

02 Mensaje
de la Junta Directiva

03 NOTICIAS **AEINSE**
AEINSE en Security Forum
GUGC
Capítulo 143 Axis en España

06 NOTICIAS
PATROCINADORES

21 ARTÍCULO
ESPECIALIZADO
**Redes IP Inteligentes
para videovigilancia**
Marc Abella

27 CONOCE A UNA **SOCIA**
Laura Díaz Enríquez

30 **AGENDA**
DEL SECTOR

33 **LEÍDO, VISTO
Y OÍDO EN...**

Feliz verano!

Mercedo verano 2026...

Un año más queremos trasladar nuestro reconocimiento a todos los asociados por vuestra dedicación y compromiso con la actividad profesional, afrontando un entorno en el que las exigencias de la ingeniería de seguridad continúan creciendo, mientras el tiempo y los recursos disponibles siguen siendo limitados.

Reflexiones del verano

En los últimos años estamos asistiendo a un desarrollo tecnológico y normativo acelerado que impacta directamente en la ingeniería de seguridad. Este avance aporta nuevas capacidades, pero también incrementa la complejidad de los proyectos, las soluciones y los procesos asociados. La evolución de las amenazas, la incorporación de nuevas tecnologías, la integración de sistemas y el aumento de los requisitos normativos hacen que cada proyecto requiera una mayor dedicación, en un contexto de agendas exigentes, recursos limitados y un mercado cada vez más competitivo.

Ante este escenario, creemos necesario reflexionar sobre cómo debemos afrontar este desafío y qué espera la sociedad de nuestra actividad profesional.

Es evidente que la mejora de nuestra eficiencia es un factor clave. Aunque algunas soluciones puedan parecer obvias, requieren una reflexión profunda y una aplicación adecuada.

Las herramientas de inteligencia artificial representan, sin duda, un elemento transformador para mejorar la eficiencia de la ingeniería. Su capacidad para analizar información, generar documentación y apoyar procesos técnicos aporta importantes oportunidades. Sin embargo, en su estado actual también pueden introducir desviaciones respecto al resultado esperado, que deben ser identificadas y corregidas por el profesional. Esta supervisión sigue requiriendo conocimiento, experiencia y dedicación. Utilizar la inteligencia artificial para abordar problemas complejos será cada vez más necesario, pero quizás también debemos plantearnos otra cuestión: ¿podemos simplificar algunos de los problemas antes de resolverlos?

La historia industrial nos muestra el valor de la estandarización. La estandarización permitió producir en masa, intercambiar componentes, reducir costes y aumentar la especialización. Sin embargo, la búsqueda actual de innovación y personalización ha llevado a que no todo pueda

ni deba ser estandarizado. La clave puede estar en encontrar un equilibrio: disponer de una base común estandarizada sobre la que desarrollar soluciones diferenciales que aporten verdadero valor. Por ello, desde **AEINSE** planteamos una reflexión:

¿Deberíamos disponer de un estándar base para los proyectos de instalaciones de seguridad?

Un estándar base permitiría que determinados elementos fundamentales de los proyectos se desarrollaran bajo criterios comunes:

Los planos de distribución de elementos de seguridad deberían utilizar criterios homogéneos de representación gráfica, simbología y nomenclatura. Cambiar la forma de representar un elemento o su identificación entre proyectos no aporta valor adicional a la solución de seguridad. Las mediciones deberían definirse con criterios comunes y utilizar formatos compatibles que faciliten su integración con los sistemas ERP de las empresas instaladoras. Las pruebas básicas de puesta en marcha deberían disponer de criterios rigurosos, verificables y reconocidos mediante un estándar común.

Sobre esta base estandarizada, la ingeniería de seguridad debe aportar aquello que realmente genera valor: nuevos enfoques frente a amenazas emergentes, análisis avanzado de datos procedentes de los sistemas de seguridad, soluciones más eficientes, eficaces y resilientes.

Una ingeniería basada en estándares no significa limitar la innovación. Al contrario, permite reducir la carga documental y eliminar tareas repetitivas, liberando recursos para dedicar más esfuerzo al análisis, al diseño y a la mejora de la seguridad.

Desde **AEINSE** invitamos a todas las partes interesadas a reflexionar sobre la creación de un estándar base para proyectos de instalaciones de seguridad como herramienta de mejora, eficiencia y reducción de complejidad desde el origen. Os deseamos a todos un feliz verano.

