



Asociación Española de
Ingenieros de Seguridad

02 Mensaje
de la Junta Directiva

03 NOTICIAS **AEINSE**
Iván Ballesteros / Nuevo Blog
AEINSE / Emilio Castro
ESSIIF-Fire&Security School

07 NOTICIAS
PATROCINADORES

22 ARTÍCULO
ESPECIALIZADO
Guía Ingeniería: arquitectura
y cumplimiento ENS
en sistemas videovigilancia IP
Alberto Alonso

29 CONOCE A UN **SOCIO**
José A. Manzanares

33 **AGENDA**
DEL SECTOR

38 LEÍDO, VISTO
Y OÍDO EN...



**Ingeniería de Seguridad:
la próxima generación...**

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 vocación por la ingeniería de seguridad

En más de un foro se ha tratado el déficit de ingenieros en el sector y se acepta con resignación que, en general, las matrículas en Ingeniería en España han caído significativamente en las últimas décadas.

Esto implica que el problema de la falta de ingenieros no afecta únicamente al ámbito de la seguridad, sino a todos los sectores que requieren estas disciplinas. Según Google (2026), fuente de datos que utilizaremos a lo largo de este documento, el número de ingenieros por cada 100.000 habitantes en algunas regiones del planeta es: China, 100; Europa, 55; Estados Unidos, 40; y España, 25.

Un argumento recurrente apunta a que la caída de las matrículas en Ingeniería se debe a que otras disciplinas STEM (Science, Technology, Engineering and Mathematics) son más atractivas. Sin embargo, el número de graduados en STEM por cada 100.000 habitantes en estas mismas regiones es: Europa, 488; China, 271; Estados Unidos, 246; y España, 96.

Por tanto, justificar que la caída de las matriculaciones en Ingeniería se debe al auge de otras carreras del ámbito STEM parece poco acertado: también tenemos un déficit en las disciplinas STEM.

Las empresas del sector llevan años manifestando la dificultad de contratar ingenieros, en una situación permanente de pleno empleo. ¿Por qué no aumentan entonces las matriculaciones en un área que ofrece pleno empleo?

Si el pleno empleo no es suficientemente atractivo para matricularse en Ingeniería, ¿qué nos dice el rango salarial comparado con otros grados universitarios? En general, los graduados en Ingeniería tienen una prima salarial por encima de la media de los grados universitarios. La prima en estas mismas regiones es: Estados Unidos, 60%; China, 50%; Europa, 30%; y España, 22%.

Está claro que la prima salarial por disponer de un grado en Ingeniería es superior a la media de los grados universitarios en España. Y, aunque tenemos trabajo por hacer para alcanzar una prima más próxima a la de otras regiones, la diferencia salarial entre la Ingeniería y otros estudios de grado tampoco parece ser el motivo de las bajas matriculaciones. Si el pleno empleo y la prima salarial no son suficientes para convencer, veamos si el coste anual de estudiar Ingeniería constituye una barrera. El coste medio de la matrícula anual en estas mismas regiones es: Estados Unidos, 12.000 €; Europa, 2.500 €; China, 1.500 €; y España, 1.300 €.

Por lo tanto, la falta de tracción de las matriculaciones en Ingeniería no parece deberse a la falta de empleo, a la prima salarial o al coste de la matrícula. En esta editorial proponemos como hipótesis la vocación como el elemento diferencial que puede influir en la baja tasa de matriculaciones en Ingeniería.

Entendemos la vocación como una inclinación profunda y estable hacia una determinada actividad. El grado de dificultad de la carrera, tanto como barrera para matricularse como causa del abandono de los estudios de Ingeniería, puede ser un indicador de un problema de vocación.

Si aceptamos que la **vocación** es un proceso que se descubre y se consolida a través de estímulos durante la infancia y la adolescencia, cabe preguntarse si la vocación por la Ingeniería se ha visto suficientemente favorecida por las sucesivas reformas educativas. Al menos, la reducción de las matrículas así parece indicarlo; la proporción de la carga horaria del bloque de asignaturas STEM en la educación secundaria obligatoria en estas mismas regiones alcanza: China, 55%; Europa, 38%; Estados Unidos, 35%; y España, 31,7%.

¿Qué podemos hacer desde el sector para adaptarnos a esta situación?

Desde AEINSE queremos **descubrir y fomentar la vocación por la Ingeniería de Seguridad** en las etapas formativas previas a los estudios de grado, empezando por los ciclos de Formación Profesional, apoyando su incorporación al sector y buscando caminos para aquellos que quieran continuar posteriormente con estudios de grado en Ingeniería.

Desde AEINSE queremos **apoyar las iniciativas de otras asociaciones** que se orienten a aumentar la vocación por la Ingeniería de Seguridad.

Desde AEINSE queremos **potenciar la importancia de la Ingeniería de Seguridad en los proyectos** y la necesidad de que el mercado demande sus servicios.

Desde AEINSE queremos **apoyar a los ingenieros para practicar mejor la Ingeniería de Seguridad** y contribuir, con nuestro propio ejemplo, a mejorar el atractivo de nuestra profesión y de nuestra vocación. Potenciar la vocación por la Ingeniería de Seguridad es una responsabilidad que compartimos todos los que formamos parte de este sector. Por ello, desde AEINSE invitamos a empresas, profesionales, universidades, centros de formación y asociaciones a sumarse a esta causa, cada uno desde su ámbito de actuación. Necesitamos acercar la Ingeniería de Seguridad a las nuevas generaciones, despertar su interés y mostrarles el valor y el impacto que nuestra profesión puede aportar a la sociedad. Si queremos contar con los ingenieros de seguridad que necesitaremos mañana, debemos empezar hoy a despertar su vocación.



Entrevista a nuestro presidente Iván Ballesteros en Seguritecnia

La revista Seguritecnia publica en la página 36 de su número 520, julio – agosto, la entrevista realizada a nuestro presidente.

En ella, **Iván** analiza los objetivos prioritarios de **AEINSE**, que incluyen, entre otros, el reconocimiento profesional del ingeniero, integrar la ciberseguridad en los sistemas físicos, impacto de la IA, el seguimiento y colaboración en la normativa y la alineación de la seguridad con el negocio y su continuidad.

Respecto al impacto de la inteligencia artificial, manifiesta que “La IA no va a parar, pero no nos va a quitar el trabajo, nos va a dejar tiempo para dedicarnos a proyectos más complejos”.

[Entrevista completa](#) 

NOTICIAS AEINSE

BLOG AEINSE

Quien lleva años en seguridad acumula un conocimiento que casi nunca sale del entorno del trabajo diario. El blog de AEINSE <https://www.aeinse.es/blog> existe para que ese conocimiento se comparta y crezca.

Blog AEINSE

COMUNICACIÓN

CONÓCEMOS

OFERTAS DE EMPLEO

QUIERO SER SOCIO

FORO

CONTACTO

ACCESO

Actividades

Noticias

Blog

Boletines

Documentos

Guías

Enlaces

INICIO / COMUNICACIÓN / BLOG AEINSE

25

Agosto
2026

0
comentarios

NIS2, ENS y Compliance Act: el nuevo marco que está cambiando la gestión de seguridad

5 CLAVES PARA UNA ESTRATEGIA DE SEGURIDAD EFICAZ



Se añade una publicación cada quince días, sobre los temas de interés relativos a: CCTV, intrusión, incendio, control de accesos, ciberseguridad, centros de control CRA, riesgos, normativa, biometría, convergencia seguridad-ciberseguridad y ejercicio profesional.

El blog se enmarca en uno de los fines de la asociación: facilitar el intercambio y la difusión del conocimiento en el sector de la seguridad.

Compartir las experiencias, conocimientos y aprendizajes que genera el sector contribuye a favorecer una cultura de seguridad basada en el conocimiento, apoyar la formación continua de los profesionales y acercar a la sociedad información de carácter técnico y profesional.

Cada publicación se difunde posteriormente a través del perfil oficial de AEINSE en LinkedIn, ampliando así su alcance y facilitando el acceso a sus contenidos.

Felicitación a nuestro socio y compañero **Emilio Castro** por la consecución de las **tres certificaciones de ASIS Internacional**



Tras 20 años de experiencia en el diseño, implantación y gestión de sistemas complejos de seguridad, Emilio ha completado el ciclo de certificaciones de ASIS International al obtener recientemente la credencial PSP® (Physical Security Professional), que se une a las certificaciones ya obtenidas previamente: PCI® (Professional Certified Investigator) y CPP® (Certified Protection Professional).

Con este logro, accede a la Triple Corona de ASIS International, convirtiéndose en el **primer Ingeniero en España** en ostentar simultáneamente estos tres prestigiosos estándares globales bajo un perfil de Ingeniería, y sumándose al escaso grupo de aproximadamente doscientos profesionales que también la ostentan a nivel mundial.



