colaboración y genera beneficios para la sociedad en general.

¿Cómo conociste a AEINSE y qué te movió a asociarte?

Conocí AEINSE a través de personas involucradas en compañías de distribución de soluciones de seguridad con las que trabajo desde Motorola Solutions y que también pertenecen a AEINSE. Me parece muy interesante, beneficioso y enriquecedor pertenecer a una asociación con un objetivo en común donde poder intercambiar distintos puntos de vista y estar en relación con los distintos actores del mercado de seguridad tecnológica (ingenieros de proyectos, distribuidores, fabricantes, etc).

Pienso que la asociación y la posibilidad de compartir experiencias y oportunidades es muy interesante, en AEINSE existen distintos grupos de trabajo donde poder compartir experiencias en Inteligencia Artificial, Ciberseguridad, Infraestructuras, etc.



Pienso es un gran hito para la sociedad española visibilizar a los ingenieros de seguridad y contribuir a una mayor capilaridad en distintos organismos y profesionalización de la actividad de ingeniería de seguridad.

Fuera del trabajo diario, tendrás aficiones personales ¿Qué te gusta hacer?

En mi tiempo libre, sobre todo le dedico tiempo a la familia, durante los días laborales de la semana estoy viajando continuamente, y el fin de semana lo organizo para hacer planes familiares y dedicar tiempo de calidad a mi familia, solemos hacer actividades de ocio y deportivas. También hacer escapadas, nos encanta viajar y conocer nuevos sitios y personas. Como norma habitual realizamos un viaje internacional en familia al año, habitualmente coincidiendo con las vacaciones de verano. Como deportes me gusta el golf (en el cual me estoy adentrando recientemente. Tenemos gran variedad de campos en la Costa del Sol) y aprovechando la cercanía con el mar donde vivo también soy aficionado a las embarcaciones de recreo.

Que sugieres a nuestra asociación para que tengamos una mayor visibilidad y aportemos más valor a los socios.

Como comentaba anteriormente es un hito muy importante para la sociedad la visibilidad de los ingenieros de seguridad a través de AEINSE, pienso que la directiva anterior y la actual está haciendo un gran trabajo. Como sugerencia sería interesante alcanzar más visibilidad en la Administración Pública y generar sinergias y oportunidades de colaboración.

Todavía falta profesionalización en algunos proyectos desde la administración local, Ayuntamientos o instituciones que carecen de personal especializado en algunos casos y por ello es necesario generar sinergias y colaboración conjunta para dinamizar, agilizar y elaborar de forma profesional dichos proyectos.

También sería muy interesante generar sinergias desde AEINSE con el Colegio Oficial de Graduados en Ingeniería de Telecomunicación con el fin de incrementar los visados/verificados de proyectos de seguridad que den garantía de profesionalidad y buen hacer en la elaboración, implantación y ejecución de los proyectos.



La Fundación Borredá presenta el estudio: “Seguridad Civil y Empresa. Descifrando la Seguridad Corporativa”

ENE
14

El pasado 14 de enero en el Instituto de Ingeniería de España, Madrid, la fundación Borredá realizó la presentación del estudio ‘Seguridad Civil y Empresa. Descifrando la Seguridad Corporativa’.

Entendiendo por Seguridad Civil “*el conjunto de personas, instituciones, y empresas que desde el sector privado llevan a cabo todo tipo de actividades encaminadas a la mejora de la seguridad, propia o de terceros, cualquiera que sea su normativa regulatoria*”, el documento profundiza en el estudio de cada ámbito

En su elaboración han participado siete expertos, entre ellos, nuestro compañero **Enrique Bilbao**, que analizan a lo largo de ocho capítulos cuestiones relacionadas con la gestión de riesgos, la resiliencia empresarial, los profesionales de la Seguridad Corporativa, la gobernanza o la aportación de esta disciplina a la Seguridad Nacional.