NOTICIAS AEINSE



BCN

03-04
JUN
2026



Patrocinadores, socios y el presidente de AEINSE en Security Forum



Un año más, y este es el decimotercero, tuvo lugar los pasados días 3 y 4 de junio en Barcelona, en el incomparable marco de las Drassanes Reials, el evento profesional Security Forum.

Nuestro presidente, **Iván Ballesteros**, compartió su vista al evento con nuestros patrocinadores allí existentes y con varios socios visitantes. Teniendo oportunidad de cambiar opiniones sobre el sector, los avances tecnológicos y compartir algún minuto para relajarse. Cena informal que nos permitió dialogar, conocernos mejor y hablar de proyectos futuros.

AEINSE, en la figura de nuestro presidente Iván Ballesteros, participa en el Centro Universitario de la Guardia Civil como ponente en la asignatura Seguridad e Infraestructuras frente a Impacto e Intrusión

**26
MAY
2026**

El Centro Universitario de la Guardia Civil (CUGC), adscrito a la Universidad Carlos III de Madrid (UC3M), es un centro de educación superior responsable de la formación universitaria de los futuros Oficiales de la Guardia Civil.

En el Grado en Ingeniería de la Seguridad se desarrolla la asignatura “**Seguridad e Infraestructuras frente a Impacto e Intrusión**”, donde de forma habitual se imparten conferencias desde el departamento de Planes y Directrices Técnicas del SEPROSE en colaboración con el sector privado.

En el ámbito de esta asignatura, el **Servicio de Protección y Seguridad de la Guardia Civil**, con la intención de fomentar los niveles de colaboración, invitó a **AEINSE** a dar una ponencia con el título “La seguridad en edificios: medidas pasivas en casas cuarteles, embajadas y ministerios”. **AEINSE** agradece al **SEPROSE** esta invitación y preparó un contenido específico para la ponencia impartida el pasado 26 de mayo en el campus de CUGC en Aranjuez.

Iván desarrolló el tema desde cuatro enfoques:

- I. El análisis de riesgos y la resiliencia como herramientas para identificar las necesidades de seguridad física. En ella explicó cómo utilizar herramientas de análisis de riesgos para determinar las medidas concretas de seguridad que requiere una instalación.
- II. La dificultad de despliegues de las protecciones pasivas. Los edificios están contruidos, el exterior está comprometido con el urbanismo, no todo es certificable ni se puede ensayar.
- III. CPTED y su aplicación a instalaciones como Casas Cuarteles, Ministerios o Embajadas. La prevención del delito y los adversarios decididos.
- IV. Herramientas para identificar el grado de seguridad de las medidas de protección en Casas Cuarteles, Ministerio o Embajadas. Diversas técnicas para evaluar la seguridad de una instalación contra una amenaza concreta.

El Capítulo 143 de AXIS International en España contó con la participación de AEINSE en la sesión práctica **“Analítica del dato aplicada a la seguridad corporativa”** que tuvo lugar el pasado 9 de junio en la sede de AXIS

09
JUN
2026

En la sesión, Iván Ballesteros, presidente de AEINSE, abordó el impacto del análisis de datos en la ingeniería; desde identificar los datos a registrar hasta el futuro análisis para obtener información para la gestión de la seguridad.

Entre otros aspectos se destacó:

La necesidad de planificar los datos que deben estar disponibles en los sistemas de seguridad y el uso que se le va a dar ya que son un elemento clave.

Diferenciar la explotación de los datos en tiempo real para identificar alertas, alarmas por confirmar y alarmas confirmadas; de la explotación a posteriori para analizar los factores de riesgo o la madurez del sistema de seguridad.

Los indicadores como producto del análisis de datos no son los mismos para todas las empresas, ni siquiera del mismo sector. Los indicadores y sus métricas deben ajustarse a cada empresa. Indicadores mal definidos pueden producir una falsa sensación de seguridad.

Las bases de datos, o los procesos para obtener los datos de los sistemas de seguridad, son desconocidos en muchas empresas.

La sesión finalizó con preguntas abiertas por los asistentes a la mesa de la sesión en las que se daba respuesta bajo distintas perspectivas.

Nuestro agradecimiento al **Capítulo de Axis international en España** por habernos invitado a participar en esta sesión.