Curso “Experto en Ingeniería y Tecnología de Seguridad”

ESSIIF – Fire & Security School ha desarrollado este programa formativo con el objetivo de proporcionar al alumnado una formación completa y cualificada en ingeniería y tecnología de seguridad desde una visión amplia y transversal.

El curso, con metodología online **comienza el 19 de octubre y finalizará el 11 de junio de 2027**, con **250 horas de clases en vivo/directo** vía plataforma de videoclases y **750 horas** de dedicación estimada.

Título propio ESSIIF y certificado de Universidad Isabel I.

En virtud del acuerdo de colaboración entre AEINSE y ESSIIF, los socios de AEINSE tenemos un importante descuento adicional.

[+información](#) 

ADI

AXIS[®]
COMMUNICATIONS

Casmar
Compromiso en la seguridad

alhua
TECHNOLOGY

DESICO[®]

DORLET

ff FFV
GEUTEBRÜCK

HID[®]

IQSIGHT

Hanwha Vision

Johnson
Controls

LANACCESS 30th

LEGIC

Sicuralia
Business

VIGI
by tp-link

SCATI

AEINSE
Asociación Española de
Ingenieros de Seguridad

DESICO[®]

LA CIBERRESILIENCIA TAMBIÉN FORMA PARTE DE LA SEGURIDAD FÍSICA

SEGURIDAD DESDE EL DISEÑO

PROTECCIÓN DURANTE TODO EL CICLO DE VIDA

DESICO Y LA LEY DE CIBERRESILIENCIA (CRA)

La Ley de Ciberresiliencia (CRA) entra en juego: ciberseguridad desde el diseño en DESICO

El 11 de septiembre de 2026 comenzó a aplicarse el artículo 14 del Reglamento (UE) 2024/2847 de Ciberresiliencia (CRA). Desde esa fecha, los fabricantes deben notificar vulnerabilidades explotadas activamente e incidentes graves que afecten a sus productos con elementos digitales. Las comunicaciones se tramitan mediante la plataforma única de notificación (SRP), gestionada por ENISA, con una alerta temprana en 24 horas y una notificación completa en 72 horas.

Es el primer hito de un reglamento plenamente aplicable el 11 de diciembre de 2027. La ciberseguridad deberá formar parte del diseño, desarrollo y mantenimiento del producto. La gestión de vulnerabilidades, el periodo de soporte, la evaluación de conformidad y el marcado CE serán requisitos para comercializar estos productos en la UE.

En DESICO llevamos tiempo trasladando este enfoque a nuestras soluciones. Incorporamos requisitos de ciberseguridad desde el diseño, análisis de riesgos, políticas de control de accesos lógico, comunicaciones seguras, cifrado de la información, trazabilidad, gestión de dependencias y actualizaciones seguras. También reforzamos procesos para detectar, evaluar, corregir y comunicar vulnerabilidades durante todo el ciclo de vida de nuestros productos.

Este enfoque guía la evolución de nuestras soluciones y nuestra adaptación a los principales marcos nacionales y europeos de ciberseguridad, como la CRA, el ENS y NIS2, para desarrollar soluciones de seguridad física cada vez más seguras, mantenibles y resilientes.



ODISEE

el nuevo Open Physical Security Software de DORLET

ODISEE es una plataforma abierta y 100% web, desarrollada por DORLET para unificar, optimizar y proteger todo el ecosistema de seguridad física de forma centralizada, cibersegura y adaptada a cualquier organización.

Este software nace para dar respuesta a una realidad ampliamente conocida: en muchas ocasiones, los sistemas no están plenamente integrados y no hablan el mismo idioma, lo que obliga a los operadores a saltar de pantalla en pantalla y tomar decisiones precipitadas en plena emergencia.

En este contexto, **ODISEE** se sitúa en una capa superior, permitiendo orquestar todos los sistemas de seguridad de forma ordenada e inteligente.

Desde **ODISEE** es posible monitorizar eventos en tiempo real, gestionar alarmas mediante flujos de trabajo trazables (Workflows) o analizar informa-

ción procedente de diferentes dispositivos y sistemas.

Con estas y muchas otras funcionalidades, es posible anticipar riesgos y facilitar la toma de decisiones estratégicas incluso en proyectos complejos o multisede.

Con **ODISEE**, **DORLET** refuerza su apuesta por la integración, la ciberseguridad y la innovación tecnológica, ofreciendo a las organizaciones una herramienta avanzada para gestionar la seguridad física de forma inteligente, escalable y preparada para los desafíos del presente y del futuro.

NOTICIAS PATROCINADORES



Seguridad integral, información útil

La seguridad actual exige detectar amenazas, investigar incidentes y conocer en todo momento el estado de los sistemas. En FF Videosistemas desarrollamos herramientas que responden a estas necesidades de forma integrada.

Los sistemas de analítica generan numerosos eventos que requieren atención personalizada. Nuestra solución los reúne en un único visor y ofrece un seguimiento automatizado de cada detección. La información se actualiza sin que el usuario tenga que intervenir, lo que facilita la supervisión y agiliza la respuesta.

Las analíticas aportan además metadatos sobre los objetos detectados y la escena. PNS Nexus es una herramienta de análisis forense que permite procesar hasta 200 cámaras por servidor con capacidad de búsqueda de personas, vehículos, objetos y reidentificación para poder localizar a una persona a través de las cámaras de la instalación.

Tan necesario como aprovechar los metadatos de la IA es conocer en tiempo real el estado de los sistemas para anticipar incidencias.

Por eso hemos desarrollado tres herramientas de supervisión: monitorización de los componentes de grabación, un panel con el resumen diario de eventos de IA y seguimiento en tiempo real de las conexiones con las cámaras.

La protección de los datos completa esta visión integral: utilizamos cifrado y contamos con la certificación ISO 27001 para la gestión de la seguridad de la información.

[+información](#) 



HID Signo Decor 30

Montaje empotrado
Diseño vanguardista
Calidad Signo



HID, líder mundial en soluciones de identidad confiable y control de acceso, ha lanzado su nuevo lector Signo Décor 30 en respuesta a la petición de arquitectos, especificadores e integradores: ... “Contar con un lector Signo diseñado para espacios de alta estética, sin comprometer la seguridad”

El lector **Signo Décor** aporta un diseño elegante y de montaje empotrado, ofreciendo la misma seguridad, confiabilidad y compatibilidad con credenciales móviles y administración remota que el resto de la **familia Signo**.

Principales Características:

- **Diseñado para integrarse:**
Se monta a ras en cajas de empotrar eléctricas estándar 90x90, por lo que se percibe como parte de la arquitectura del recinto.
- **Ideal para zonas de alto tránsito:**
Clasificación de resistencia al impacto IK10 con una robusta superficie de vidrio. Certificación UL294 para uso en interiores y exteriores.
- **Preparado para dispositivos móviles:**
Soporta Bluetooth y NFC nativos. Compatible con HID Mobile Access, incluyendo Apple Wallet y Google Wallet.
- **Seguridad de primera clase:**
Secure Element con certificación EAL5+. Autenticación confiable mediante SIO. Compatibilidad inmediata con el protocolo OSDP para una comunicación bidireccional segura.
- **Gestión remota:**
actualizaciones de firmware, configuración y diagnóstico remotos mediante **HID Reader Manager** y **HID Linq**. Gestión centralizada e informes a través de la plataforma **HID Origo**.



[+información](#)

[HID SIGNO Décor 30 Hoja de datos](#)



FLEXIDOME MULTI+ 7100i

IQSIGHT ha anunciado el lanzamiento de la cámara FLEXIDOME multi+ 7100i, expandiendo su familia de soluciones multisensor. Esta plataforma unificada destaca por sus características clave:

Cobertura de 360°

Cuenta con cuatro sensores independientes de 5 megapíxeles que ofrecen una vista completa de 20 MP desde una sola dirección IP.

Diseño modular flexible:

Permite combinarse con cámaras fijas, panorámicas o PTZ para adaptarse a los requisitos exactos del cliente.

Calidad de imagen avanzada:

Incorpora tecnologías HDR-X (Alto Rango Dinámico), Starlight e iluminación infrarroja (IR) inteligente para garantizar claridad en condiciones extremas de luz.

Inteligencia artificial integrada:

Incluye la analítica IVA Pro para detección de objetos. Al combinarse con la cámara AUTODOME 7100s, activa la solución MultiGuard PTZ, rastreando automáticamente los objetos de interés detectados.

Este modelo se une a las versiones dual 7100i IR y multi 7000i, consolidando un catálogo diseñado para reducir costes de instalación y optimizar la seguridad urbana, del transporte y del sector industrial.