PRESENTACIÓN **V Estudio Mujer y Seguridad**

**V Estudio
Mujer y Seguridad**
24 de febrero 2026

**FEB
2026**

El pasado 25 de febrero, en el ForoSICUR, tuvo lugar la jornada “Mujeres que inspiran: presente y futuro de la seguridad”, organizada por el Observatorio Mujer y Seguridad. Una parte destacada de la misma fue la presentación del V Estudio Mujer y Seguridad con los datos actualizados de la representación de la mujer en la Seguridad Pública y Privada entre otros contenidos.

Con su lectura se puede constatar una evolución positiva pero especialmente lenta e insuficiente. Respecto al año 2024, los incrementos de incorporación de la mujer en 2025, tanto en la Policía Nacional, como en las autonómicas, en la Guardia Civil y en la Seguridad privada, en 2025 están por debajo del 1%, excepto en los Mossos d'Esquadra, el 1,96%, y la Ertzaintza, el 1,03% no hay datos oficiales y, la colaboración de las empresas en facilitar estos datos no ha sido suficiente para generar datos estadísticos.

[Acceso al informe](#) 

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS



II Jornada DORA

El pasado 21 de enero, en la sede de Cecabank, Madrid, se celebró la II jornada DORA con el lema “Evolución, balance y perspectivas de un marco en transformación”. Organizada por Red Seguridad y la Fundación Borredá, acogió a numerosos profesionales de ciberseguridad para evaluar el impacto real de la implantación del Reglamento DORA un año después de su implantación, marcando un hito en la forma en la que las entidades financieras y aseguradoras debían abordar la resiliencia operativa digital.

Todos los ponentes coincidieron en que el **Reglamento DORA** no solo ha reforzado la resiliencia y la ciberseguridad del sector financiero, sino que ha ampliado el debate a otros actores y sectores que, hasta ahora, habían quedado al margen.

El Congreso se cerró con la entrega de las **Distinciones de Cuadernos de Seguridad** a diversos profesionales y entidades en reconocimiento a su labor en pro del sector.

[+información](#) 

ASLAN Congreso y Expo

AGENDA DEL SECTOR Y OTROS ASUNTOS DE INTERÉS

ASLAN 2026
17, 18 y 19 MARZO MADRID

Inicio Programa EXPO Speakers Investigación FAQs

¿Agentes IA, resiliencia, activos digitales...?
Evolucionamos
17, 18 y 19 de marzo / Palacio de Congressos Ifema / + 550 Expositores + 200 Speakers

CONGRESO ASLAN2026. 33ª EDICIÓN DEL GRAN EVENTO ANUAL EN ESPAÑA ORGANIZADO POR LA ASOCIACIÓN NACIONAL DE LA INDUSTRIA TECNOLÓGICA .

ASLAN 2026
17, 18 y 19 MARZO MADRID

La Asociación @aslan, que agrupa a 212 fabricantes y proveedores especializados en innovación digital y ciberseguridad, organiza los días 17, 18 y 19 de marzo en el Palacio de Congressos de Madrid, la 33ª edición del Congreso&EXPO ASLAN2026 bajo el título:

¿AGENTES IA, RESILIENCIA, ACTIVOS DIGITALES...? EVOLUCIONAMOS

Múltiples tiempos de grandes cambios. Participa en el gran Congreso & EXPO anual que la Asociación @aslan organiza con el apoyo de cerca de 200 empresas especializadas en innovación digital y CXOs que están liderando la re-evolución de grandes organizaciones en España: mejorando la productividad, desarrollando nuevos negocios, reforzando la ciberresiliencia...

ASLAN2026 es una oportunidad para conocer cómo está evolucionando la ciberseguridad, el puesto de trabajo digital, la automatización o la gestión del dato gracias a la IA y cómo afrontar los nuevos retos para redes, entornos multi-cloud, infraestructuras inteligentes y centros de datos.

DATA RESILIENCE **CYBER SECURITY** **DIGITAL WORKSPACE** **ARTIFICIAL INTELLIGENCE** **CLOUD DATACENTER** **INTELLIGENT NETWORKS**

**MAR
2026**

La Asociación @aslan con el apoyo de cerca de 200 empresas especializadas en innovación digital y CXOs que están liderando la re-evolución de grandes organizaciones en España, celebró la 33ª edición de su Congreso & EXPO ASLAN tuvo lugar los días 17, 18 y 19 de marzo de 2026, en el Palacio de Congressos de Ifema, Madrid.