ADI

AXIS[®]
COMMUNICATIONS

Casmar
Compromiso en la Seguridad

Alhuda
TECHNOLOGY

DESICO[®]

DORLET

ff
FFV
GEUTEBRÜCK

HID[®]

IQSIGHT

Hanwha Vision

Johnson
Controls

LANACCESS 30

LEGIC

Sicuralia
Business

VIGI
by tp-link

SCATI

AEINSE
Asociación Española de
Ingenieros de Seguridad



La seguridad que trabaja mientras el mundo se va de vacaciones

Las vacaciones son sinónimo de descanso, desconexión y cambio de ritmo. Oficinas que se vacían, agendas que se relajan y profesionales que, por unos días, dejan atrás su actividad diaria. Sin embargo, mientras las personas se toman un respiro, hay algo que no puede permitirse parar ni un solo momento: la seguridad de las infraestructuras críticas.

Detrás de cada vuelo que despegue con normalidad, de cada hospital que mantiene su actividad las 24 horas o de cada puerto que gestiona mercancías estratégicas y cruceros, existe un ecosistema de seguridad que opera de forma permanente. Y es que los sectores estratégicos no entienden de temporadas bajas. En muchos casos, incluso ocurre lo contrario: los periodos vacacionales pueden suponer un aumento de la actividad.

Alguno de los espacios más concurridos de España, como el Aeropuerto de Adolfo Suárez Madrid Barajas o el Aeropuerto del Prat en Barcelona están protegidos con las soluciones de DORLET.

Si bien es cierto que para una inmensa mayoría de usuarios estos sistemas pasan prácticamente desapercibidos, tú puedes estar tranquilo: todos siguen funcionando sin descanso para que tú puedas, simplemente, descansar.



NOTICIAS PATROCINADORES



Nuevas herramientas para monitorizar el estado de los sistemas de grabación Geutebrück

En el sector de la seguridad, la capacidad de anticiparse a incidencias es clave para garantizar la continuidad operativa de las instalaciones. Con este objetivo, desde F.F. Videosistemas hemos desarrollado nuevas herramientas que facilitan la supervisión, el mantenimiento preventivo y la gestión proactiva de las instalaciones.

Entre ellas destaca la monitorización en tiempo real del estado de las cámaras, que notifica y muestra de forma inmediata desconexiones, pérdidas de señal y problemas de comunicación.

A su vez, **PNS-PRO Task Manager** supervisa de manera continua los recursos críticos del sistema de grabación –CPU, memoria, almacenamiento, red y procesos–, facilitando la detección temprana de anomalías y la prevención de fallos.

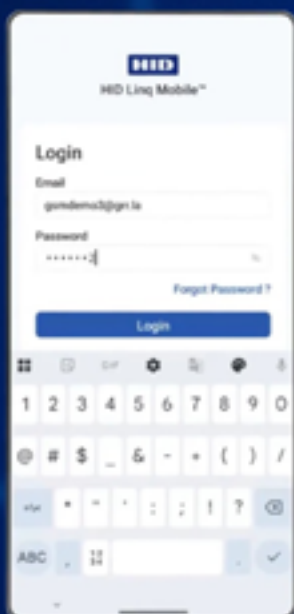
El **Dashboard de Eventos PNS-PRO-IA** permite visualizar de forma clara, centralizada e intuitiva toda la actividad generada por las cámaras con inteligencia artificial **PNS-PRO-IA**, permitiendo identificar zonas de mayor actividad y eventos relevantes para una gestión más eficiente de la seguridad.

En conjunto, estas herramientas refuerzan el mantenimiento preventivo, reducen costes operativos y mejoran la capacidad de respuesta de los sistemas.

Además, cada incidencia es notificada automáticamente a través de un evento que queda registrado en el sistema, garantizando la trazabilidad de las incidencias y una actuación rápida y eficaz ante cualquier anomalía.

Consulte con nuestros comerciales los requisitos necesarios para la implantación de estas funcionalidades.

[+información](#)



Linq Mobile optimiza la gestión de lectores HID

Nos complace anunciar HID Linq Mobile,
la última incorporación al portafolio de herramientas Linq.

Esta aplicación simplifica la gestión "in situ",
desde un teléfono móvil, de los lectores HID,
con una experiencia de usuario mejorada.



HID Linq



HID Signo Readers



HID OMNIKEY SE
Reader Core

Desde una sola aplicación e inicio de sesión, los técnicos pueden configurar, actualizar y mantener tanto los **lectores HID Signo** como los módulos de lector integrados **HID OMNIKEY SE Reader Core**

Principales Características:

Una sola App e inicio de sesión - Gestione varios tipos de lectores a través de una interfaz única y fluida.