TNO-C4082T

Cámara térmica con lente tele VGA



TNO-C4080T

Cámara térmica con lente



TNO-C4062T

Cámara térmica con lente tele VGA



TNO-C4060T

Cámara térmica con lente



TNO-C4052T



TNO-C4050T



TNO-C4042T



TNO-C4040T

Cámaras Térmicas VGA Ultrasensibles con Inteligencia Artificial

Hanwha Vision ha lanzado su nueva serie de Cámaras Térmicas VGA con lente Tele: solución basada en Inteligencia Artificial, altamente precisa, para vigilar infraestructuras críticas, protección perimetral, monitorización de costas y operaciones de seguridad fronteriza, en las condiciones más desafiantes.

En el corazón de la nueva línea se encuentra una sensibilidad térmica líder con NETD por debajo de 16mK, lo que permite capturar datos térmicos excepcionalmente depurados, incluso en entornos de baja visibilidad. Esta precisión permite al motor de Inteligencia Artificial clasificar objetos con mayor precisión, incluyendo personas y vehículos que puedan estar parcialmente ocultos, así como individuos que pueden estar agachados o tendidos.

Y más allá de la vigilancia perimetral convencional, la nueva serie cuenta con capacidades de Detección de Embarcaciones para entornos marítimos. La tecnología permite a los operadores detectar y clasificar embarcaciones con precisión, utilizando los mismos análisis inteligentes aplicados a personas y vehículos en tierra.

Diseñado para protección costera, seguridad portuaria y el control fronterizo marítimo, el sistema mantiene un rendimiento fiable con niebla, lluvia, nieve y oscuridad total.

A nivel de ciberseguridad, las cámaras cuentan con Elemento Seguro Certificado Nivel 3 FIPS 140-3, proporcionando cifrado basado en hardware, para proteger los sistemas contra el acceso no autorizado y las amenazas cibernéticas.

A nivel de certificaciones, la serie cumple con IP66/67, NEMA 4X e IK10, junto con MIL-STD-810H, para operaciones en entornos complejos.

[+ información](#) 

NOTICIAS PATROCINADORES



La nueva versión del sistema de gestión de seguridad CCURE IQ 3.20 incorpora gestión avanzada de incidentes basada en workflows

Johnson Controls ha presentado en la reciente feria de seguridad Global Security Exchange (GSX) 2026 en Atlanta, la versión CCURE IQ 3.20 que introduce nuevas capacidades orientadas a la estandarización de procesos operativos y la mejora de la trazabilidad en los centros de operaciones de seguridad.

Entre las funcionalidades más relevantes destaca la incorporación de un módulo nativo de **gestión de incidentes**, integrado directamente en la plataforma y diseñado para cubrir todo el ciclo de vida del incidente: creación, investigación, resolución y generación de informes.

El sistema permite asociar incidentes a uno o varios eventos de seguridad, así como crear incidentes independientes para gestionar situaciones detectadas por operadores o comunicadas por terceros. Esta capacidad facilita la correlación de eventos y la gestión centralizada de incidencias operativas y de seguridad.

Uno de los componentes clave es el **Workflow Builder**, una herramienta gráfica que permite modelar procedimientos operativos mediante flujos de trabajo configurables, árboles de decisión y reglas de actuación. Los workflows pueden activarse automáticamente en función del tipo de evento detectado o seleccionarse manualmente por el operador, garantizando una respuesta homogénea y alineada con los procedimientos internos de la organización.

Además, cada incidente puede incorporar evidencias, documentación, vídeos, imágenes y registros de auditoría, mejorando las capacidades de investigación, cumplimiento normativo y análisis posterior.

NOTICIAS PATROCINADORES



Cómo crear un puesto de videovigilancia sin PC

No todos los puestos de vigilancia necesitan un ordenador de propósito general. Cuando la función del operador se centra en supervisar la instalación, Smart Monitor de Lanaccess permite crear una posición de vigilancia conectada directamente al monitor y a la red de videovigilancia, sin necesidad de instalar un PC.

El dispositivo, de 12 × 12 × 2,2 cm, se acopla al propio monitor mediante HDMI y se comunica con cámaras y videograbadores a través de la red IP existente. Solo necesita un monitor y, si este no es táctil, un ratón o un joystick.

Desde el puesto de vigilancia, el operador puede:

- Visualizar mosaicos de hasta 25 cámaras y gestionar hasta 8 videograbadores de forma simultánea.
- Trabajar con imágenes de hasta 4k a 60 fps.
- Descarga de grabaciones a USB con previa identificación del usuario.

Con varias cámaras en pantalla, el equipo selecciona automáticamente el flujo adecuado para cada vista y, al ampliar una, utiliza el que ofrece mayor detalle. Además, incorpora un servidor web propio desde el que se actualiza el firmware, se cambia el idioma de configuración y se comprueba su estado de forma remota.

[+información](#) 

LEGIC connect26

Acceso de Confianza en Movimiento

El jueves 16 de septiembre dimos la bienvenida en Zúrich a todo el ecosistema del Control de acceso con motivo de nuestro evento **LEGIC connect26**, bajo el lema de este año: «Acceso de confianza en movimiento».

El mensaje desde el escenario: el sector del acceso está experimentando la mayor transformación de su historia, con más cambios en cinco años que en los treinta y cinco anteriores.

Las clases magistrales y las ponencias principales se pueden ver en los enlaces siguientes:

Cinco fuerzas están redefiniendo todo a la vez:

1. **La convergencia del acceso físico y lógico**
2. **Los estándares abiertos y la interoperabilidad**
3. **Enfoque en soluciones en la nube y credenciales móviles**
4. **Las nuevas normativas**
5. **La creciente demanda de soberanía**

La biometría, la inteligencia artificial, la robótica y la criptografía poscuántica están acelerando estas tendencias. También presentamos nuestra marca renovada y la idea que subyace en todo lo que hacemos: «Excelencia invisible». LEGIC es el componente inteligente y de confianza que se encuentra en el corazón de los sistemas de acceso modernos. Los visitantes disfrutaron de ponencias magistrales de primer nivel a cargo de Apple, UBS, Acre Security, ANYbotics, IDEMIA Public Security y Google. Mesa redonda «La revolución de las credenciales», en directo desde el escenario, con la participación de NXP Semiconductors, HID, LEGIC, The LEAF Community y Connectivity Standards Alliance (Aliro).

Clases magistrales

1. [Creación de productos CRA ready con LEGIC](#)
2. [Acreditación móvil con LEGIC](#)
3. [Iniciación de LEGIC neon-on-card](#)
4. [Demostración de LEGIC Orbit, LOCS y la aplicación Utility](#)
5. [¿Qué nos depara el futuro en LEGIC?: un adelanto](#)

Ponencias principales:

1. [La revolución de las credenciales \(LEGIC, NXP, HID, Aliro y LEAF\)](#)
2. [La clave está en tu Wallet: conversación con Lucyna Janas \(Google\)](#)
3. [Creación de la puerta de entrada digital / Caso práctico de UBS](#)
4. [El ecosistema de Apple en el control de acceso y más allá](#)
5. [La identidad en la era de la IA](#)
6. [Un Credencial de identificación para robots](#)
7. [Acceso físico para la era de la IA y la era poscuántica](#)

LEGIC



NOTICIAS PATROCINADORES



Sicuralia presenta la barrera digital SI-300D1

Sicuralia Systems anuncia el lanzamiento de la nueva barrera de microondas digital SI-300D1, desarrollada para sustituir a la emblemática serie analógica SI-300H empleada habitualmente en infraestructuras críticas como centros penitenciarios e instalaciones de alta seguridad.

Esta evolución tecnológica responde a la creciente dificultad en el acopio de componentes analógicos clásicos y a la necesidad de alinearse con los exigentes estándares de rendimiento actuales.

Certificada bajo la norma **EN-50131-1 Grado 4 Clase IV**, la **SI-300D1** integra Análisis Digital (FBM) para diferenciar intrusiones humanas reales de factores ambientales, alcanzando una probabilidad de detección del 99% y reduciendo drásticamente las falsas alarmas.

Entre sus ventajas clave destacan la tecnología F.S.T.D. (Fuzzy Side Target Discrimination -Discriminación de objetivos con contornos difusos) para ignorar interferencias en los bordes del haz causadas, por ejemplo,

por vegetación o vallas metálicas adyacentes., 16 canales de modulación, antienmascaramiento dinámico y gestión remota.

En proyectos de renovación dentro del ámbito penitenciario, la **SI-300D1** garantiza una instalación retroactiva fluida y sin costes de obra civil. Ofrece plena compatibilidad con los voltajes de alimentación preexistentes, salidas por relés NC y adaptación a los postes antiguos de hasta 110 mm mediante el herraje opcional **SI-300ADG110**.