Bajo el lema "Agentes IA, Resiliencia, Activos digitales...? Evolucionamos.", esta edición 2026 se ha estructurado alrededor de dos temáticas centrales: Inteligencia Artificial y el nuevo espacio dedicado a ciberresiliencia.

[+información](#)

LEÍDO, VISTO Y OÍDO EN...



La Inteligencia Artificial y su impacto en la sociedad

“¿Podremos seguir confiando en nuestros sentidos en un mundo donde lo falso puede parecer más real que lo auténtico, gracias a las tecnologías como los deepfakes? ¿Seremos capaces de establecer un marco regulatorio efectivo que equilibre el progreso tecnológico con la ética y la seguridad? ¿Qué riesgos surgirán si delegamos la toma de decisiones en sistemas de IA, especialmente en cuestiones críticas como la salud, la justicia o la política?”...

El libro de **Omar Arias Zurita** se propone dar respuestas a estas y otras preguntas a través de describir los fundamentos de la IA generativa A, su desarrollo y el impacto en la sociedad.

Publicado en abril 2025 · ISBN 979-8280305076



LEÍDO, VISTO Y OÍDO EN...



CUADERNOS DE SEGURIDAD



2026

El año de la completa industrialización del cibercrimen

“2026 será recordado como el año en el que la ciberdelincuencia dejó atrás el modelo ‘como servicio’ para convertirse en una industria plenamente automatizada”
En el número 5 – octubre 2025- leemos en la página 10 un interesante artículo sobre la **Banalización de la seguridad de las comunicaciones**.

Trend Micro, especialista global en ciberseguridad, ha publicado su informe anual de predicciones de seguridad para 2026, en el que advierte de que el próximo año marcará un punto de inflexión decisivo en la evolución del cibercrimen.

La convergencia entre inteligencia artificial avanzada y automatización masiva dará paso a ataques capaces de operar con una velocidad, escala y sofisticación sin precedentes, impulsando un modelo delictivo completamente autónomo

[artículo completo](#)



LEÍDO, VISTO Y OÍDO EN...



Blog Manuel Sánchez



Presente y futuro de la Seguridad Global

“La seguridad global en 2025 se define por un enfoque de convergencia absoluta, donde las dimensiones físicas, digital y geopolítica ya no se gestionan por separado, sino como un ecosistema único”.

Un interesante decálogo desarrollado por **Manuel Sánchez** que recoge objetivos y acciones a acometer en materia de seguridad en los distintos sectores o áreas de actividad en su artículo Presente y futuro de la Seguridad Global, integral e integrada.

[Leer artículo completo](#) 



LEÍDO, VISTO Y OÍDO EN...



BOLETIN AES ENERO 2026

Leemos en un artículo de Ricardo Cañizares, Asesor de la Asociación: **“la obsolescencia de los elementos que formar parte de los Sistemas Electrónicos de Seguridad se ha convertido en un punto crítico que hay que tener en cuenta a la hora de diseñar, implantar y mantener estos sistemas”.**

El autor, con el título **La obsolescencia de los Sistemas Electrónicos de Seguridad y sus implicaciones**, destaca en su artículo los riesgos a la hora de seleccionar sistemas electrónicos de seguridad a la vista de la velocidad de los cambios tecnológicos y los problemas de obsolescencia.

Leer el artículo completo: [aquí](#) 

PATROCINADORES

ADI

AXIS
COMMUNICATIONS

Casmar
Compromiso con la seguridad

ahua
TECHNOLOGY

DESICO®

DORLET

VIDEOSISTEMAS
ff FFV
GEUTEBRÜCK

HID

IQSIGHT

Hanwha Vision

Johnson
Controls

LANACCESS 30 años

LEGIC

Sicuralia
Systems

VIGI
by tp-link

SCATI

ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD
BOLETÍN N°65 MARZO 2026

π
AEINSE
Asociación Española de
Ingenieros de Seguridad