Tarjetas de configuración virtual:

Almacene y reutilice plantillas de configuración para ser utilizadas más rápidamente en **lectores Signo** y los **módulos OMNIKEY SE Reader Core**.

Actualizaciones más rápidas:

Reduce el tiempo de las actualizaciones de firmware de los lectores y ahorra tiempo para mantener sus dispositivos actualizados y ciberseguros.

Conectividad Segura:

Realice actuaciones en terreno a través de BLE y NFC.

Firmwares soportados:

- **Signo:** 10.0.7.5 y posteriores
- **OMNIKEY SE Reader Core embedded reader modules:** FW25.A y posteriores

Para mayores detalles visite [HID Linq Mobile](#) 

- [Portafolio de herramientas Linq](#)
- [HID Signo](#)
- [HID OMNIKEY SE Reader Core](#)
- [HID Linq](#)
- [HID Signo Readers](#)
- [HID OMNIKEY SE Reader Core](#)
- [HID Linq Mobile](#)



Bosch Video Management System

Bosch Video Management System continúa ofreciendo los máximos estándares de seguridad y resiliencia, con nuevas funcionalidades introducidas en sus últimas versiones que permiten al operador de seguridad conseguir una mayor efectividad y agilidad en entornos críticos.

El seguimiento inteligente de personas permite localizar y monitorizar de forma efectiva a una o varias personas, de forma automática o manual, tanto en directo como en grabaciones.

Además, la integración de **IVA Pro Context**, analítica que revoluciona el concepto de videovigilancia al ofrecer información exhaustiva sobre la realidad que capta cada cámara, convierte al sistema de videovigilancia en un agente activo del sistema de seguridad, frente a su clásico papel pasivo.

Por último, la búsqueda forense mediante texto permite buscar eventos en las imágenes grabadas a través de frases simples y directas.

Sumado a ello, otras funcionalidades como la marca de agua en las exportaciones de video, para establecer mayor seguridad y permitir la auditoría del sistema a mayor nivel, la evolución de **SNMP v3**, para reforzar la seguridad en las integraciones de alto nivel, y la gestión de listas de matrículas, complementan y mejoran el sistema de gestión y grabación de videovigilancia de **IQSIGHT**.

Soluciones Cámaras Rugged PTZ de Hanwha Vision

Hanwha Vision, ha anunciado el lanzamiento de cámaras Rugged PTZ, desarrolladas específicamente para entornos complejos.

Los modelos han sido diseñados para ofrecer un alto rendimiento en condiciones extremas: temperatura operativa de -50 °C a +60 °C y resistencia probada a vientos huracanados de categoría 5.

Cuenta con **certificación IP68 e IK10**, y cumple con el estándar militar **MIL-STD-810H**. Ya sea expuestas a la salinidad en puertos o al polvo y la arena en zonas industriales, estas cámaras de la **Serie T** se consolidan como una solución robusta y fiable.

Vienen equipadas con un potente zoom óptico de 55x (2MP) o 43x (4MP y 8MP) y un alcance IR de hasta 500 metros, permitiendo capturar detalles en áreas de gran extensión. Su amplio rango de inclinación y las versátiles opciones de montaje garantizan una máxima flexibilidad de instalación.

Las cámaras incorporan Inteligencia Artificial (**chip-set Wisenet 9**) para mejorar la operativa. El motor de clasificación de objetos identifica personas, ros-

tros, vehículos y matrículas, mejorando de forma notable la velocidad y precisión en las búsquedas forenses. También permite que el auto-tracking inteligente mantenga el foco sobre el objetivo de forma eficaz.

Destaca por último la función enmascaramiento dinámico de privacidad (o DPM) garantizando el cumplimiento normativo de protección de datos. Estos modelos incorporan un alto nivel de ciberseguridad, con certificaciones como **FIPS 140-3 Nivel 3** y **ETSI EN 303 645**, avalando su resiliencia frente a amenazas cibernéticas.

Más información sobre estos nuevos modelos (**TNP-A6550RW, TNP-A7430RW y TNP-A9430RW**) en:

[+ información Hanwha](#)
[+ información Hanwha en YouTube](#) 



Johnson Controls presenta su radar en acción durante un evento en Sevilla

Johnson Controls celebró la pasada semana en Sevilla una jornada dirigida a consultores, ingenierías y clientes finales, con la participación de sus divisiones de Seguridad, Fuego y Building Management Systems (BMS).