[+información](#) 





TP-Link presenta Omada | VIGI Conecta Summit 2026

EL ENCUENTRO DE LA TECNOLOGÍA DEL PRESENTE QUE IMPULSA EL FUTURO

TP-Link, experto en soluciones de conectividad, videovigilancia e IoT, celebró el pasado 24 de septiembre en Madrid la segunda edición del Omada | VIGI Conecta Summit, un encuentro exclusivo para su canal que reunió a más de 300 integradores de sistemas, instaladores, distribuidores y partners tecnológicos.

La jornada sirvió para presentar las **últimas novedades de Omada**, su solución de networking para empresas, y de **VIGI**, su videovigilancia inteligente.

Destacaron un adelanto exclusivo de los nuevos puntos de acceso Wi-Fi 8 y la **gama Omada Fusion**, diseñada para pymes y puntos de venta, que integra router y controlador en un único equipo y, según el modelo también puede integrar NVR.

Uno de los grandes atractivos fue el despliegue en directo de una **solución Omada Campus** en el propio espacio del evento, desde la selección de equipos

hasta su instalación y configuración. El programa incluyó además una zona de exposición, una mesa redonda sobre el sector Hospitality y casos de éxito en sanidad y administración pública presentados junto a partners y clientes finales.

“Nuestros partners ya están convirtiendo estas soluciones en proyectos reales que generan valor para sus clientes. Ese es precisamente el espíritu del Conecta Summit”, afirmó **Aaron Wei, Country Manager de TP-Link España.**

ANALÍTICAS INTELIGENTES DE VÍDEO
Inteligencia artificial para seguridad y operaciones

SCATI ANALYTICS

Detección inteligente de eventos. Automatización de procesos. Decisiones inteligentes.

www.scati.com

ISO 9001 EU NDAA ONVIF

SCATI Analytics

Inteligencia Artificial para seguridad y operaciones

La Inteligencia Artificial transforma el vídeo en información útil para anticiparse a los riesgos, automatizar procesos y facilitar decisiones de forma más rápida y eficiente.

SCATI ANALYTICS transforma el vídeo en información accionable para detectar riesgos, automatizar procesos, prevenir el fraude y mejorar la eficiencia de las

Una completa gama de analíticas permite adaptar la solución a las necesidades de cada entorno:

- Reconocimiento facial y análisis demográfico.
- Lectura de matrículas (LPR) y clasificación de vehículos.
- OCR, códigos QR y códigos de barras.
- Conteo de personas, multitudes, filas y mapas de calor.
- Intrusión, cruce de línea, merodeo y objetos abandonados o robados.
- Estimación de poses y detección de comportamientos agresivos.
- Equipos de protección personal (EPI).
- Identificación de billetes.
- Detección de accesorios, personas tumbadas y pernocta.

Y cuando las analíticas se combinan, su potencial se multiplica. Mediante reglas lógicas, **SCATI ANALYTICS** correlaciona distintas condiciones para interpretar escenarios complejos y generar alertas únicamente cuando se cumplen los criterios definidos. Así es factible, por ejemplo, detectar posibles situaciones de fraude en cajeros, verificar operaciones de devolución o alertar del incumplimiento del uso de EPI en una zona determinada.





Axis presenta la cámara Q2802-E

Vigilancia biespectral con IA y resolución 4K

Axis Communications ha lanzado la **AXIS Q2802-E**, una cámara biespectral avanzada diseñada para elevar los estándares de la vigilancia perimetral. Este dispositivo “todo en uno” combina un sensor térmico de alta resolución (VGA) para una detección fiable con una cámara visual 4K, permitiendo una identificación precisa de los objetivos.

Gracias a la integración de inteligencia artificial, la cámara ejecuta **AXIS Object Analytics** para detectar, clasificar y rastrear objetos. Además, es compatible con **AXIS Perimeter Defender** para optimizar la detección de largo alcance de personas y vehículos. Una de sus funciones más destacadas es la fusión de imágenes, que combina los flujos térmico y visual en una sola imagen nítida y coherente.

Construida para entornos exigentes, la **AXIS Q2802-E** cuenta con carcasa resistente a vandalismo grado IK10 y protección contra vientos huracanados. En materia de ciberseguridad, el dispositivo integra **Axis Edge Vault** con certificación **FIPS 140-3 Nivel 3**, garantizando la protección de datos y claves.

Disponible en cuatro variantes de objetivos para adaptarse a distintos campos de visión, esta solución es ideal para quienes buscan detección térmica de alta resolución y verificación visual excepcional en un solo equipo.

casmar

ENS Categoría Alta

Únicos como distribuidor en España



Casmar obtiene la certificación ENS Categoría Alta la más exigente del sector

Casmar se ha convertido en el único distribuidor de España que actualmente posee la certificación ENS Categoría Alta, el nivel máximo del Esquema Nacional de Seguridad, tras partir de la Categoría Media.

No es una declaración propia, sino una certificación auditada por una **entidad acreditada por ENAC**, renovable cada dos años, lo que convierte este logro en un salto de madurez difícil de igualar a corto plazo.

¿Qué significa en la práctica? Que los sistemas donde un incidente tendría consecuencias muy graves exigen los controles más rigurosos, una gestión avanzada de riesgos y las máximas garantías de continuidad operativa, y **Casmar** ya cumple con todo ello.

Para integradores e instaladores que trabajan en proyectos sujetos al ENS, ya sea administración pública o infraestructuras críticas en energía, transporte,

agua, sanidad o finanzas, esto se traduce en algo muy concreto: un argumento objetivo y documentable ante el cliente final, sus auditores y su CISO, además de un acceso más fácil a proyectos exigentes con la cadena de suministro cubierta desde el origen.

La certificación sitúa también a **Casmar** frente a la directiva europea NIS2, que traslada a los sectores regulados la exigencia de garantías de seguridad en toda la cadena de suministro, consolidando así su papel como socio de confianza.

2026
TECHXPERIENCE
DAHUA CERTIFICATION

Te invitamos a formar parte de una jornada de formación práctica donde podrás profundizar en las soluciones Dahua junto a nuestros expertos, con demostraciones en vivo y manejo directo de los equipos. Amplía tus conocimientos, resuelve tus dudas y consigue tu certificación oficial Dahua con diploma.

Dahua
Certification

- Certificación oficial Dahua
- Formación con Diploma
- Prácticas con equipos y maquetas reales

¡Plazas limitadas! Inscripción abierta hasta cubrir aforo.

REGISTRO POR DH PARTNER APP.

Ver ciudades

Dahua Iberia presenta TechXperience 2026 H2



Dahua Iberia vuelve a recorrer España con TechXperience 2026 H2; una nueva edición de su programa de formación dirigido a instaladores, integradores y profesionales del sector de la seguridad electrónica.

La iniciativa recorrerá 10 ciudades de España con un formato especialmente práctico, combinando formación, demostraciones en vivo y manejo directo de equipos.

Durante las jornadas, los asistentes podrán conocer de primera mano las últimas tecnologías y soluciones de **Dahua**, ver su funcionamiento en escenarios reales y resolver dudas junto a los expertos de la compañía.

Las sesiones serán impartidas por expertos de Dahua y finalizarán con un proceso de certificación oficial

Dahua y entrega de diploma, reforzando el compromiso de la compañía con la formación continua y la especialización de sus partners.

TechXperience 2026 H2 busca acercar la innovación de **Dahua** a los profesionales del sector mediante una experiencia formativa orientada a la aplicación práctica, facilitando un conocimiento más profundo de las soluciones y de sus posibilidades de integración en distintos proyectos.

[+información](#) 



LEY ORGÁNICA 3/2018,
de 5 de diciembre, de
Protección de Datos
Personales y garantía de los
derechos digitales
(LOPDGDD)

REAL DECRETO 311/2022,
de 3 de mayo,
por el que se regula el
Esquema Nacional de
Seguridad (ENS)

Alberto
Alonso

Responsable del Programa de Ingenierías, Ciberseguridad y Compliance de
Axis Communications en España

GUÍA DE INGENIERÍA:

ARQUITECTURA Y CUMPLIMIENTO DEL ENS EN SISTEMAS DE VIDEOVIGILANCIA IP

LOS SISTEMAS DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV) Y VIDEOVIGILANCIA HAN EVOLUCIONADO DE SIMPLES HERRAMIENTAS DE SEGURIDAD FÍSICA A COMPLEJOS SISTEMAS DE INFORMACIÓN INTERCONECTADOS QUE ACTÚAN EN LA ACTUALIDAD COMO SISTEMAS DISTRIBUIDOS DE PROCESAMIENTO DE DATOS. CUANDO ESTAS INFRAESTRUCTURAS SE DESPLIEGAN EN EL SECTOR PÚBLICO, O EN OPERADORES PRIVADOS QUE PRESTAN SERVICIOS TECNOLÓGICOS A LA ADMINISTRACIÓN, EL DISEÑO DEBE REGIRSE IMPERATIVAMENTE POR EL ESQUEMA NACIONAL DE SEGURIDAD (ENS) PUBLICADO EN EL BOE COMO R D 311/2022

LA INGENIERÍA DEL SISTEMA NO PUEDE TRATARSE DE FORMA AISLADA; LOS FLUJOS DE VÍDEO, METADATOS Y TELEMETRÍA DE CONTROL REPRESENTAN ACTIVOS DE INFORMACIÓN CRÍTICOS CUYA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD, AUTENTICIDAD Y TRAZABILIDAD (DIMENSIONES CIDAT) DEBEN GARANTIZARSE DESDE LA FASE DE DISEÑO TÉCNICO (SECURITY BY DESIGN).

Criterios de categorización e impacto en el diseño (nivel Medio o Alto)



El ENS establece, en el Anexo I, tres niveles de seguridad, bajo, medio y alto, para cada dimensión afectada en el sistema en función del impacto de un incidente. Esto da lugar a tres categorías de seguridad del sistema: Básica, Media y Alta. Bajo el marco del ENS, el diseño de un sistema de videovigilancia queda excluido por norma general de la categoría Básica, debiendo proyectarse soluciones bajo los requerimientos de categoría Media o Alta.

La justificación técnica responde al análisis de impacto y al cálculo de riesgos en los siguientes escenarios:

1. Tratamiento masivo y escala del sistema:

La concurrencia de flujos de vídeo de un gran número de usuarios o ciudadanos de forma continua monitoriza de forma indiscriminada a un número indeterminado de personas. Esto se considera un tratamiento de datos a gran escala según el Reglamento General de Protección de Datos (RGPD), lo que eleva el umbral de protección técnica e impide normativamente la clasificación del sistema como Básico.

2. Procesamiento de categorías especiales de datos:

Si la analítica de vídeo integrada implementa reconocimiento facial, comparación biométrica o analíticas de patrones de conducta, la clasificación del sistema se eleva automáticamente a Categoría Alta, dado que procesa datos de categorías especiales según el RGPD.

3. Seguridad de las personas e instalaciones críticas:

Un sabotaje lógico al sistema de cámaras facilita intrusiones físicas, por ejemplo, en sedes gubernamentales, centros de mando o centros penitenciarios. La pérdida de disponibilidad del flujo de vídeo impacta directamente en la seguridad de la instalación, lo que eleva el riesgo a un nivel de impacto grave (Medio) o muy grave (Alto).

4. Vulnerabilidad vectorial en redes distribuidas:

Las cámaras IP son endpoints de internet de las cosas (IoT) instalados habitualmente en ubicaciones desprotegidas perimetralmente (vía pública, fachadas). Un sistema de categoría Básica carecería de los mecanismos de defensa en capas (Defense in Depth) y de la segmentación técnica necesarios para evitar movimientos laterales hacia la red central corporativa tras un compromiso físico del dispositivo.



Especificaciones técnicas exigibles

Como consecuencia directa de la clasificación en Nivel Medio o Alto, el ENS activa un catálogo de exigencias estrictas e imperativas recogidas en el Anexo II del Real Decreto 311/2022 sobre los componentes de la infraestructura:

Gestión de identidad y control de acceso perimetral ([op.acc.1] y [op.acc.2])*

- **Autenticación de endpoints mediante IEEE 802.1X:** Queda estrictamente prohibido el direccionamiento IP estático sin autenticación en switches de acceso. Cada cámara IP debe actuar como un suplicante (supplicant), autenticándose frente a un servidor RADIUS/TACACS+ mediante certificados digitales dinámicos (protocolo EAP-TLS). Cualquier caída de enlace (link) o sustitución no autorizada del hardware debe desencadenar el bloqueo automático del puerto físico (Port Security).

- **Control de acceso de operadores:** El acceso al VMS debe requerir un control de acceso basado en roles (RBAC) integrado con el proveedor de identidad corporativo (Active Directory mediante SAML 2.0 u OIDC). Para accesos interactivos, es de obligado diseño la Autenticación Multifactor (MFA) obligatoria.
- **Bastionado (Hardening) de dispositivos:** Las plantillas de configuración de las cámaras IP, codificadores y servidores de grabación deben incluir la desactivación total de servicios y demonios inseguros o innecesarios en producción, tales como Telnet, FTP, UPnP, HTTP (puerto 80) y protocolos de descubrimiento automatizado de red no controlados.

Seguridad en comunicaciones y almacenamiento ([mp.com.1] y [mp.info.1])*

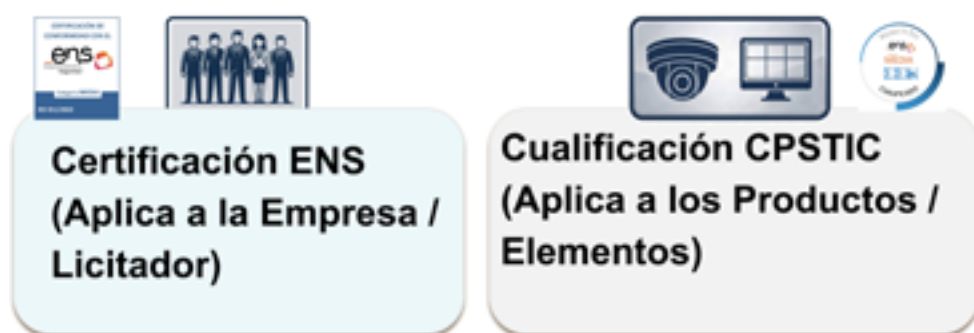
- **Cifrado de flujos en tránsito:** Queda descartado el uso de RTSP/RTP sin cifrar. Todo flujo de vídeo transmitido a través de la red de transporte debe encapsularse mediante protocolos criptográficos seguros: SRTP (Secure RTP) con cifrado AES-128/256 para el flujo de media, y HTTPS sobre TLS 1.3 para los canales de señalización, gestión y control PTZ. Para interconexiones WAN o despliegues en la nube, se requiere la tunelización mediante IPsec VPN.
- **Aislamiento y segmentación lógica:** La infraestructura de vídeo debe operar sobre una VLAN de seguridad dedicada y totalmente estanca. El tráfico debe ser inspeccionado por un cortafuegos de nueva generación (NGFW), bloqueando cualquier conexión con segmentos corporativos generales o redes públicas mediante la aplicación de políticas de denegación por defecto (Zero Trust).
- **Cifrado de datos en reposo:** Los repositorios lógicos de almacenamiento (unidades DAS, cabinas SAN/NAS o servidores de grabación) deben implementar cifrado de volumen a nivel de bloque mediante AES-256, protegiendo así la confidencialidad de las grabaciones frente a la extracción física de las unidades de disco.

Explotación, sincronización y resiliencia ([op.exp.2] y [op.exp.3])*

- **Centralización e inalterabilidad de eventos:** El software VMS debe reenviar en tiempo real registros syslog estructurados hacia un repositorio centralizado de seguridad (SIEM). Los logs de auditoría deben registrar la identidad, la marca de tiempo (timestamp), el ID de la cámara y la acción precisa (visualización, reproducción o exportación).
- **Sincronización de tiempo confiable:** Para mantener la validez legal de las grabaciones como evidencia judicial, todos los dispositivos (endpoints y servidores) deben sincronizarse mediante NTP (Network Time Protocol) autenticado (NTPv4) con un servidor de estrato oficial, como los del Real Instituto y Observatorio de la Armada (ROA).
- **Topologías de alta disponibilidad:** En diseños de Categoría Alta, los grabadores deben proyectarse en configuraciones de conmutación por error (Server Failover N+1 o N+M) y almacenamiento con tolerancia a fallos redundante por hardware (RAID 6 o ZFS), respaldados por sistemas de alimentación ininterrumpida (SAI) monitorizados vía SNMPv3.

Uso obligatorio del CPSTIC. Instrucción [op.pl.5]*:

La instrucción operacional [op.pl.5] (Componentes Certificados), perteneciente a la familia de Planificación del Anexo II del Real Decreto, establece de forma tajante que para sistemas de nivel Medio o Alto se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN.



Esta directriz transforma por completo la adquisición de hardware y software de videovigilancia:

- **Garantía en las medidas de ciberseguridad:** Los componentes del sistema de videovigilancia deben cumplir con los Requisitos Fundamentales de Seguridad (RFS) que establece el CCN, los cuales los habilitan para su cualificación en el catálogo CPSTIC.
- **Vías de cualificación técnica:** Para ingresar en este catálogo del CCN, los fabricantes deben someter sus productos a evaluaciones de laboratorio bajo metodologías como LINCE (comúnmente usada para niveles Medios) o Common Criteria / ISO/IEC 15408 (exigida con frecuencia para niveles Altos).