El encuentro, que registró una elevada asistencia pese a las altas temperaturas, puso de manifiesto el creciente interés por soluciones integradas capaces de impulsar edificios más seguros, inteligentes y conectados.

Uno de los momentos clave fue la demostración en vivo del sistema de radar, desplegado en la orilla del río Guadalquivir, donde se llevaron a cabo pruebas reales de detección de embarcaciones a lo largo y ancho del tramo monitorizado.

Se trata de una solución con características únicas en el mercado, capaz de realizar detecciones de hasta 500-600 metros en ángulos de hasta 120°, incluso en condiciones de visibilidad reducida.

Además, el sistema se sincroniza con cámaras de CCTV, permitiendo el seguimiento en tiempo real de los objetivos detectados. Esta información queda registrada en el sistema VMS de vídeo para su análisis posterior, consolidándose como una tecnología diferencial para la protección perimetral.



Lanaccess incorpora el lenguaje natural en LAVA

Lanaccess presenta una nueva funcionalidad en la analítica LAVA que permite configurar detecciones de vídeo escribiendo en lenguaje natural.

El operador describe lo que quiere identificar y el sistema genera la regla de detección al momento, agilizando la adaptación de la analítica a situaciones concretas de cada instalación. Esta capacidad complementa las detecciones basadas en redes neuronales ya disponibles en LAVA.

El lenguaje natural permite cubrir casos cambiantes o específicos de cada empresa, por ejemplo:

- **Retail:** detectar carros de compra fuera del recinto.
- **Banca:** identificar una caja fuerte o cajero con la puerta abierta más tiempo del habitual.
- **Industria:** detectar el acceso a una zona de maquinaria sin EPI visible.

La configuración se realiza en tres pasos: (1) delimitar la zona de análisis sobre la imagen; (2) describir el evento que debe detectarse; y (3) definir el intervalo de detección y el tipo de alerta.

Cuando se cumple la condición, LAVA genera una alarma con la hora, el tipo de evento y una captura del momento.

Además, cada detección genera metadatos asociados a la grabación, disponibles en Lanaccess Suite para facilitar la búsqueda forense posterior por tipo de evento, fecha, hora o zona.

[+información](#) 

NOTICIAS PATROCINADORES

El cumplimiento de las normas de la CRA va más allá del componente

Componentes pueden facilitar el cumplimiento normativo

Fabricantes siguen siendo responsables

LEGIC y la Ley de Resiliencia Cibernética (CRA)

La Ley de Resiliencia Cibernética es un reglamento europeo cuyo objetivo es mejorar significativamente la ciberseguridad de los productos con elementos digitales comercializados en el mercado de la UE. Establece requisitos obligatorios como la seguridad desde el diseño, la gestión de vulnerabilidades, la notificación de incidentes y la seguridad de extremo a extremo a lo largo de todo el ciclo de vida del producto. El objetivo es claro: los productos conectados deben permanecer seguros durante toda su vida útil.