La mera certificación comercial extranjera de manera aislada no conlleva la cualificación, sino la verificación del cumplimiento de los RFS definidos por el propio CPSTIC y el Organismo de Certificación OC-CCN para cada familia de producto.

- **Evidencia formal:** Si un modelo de cámara IP o software VMS concreto no figura en la lista pública del CPSTIC, el sistema incurrirá en una no conformidad de auditoría.
- **Excepción por ausencia de mercado:** Solo se exime su uso si el ingeniero de diseño justifica documentalmente en la Declaración de Aplicabilidad y en el Análisis de Riesgos formal del proyecto la ausencia absoluta de alternativas en el mercado nacional que estén incluidas en el catálogo.

Aseguramiento de la conformidad continuada: Auditorías (Art. 31)



Los sistemas de videovigilancia categorizados en Nivel Medio o Alto están sujetos a obligaciones de control formal muy estrictas para mantener su vigencia regulatoria:

- **Auditoría regular bienal:** De acuerdo con el Artículo 31 del Real Decreto 311/2022, estos sistemas deben someterse a una auditoría formal ordinaria al menos cada dos años. Esta auditoría debe ser ejecutada por una Entidad Acreditada independiente.
- **Auditorías extraordinarias por cambios tecnológicos:** Se debe realizar una auditoría técnica extraordinaria siempre que se produzcan modificaciones sustanciales o reemplazos estructurales en la infraestructura de videovigilancia (como una migración masiva de almacenamiento local a entornos cloud VSaaS o la adición de módulos de computación de IA para reconocimiento facial). Esto anula la conformidad vigente y obliga a evaluar el sistema antes de pasar de nuevo a explotación.
- **Dictamen y Plan de Adecuación:** El informe analiza la conformidad técnica de cada elemento con las medidas del ENS. Los hallazgos de vulnerabilidades generarán un Dictamen de Auditoría que obliga a la organización a presentar un Plan de Adecuación inmediato para corregir las deficiencias, bajo riesgo de perder la certificación.

Impacto en la elaboración de pliegos técnicos (PPT)

Cualquier empresa de seguridad privada o proveedora tecnológica que licite para instalar o mantener sistemas de videovigilancia en la Administración pública debe cumplir con el artículo 2 del Real Decreto 311/2022.

Habitualmente, la inclusión de cláusulas de ciberseguridad en los dispositivos de videovigilancia dentro de los proyectos es muy dispar y, en ocasiones, escasa, debido a la falsa creencia de que no hay normativa aplicable. Este mandato aplica de igual manera a aquellos sistemas que, siendo de titularidad privada o estando ubicados en entornos privados, sean operados por entidades públicas, como las Fuerzas y Cuerpos de Seguridad (por ejemplo, las Unidades de Control Organizativo o UCO en los estadios de fútbol).

El error común en las licitaciones

En ocasiones, los pliegos incurren en un grave error técnico-jurídico al exigir literalmente un “certificado de conformidad con el ENS para los productos a licitar”. El ENS no certifica productos de hardware o software de forma aislada, sino que certifica la conformidad de los sistemas implantados y las organizaciones. Pedir un certificado ENS para una cámara es una exigencia jurídicamente imposible de emitir.

Lo correcto es exigir las medidas de seguridad del marco de referencia del ENS según su categoría. La instrucción [op.pl.5], en combinación con el artículo 19 del Real Decreto 311/2022, establece como obligatorio el uso de soluciones incluidas en el catálogo CPSTIC.

Plantillas recomendadas para la redacción de pliegos

Para asegurar la validez legal y técnica, se recomienda incorporar en la memoria justificativa del PPT una motivación del siguiente tipo:

«El sistema de videovigilancia objeto del presente contrato realiza tratamientos de datos personales mediante la captación y tratamiento de imágenes de personas físicas. De conformidad con el artículo 32 del Reglamento (UE) 2016/679 y con la disposición adicional primera de la Ley Orgánica 3/2018 (LOPDGDD), las medidas de seguridad aplicables a dichos tratamientos, cuando son realizados por entidades del sector público, son las previstas en el Esquema Nacional de Seguridad. En consecuencia, el presente contrato deberá garantizar el cumplimiento del Real Decreto 311/2022 y de las medidas que resulten aplicables a la adquisición de productos de seguridad TIC».

Asimismo, se aconseja añadir en el apartado de requerimientos técnicos del pliego una cláusula con la siguiente redacción:

«Las cámaras IP deberán cumplir las medidas del Esquema Nacional de Seguridad que resulten aplicables al sistema objeto del contrato, de conformidad con el Real Decreto 311/2022 y con la disposición adicional primera de la Ley Orgánica 3/2018 (LOPDGDD). Como medio de acreditación de dicho cumplimiento, las cámaras deberán encontrarse cualificadas en el catálogo CPSTIC».

De prescindir de estos requerimientos, el pliego puede incurrir en un incumplimiento de la normativa vigente si no existe una justificación jurídica y técnica suficiente. En consecuencia, la mesa de contratación podría enfrentarse a alegaciones, requerimientos previos o la interposición de recursos administrativos por parte de los licitadores.

No basta con declarar de forma genérica que el sistema será conforme; el órgano de contratación tiene la obligación de justificar cómo va a verificar dicho cumplimiento de manera efectiva. Exigir cámaras cualificadas en el CPSTIC es la opción más segura desde el punto de vista jurídico para demostrar objetivamente que se ha seguido el procedimiento previsto por el CCN.



Conclusión

En definitiva, la ciberseguridad es ya un elemento inseparable de los criterios de diseño y de la elaboración de prescripciones técnicas en el ámbito de la Administración pública y sus empresas dependientes. La resiliencia de los sistemas que protegen las infraestructuras críticas o gubernamentales depende directamente de la robustez de su protección cibernética, de una arquitectura basada en la seguridad desde el diseño (Security by Design), de la segmentación estricta de las redes y de la certificación verificable de los componentes conectados.

El ENS ha consolidado de manera definitiva la ciberseguridad como el pilar fundamental de los sistemas de videovigilancia actuales.

* Nomenclatura utilizada en el Real Decreto para diferenciar las medidas de seguridad aplicables en función de nivel de las dimensiones de seguridad.

CONOCE A UN **SOCIO**

José Antonio
Manzanares

SOCIO Nº 201
iberotelco@gmail.com



Buenos días Antonio. Para comenzar, preséntate, por favor, a nuestros socios para que podamos conocerte mejor.

Buenos días y muchas gracias por la invitación. Soy Antonio y actualmente trabajo en el Ayuntamiento de Torre-Pacheco (Murcia), donde soy responsable de Prevención de Riesgos Laborales. Mi trayectoria profesional ha estado siempre bastante vinculada a la tecnología, la seguridad, la prevención y la gestión.

Además de mi actividad profesional, colaboro en consultoría y formación, porque creo que compartir conocimiento y, sobre todo, trasladar la experiencia práctica a otros profesionales es una parte muy enriquecedora de mi trabajo.



¿Cuál es tu formación académica?

Soy Graduado en Ingeniería Telemática, nada más terminar el grado realicé un MBA (Máster en Administración y Gestión de Empresas). Con el tiempo hice un Máster en Prevención de Riesgos Labores. Este curso pasado he realizado el Máster del profesorado, lo que era el antiguo CAP.

Creo que las tres formaciones se complementan bastante bien. La ingeniería aporta la parte técnica y de resolución de problemas; la prevención introduce la perspectiva de seguridad y gestión del riesgo; y el MBA me ha ayudado a entender mejor la organización, la gestión económica y la toma de decisiones dentro de una empresa o administración.

De los estudios realizados ¿Cuales te han sido hasta ahora más útiles en tu vida profesional?

Probablemente la ingeniería me proporcionó la base: capacidad para analizar problemas complejos y buscar soluciones. Aunque mi formación en PRL también ha tenido un impacto enorme en mi actividad profesional ampliando mi visión sobre la seguridad. Con el MBA comprendí que toda decisión técnica tiene detrás una dimensión económica, organizativa y estrategia, las tres perspectivas se necesitan mutuamente.

¿Qué otros cursos has seguido además de los citados académicos?

Desde que termine el Bachillerato en la Escuela de Artes y Oficios de Murcia he realizado formación relacionada con prevención de riesgos laborales, protección contra incendios, emergencias y autoprotección, instalaciones, seguridad, gestión, nuevas tecnologías e inteligencia artificial, entre otras materias.

Quizá lo más característico de mi formación sea precisamente esa diversidad. No he entendido nunca la formación como algo que termina cuando obtienes un título, sino como un proceso continuo.

Veo que eres un estudiante "insaciable". De estos más de 120 cursos que citas en tu curriculum ¿cuales destacarías, cuales te han aportado más?

Más que hablar de un curso concreto, destacaría aquellos que me han permitido conectar disciplinas diferentes. Por ejemplo, la formación en prevención, sistemas de información geográfica, emergencias y protección contra incendios me ha permitido entender mejor la seguridad desde una perspectiva

global. También destacaría la formación relacionada con instalaciones y tecnologías, porque me permite comprender técnicamente muchos de los problemas que posteriormente tengo que gestionar.

Y últimamente la inteligencia artificial me está aportando muchísimo. No solamente por la tecnología en sí, sino porque obliga a replantearse cómo trabajamos, cómo buscamos información y cómo podemos automatizar determinadas tareas.

Creo que esa conexión entre conocimientos diferentes es precisamente una de las cosas que más valor me ha aportado la formación continua.

¿En qué empresas has desarrollado tu actividad profesional y en que puesto o responsabilidad?

Mi trayectoria ha tenido diferentes etapas y responsabilidades, pero actualmente desarrollo mi actividad principal en la Administración Pública, como responsable de Prevención de Riesgos Laborales del Ayuntamiento de Torre-Pacheco.

Además, compatibilizaba actividades de consultoría y formación relacionadas con la prevención, la seguridad, la gestión y las nuevas tecnologías en varias empresas y organizaciones, de esta etapa destacaría mi experiencia en Sagiser donde empecé a desarrollar esa combinación entre la ingeniería y la gestión empresarial que posteriormente me llevo a crear iberotelco como proyecto profesional propio.

Desde la perspectiva de los riesgos laborales ¿Cómo valoras su consideración en los pliegos de petición de ofertas y, una vez adjudicado, qué opinas del cumplimiento?

Creo que hemos avanzado mucho, pero todavía existe margen de mejora.

En los pliegos, la prevención de riesgos laborales debería plantearse desde el principio como una parte integrada en la contratación y no simplemente como un requisito documental que hay que cumplir para poder presentarse.

El problema aparece cuando se confunde tener documentación preventiva con hacer prevención. Una empresa puede tener todos los documentos necesarios y, sin embargo, que la gestión preventiva real sea mejorable. Por eso creo que hay que prestar más atención a cómo se ejecuta el contrato: coordinación de actividades empresariales, formación,

procedimientos de trabajo, equipos, planificación y, sobre todo, seguimiento.

La prevención tiene que estar presente durante toda la vida del contrato, no únicamente en la fase de licitación.

En tu actividad de consultoría ¿Qué tipo de actividad es la que más te satisface hacer?

Me gusta especialmente cuando existe un problema real y hay que analizarlo y encontrar una solución.

Disfruto mucho cuando puedo combinar la parte técnica con la gestión.

Por ejemplo, analizar una situación, estudiar la normativa aplicable, identificar los riesgos y después plantear una solución que realmente pueda implantarse.

También me gusta mucho la parte de formación, porque te obliga a ordenar tus propios conocimientos. Cuando tienes que explicar algo a otra persona descubres rápidamente qué partes conoces realmente bien y cuáles necesitas seguir estudiando.

También intervienes en labores de formación. Por ejemplo, dentro del acuerdo de AEINSE con ESSIFF participaste recientemente en algún curso. ¿Podrías sugerir algunas materias en las que ves necesidad de conocimiento para los ingenieros del sector de la seguridad?

Creo que existe una necesidad importante de formación transversal.

Un ingeniero dedicado a la seguridad necesita, evidentemente, conocimientos técnicos, pero también necesita conocer normativa, gestión de emergencias, protección contra incendios, prevención de riesgos laborales y, cada vez más, herramientas digitales.

Por eso veo especialmente interesantes materias como la gestión integral de emergencias y autoprotección, la protección contra incendios desde una perspectiva práctica, el análisis de riesgos, la coordinación entre diferentes sistemas de seguridad y las nuevas tecnologías aplicadas a la seguridad.

Y añadiría la inteligencia artificial. No creo que vaya a sustituir al ingeniero, pero sí va a cambiar muchísimo la forma en que un ingeniero trabaja.

¿Cuáles consideras que son tus puntos fuertes?

Creo que uno de mis principales puntos fuertes es la capacidad de aprendizaje, me encanta la frase del autor del libro Lean Startup, Eric Ries, que decía que “La única forma de ganar es aprender más rápido que los demás”.

También destacaría mi multidisciplinariedad y capacidad para relacionar conocimientos de ámbitos diferentes lo que permite analizar los problemas desde varias perspectivas encontrando soluciones más completas.

Otro de mis puntos fuertes es la capacidad de organización y coordinación. En prevención, especialmente en una organización grande, es necesario trabajar con muchas personas, empresas y departamentos diferentes, todos sabemos la complejidad que ello supone.

Actualmente eres vocal de Buenas Prácticas y Normas ¿Puedes adelantarnos algunas ideas para potenciar estos aspectos en la Asociación?

Me gustaría que AEINSE pudiera convertirse cada vez más en un espacio donde el conocimiento de los profesionales se transforme en conocimiento compartido. Hay muchísima experiencia entre los ingenieros que trabajan en seguridad y muchas veces ese conocimiento se queda dentro de su cabeza o en su organización.

Creo que podríamos potenciar la recopilación y difusión de buenas prácticas, experiencias reales, criterios técnicos y casos prácticos.

También considero interesante trabajar en documentos de referencia que ayuden a los profesionales a aplicar la experiencia y la normativa en situaciones reales.

En definitiva, me gustaría que las buenas prácticas no fueran solamente una recopilación de documentos, sino una herramienta viva construida entre todos los profesionales de la Asociación.

Además de trabajar y estudiar, habrás podido disfrutar y desarrollar otras aficiones. Háblanos de ellas.

Una de mis grandes aficiones es el deporte y, concretamente, la natación y el triatlón. Llevo muchos años vinculado al mundo del triatlón y soy Oficial Técnico de World Triathlon, llegando a desempeñar



responsabilidades como Technical Delegate y Chief en pruebas internacionales.

Es una actividad que me ha enseñado mucho sobre organización ágil, trabajo en equipos efímeros, toma de decisiones y gestión de situaciones bajo presión.

Soy miembro de la Junta de la Asociación de Prevencionistas de la Región de Murcia (AMP), donde actualmente estamos trabajando en la elaboración de guías para integrar la prevención desde la propia fase de diseño.

Un ejemplo claro son las cubiertas de edificios, donde cada vez se incorporan más instalaciones: fotovoltaica, clima, ACS entre otras y que no están contempladas en el diseño inicial del edificio, ahora deben tenerse en cuenta accesos, cargas y zonas de trabajo seguras para su posterior mantenimiento. Muchos de los accidentes que se producen podrían evitarse si se considerasen en la fase de diseño.

También me interesa mucho la tecnología y, por supuesto, viajar y disfrutar de tiempo con la familia.

¿Qué te llevó a hacerte socio de AEINSE?

Conocí AEINSE hace cuatro años en SICUR, donde inicialmente buscaba información sobre la formación necesaria para ser director de seguridad. Fue allí donde descubrí la Asociación y, sobre todo, el valor que tiene como punto de encuentro entre profesionales de un sector que me interesa especialmente.

Creo que una asociación profesional tiene mucho valor cuando permite conectar a personas con experiencias diferentes.

En mi caso, además, me interesaba especialmente conocer mejor el mundo de la ingeniería de seguridad y poder aportar mi experiencia.

Finalmente. ¿Cómo ves el presente y futuro del ingeniero dedicado a la seguridad en las empresas?

Creo que el papel del ingeniero de seguridad va a ser cada vez más transversal.

La seguridad ya no puede entenderse como algo aislado. Está relacionada con las instalaciones, las tecnologías de la información, la protección contra incendios, las emergencias, la prevención, la ciberseguridad, la continuidad del negocio y, cada vez más, con la digitalización.

Y ahí el ingeniero tiene una ventaja importante: está acostumbrado a analizar sistemas complejos y a buscar soluciones.

Pero también creo que el profesional tendrá que mantener una formación continua. Las tecnologías cambian muy rápido, la normativa y las necesidades de las organizaciones también.

En ese contexto, asociaciones como AEINSE pueden desempeñar un papel muy importante: ayudar a los profesionales a mantenerse actualizados, compartir conocimiento y establecer buenas prácticas. Personalmente, creo que el futuro pasa por un ingeniero de seguridad cada vez más transversal, capaz de entender la tecnología, pero también la organización, las personas y la gestión del riesgo.

Congreso Ciberseguridad de Barcelona BCC26



NOV
2026

La 7ª edición del Congreso de Ciberseguridad de Barcelona, organizada por Fira de Barcelona y la Agencia Cataluña de Ciberseguridad, se celebrará del 3 al 5 de noviembre de 2026 en la Fira de Barcelona-Gran Vía.

El área expositiva y las sesiones de ponencias y mesas redondas, será, una edición más, punto de encuentro de profesionales, expertos, empresas innovadoras y responsables de seguridad .

[+información-e-inscripción](#) 

Jornada ENISE



**OCT
2026**

Organizada por INCIBE, la vigésima edición de ENISE (Encuentro Internacional de Seguridad de la Información) tendrá lugar en el Palacio de de Exposiciones y Congresos de León.

El evento está consolidado como una de las principales citas de referencia, habiendo reafirmado su papel como punto de encuentro para fomentar el desarrollo del ecosistema nacional e internacional de la ciberseguridad.

Durante los días 21, 22 y 23 de octubre, acogerá un programa de actividades que abarca desde espacios expositivos a ponencias, pasando por encuentros de negocio, mesas redondas, espacios expositivos, encuentros de negocio y sesiones de networking.

Esta edición, además, tendrá un significado especial al celebrar el 20 aniversario de ENISE.

[+información-e-inscripción](#) 

AGENDA DEL SECTOR Y OTROS ASUNTOS DE INTERÉS

La Audiencia Nacional estima el recurso de AES y anula la Guía de la AEPD de 23/11/23



La Audiencia Nacional estima el recurso de AES (Asociación Española de Empresas de Seguridad) y anula la Guía de la AEPD publicada en noviembre del 2023 sobre el control de presencia mediante sistemas biométricos.

Según comunica AES "La resolución judicial estima las pretensiones formuladas por AES y supone un pronunciamiento de especial relevancia para el conjunto de los operadores afectados por la utilización de sistemas biométricos en el ámbito del control de presencia.

Desde el inicio del procedimiento, AES sostuvo que el contenido de la Guía generaba importantes dificultades jurídicas y operativas para las empresas, al introducir criterios interpretativos con un impacto directo en la utilización de tecnologías biométricas para el registro de jornada y el control de accesos de los trabajadores".

[+ información](#) 



NORMA **UNE-ISO/IEC 42001** Gestión de la Inteligencia Artificial



La **UNE EN ISO/IEC 42001** es la adopción en España y Europa de la norma internacional **ISO/IEC 42001:2023**, que establece los requisitos para implantar, mantener y mejorar un sistema de gestión de IA (SGIA) en organizaciones que desarrollan, suministran o utilizan sistemas de inteligencia artificial.

La certificación **UNE-ISO/IEC 42001** permite a las organizaciones demostrar su compromiso con el uso seguro y responsable de la IA. Esta certificación brinda tranquilidad en la gestión y uso de sistemas de inteligencia artificial, minimizando riesgos y protegiendo contra usos indebidos.

En un contexto donde las noticias sobre IA pueden generar inquietud, esta certificación asegura transparencia y responsabilidad, ofreciendo confianza y seguridad a todas las partes interesadas.

[+información](#) 

XVIII Jornadas técnicas de seguridad en centros hospitalarios



**OCT
2026**

El 22 de octubre tuvieron lugar estas jornadas, organizadas por OSICH (Observatorio de Seguridad Integral en Centros Hospitalarios) y Seguritecnia, y bajo el lema “Calidad y Seguridad: Una misma meta”, tendrá lugar la jornada en el Hospital Universitario de Getafe (Madrid).

Evento consolidado como foro de referencia de los profesiones de la seguridad en el ámbito sanitario que reúne anualmente a los profesionales de la seguridad de la Sanidad, así como a representantes de las Fuerzas y Cuerpos de Seguridad del Estado y de servicios públicos de Salud.

LEÍDO, VISTO Y OÍDO EN...



“La anticipación normativa como ventaja competitiva”

“la pregunta clave ya no es sólo si una tecnología cumple hoy, sino si seguirá haciéndolo durante toda su vida útil. Las tecnologías de seguridad física permanecen en servicio durante años. Una decisión tomada ahora puede condicionar la capacidad futura de cumplir requisitos de ciberseguridad, resiliencia, trazabilidad, actualización, certificación o soporte. Comprar solo por funcionalidad, precio o compatibilidad inmediata puede generar...”.

Artículo de nuestro compañero **Enrique Bilbao**, director general de DESICO, publicado en la página 76 del número 113 de **Red Seguridad** con el título “La anticipación normativa como ventaja competitiva”.



LEÍDO, VISTO Y OÍDO EN...



Guía de Buenas prácticas frente al modelo de la IA ofensiva

PUBLICADA POR CCN-CERT EL PASADO MES DE JUNIO.

“La incorporación de la inteligencia artificial al ámbito ofensivo está redefiniendo los fundamentos de la ciberseguridad. Su utilización ha dejado de ser una amenaza emergente para convertirse ya en una capacidad operativa integrada en campañas reales de actores criminales y estatales.”

“Su impacto no reside únicamente en la aparición de nuevas amenazas, sino en la capacidad de acelerar, escalar y automatizar técnicas ya conocidas, reduciendo drásticamente los tiempos entre la identificación de una vulnerabilidad y su explotación. La automatización permite pasar a velocidad de máquina de la detección de una oportunidad al ataque efectivo, lo que reduce el margen de actuación defensiva y traslada gran parte de la ventaja operativa al atacante”.

[Acceso a guía](#)



LEÍDO, VISTO Y OÍDO EN...



LA AMENAZA AÉREA DE MUY BAJA COTA: UN NUEVO RETO PARA LA SEGURIDAD URBANA (I)

“La amenaza UAS en entornos urbanos ya no puede tratarse como una anomalía ocasional. Es un riesgo reconocido en documentos estratégicos, sometido a procesos de normalización técnica en Europa y llamado a integrarse de forma estable en los análisis de riesgos, los planes de seguridad, los dispositivos de protección de eventos y la formación de los responsables públicos y privados de seguridad”.

En la **página 70** del **número 387** encontramos el artículo de **Óscar Pascual**, director de consultoría en **ADVANCE SECURITY**, sobre los sistemas de aeronaves no tripuladas (UAS) y los riesgos que representan.



LEÍDO, VISTO Y OÍDO EN...



La seguridad como ventaja competitiva

“Alcanzar la perfección en el modelo de la nueva seguridad no reside en la cantidad de capital que se invierta en ello. La mejor inversión es aquella que mira hacia el futuro, la que entiende que la mejor seguridad reside en la proactividad. No invertir en seguridad causa problemas, pero invertir de manera no resiliente, también”. Entonces... ¿cuál es el modelo a seguir?.

La publicación de **Cuadernos de Seguridad – Editorial Peldaño**, analiza cómo la seguridad puede convertirse en un factor clave para mejorar la resiliencia, proteger la continuidad operativa y fortalecer la confianza.

[Descargar ebook gratis](#)



LEÍDO, VISTO Y OÍDO EN...





Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad Pública y Privada
Presidente de Grupo Estudios Técnicos (GET)
Director de Círculo de Seguridad
Socio-Consultor de ComOutGlobal

[Inicio](#) [Contacto](#) [English](#) [Mi experiencia](#) [Mi otra pasión](#) [Mis libros](#)

2 SEPTIEMBRE, 2026

MANUEL SANCHEZ

Infraestructuras Críticas. Hacia un Modelo Integral de Seguridad, Resiliencia y Gestión del Riesgo

Decálogos de Seguridad

Suscríbete al blog

Infraestructuras críticas



“Las infraestructuras actuales ya no pueden analizarse como instalaciones aisladas. La realidad genera una red de dependencias e interdependencias en la que un incidente localizado puede propagarse rápidamente a otros sistemas y organizaciones, provocando efectos en cascada”.

[Documento completo](#)



LEÍDO, VISTO Y OÍDO EN...



Manual práctico de seguridad electrónica

Antonio Gómez Montolio



La editorial Paraninfo ha publicado el libro **Manual Práctico de seguridad electrónica**, escrito por nuestro compañero **Antonio Gómez Montolio**. Una obra perfecta para conocer los principios de las tecnologías aplicadas en los sistemas electrónicos de seguridad.

Los 14 capítulos del libro recogen conocimiento sobre las medidas de seguridad utilizadas actualmente: 1. Principios de la seguridad; 2. Protección perimetral; 3. Protección periférica, interior y especializada; 4. Unidades de control; 5 Videovigilancia I, cámaras y transmisión de imagen; 6 Videovigilancia II, grabación, almacenamiento y gestión; 7. Contramedidas electrónicas; 8. Ciberseguridad; 9. Control de accesos; 10. Planes de autoprotección; 11. Protección contra incendios; 12. Seguridad física; 13. Partes de un proyecto de seguridad; 14 Casos prácticos.

ISBN 9788428371742

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°68 OCTUBRE 2026

π
AEINSE
Asociación Española de
Ingenieros de Seguridad