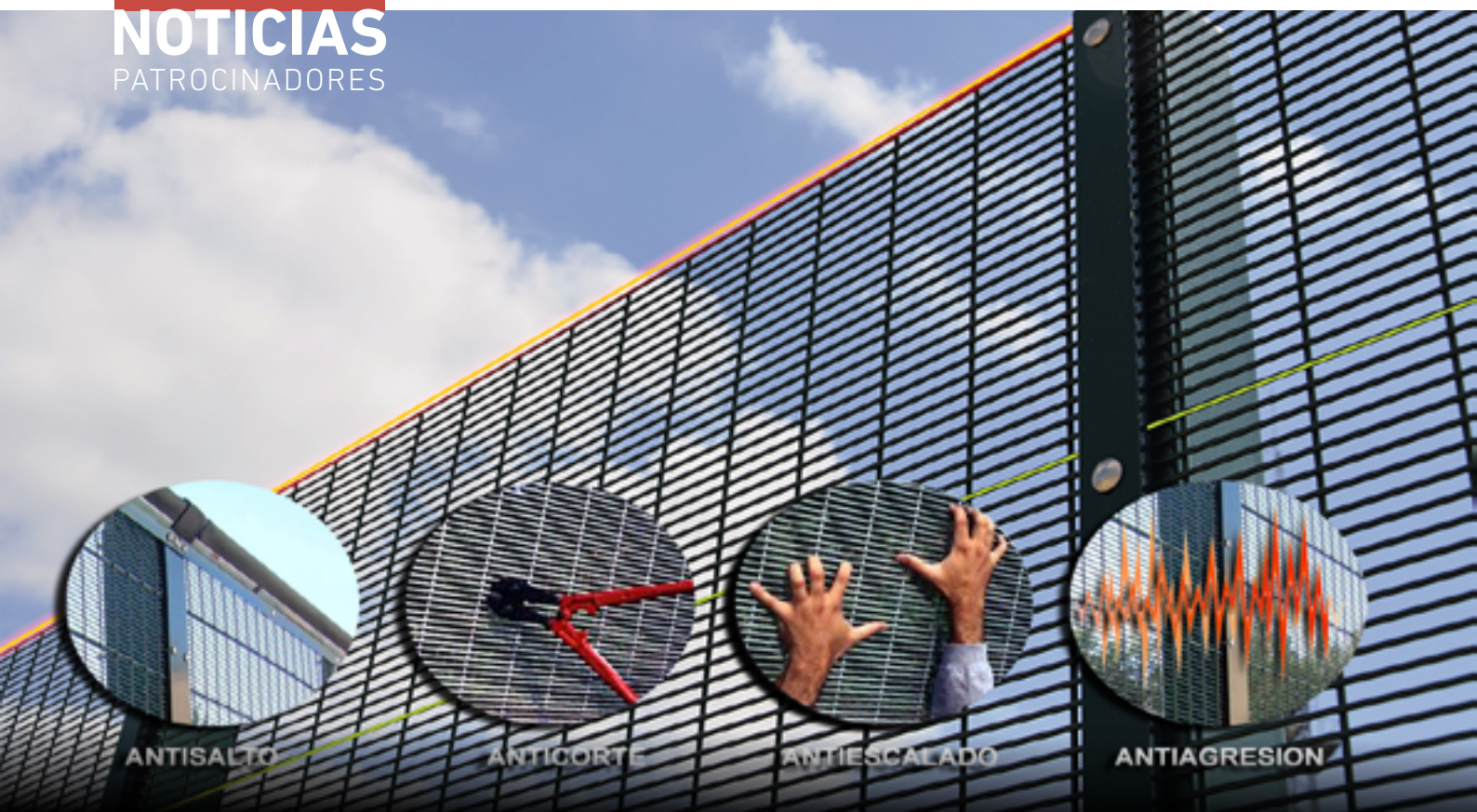
La CRA se aplica a todos los sectores y afecta por igual a fabricantes, proveedores y operadores. La ciberseguridad ya no es opcional; está regulada. Aunque la responsabilidad es compartida a lo largo de la cadena de suministro, la responsabilidad final recae en el operador económico que comercializa el producto, ya sea un fabricante, un importador o un distribuidor. No basta con utilizar componentes seguros; el verdadero cumplimiento de la CRA requiere seguridad a nivel de sistema.

Aquí es donde **LEGIC** desempeña un papel clave. **LEGIC** ayuda a las empresas a cumplir los requisi-

tos de la CRA desde la fase más temprana del diseño. No basta con añadir seguridad en una fase tardía del desarrollo. Por el contrario, debe integrarse en la arquitectura, la implementación y la gestión del ciclo de vida. Esto incluye raíces de confianza basadas en hardware, gestión segura de claves, aprovisionamiento protegido, actualizaciones de software, gestión de vulnerabilidades y protección de datos.

Las decisiones de arquitectura que se tomen hoy tienen un impacto normativo directo. Con la Plataforma de Seguridad de **LEGIC**, el cumplimiento de la CRA resulta más fácil, más eficiente y más sostenible.

NOTICIAS PATROCINADORES



Nuevo vallado sensor VPA

Sicuralia presenta el Vallado Perimetral Antiescalado VPA. Un sensor que fusiona en una única estructura, una barrera física de alta resistencia y una solución electrónica de detección avanzada.

El valor añadido del sistema reside en su total discreción: el vallado cuenta con elementos sensores invisibles totalmente integrados en su interior.

El cable sensor se aloja dentro de los propios tubos de la estructura, quedando completamente protegido ante las inclemencias meteorológicas y los intentos de sabotaje. Esta arquitectura permite ubicar con precisión cualquier intento de intrusión, garantizando la detección instantánea de cortes, agresiones, escalados, arrancados o saltos por encima de la valla.

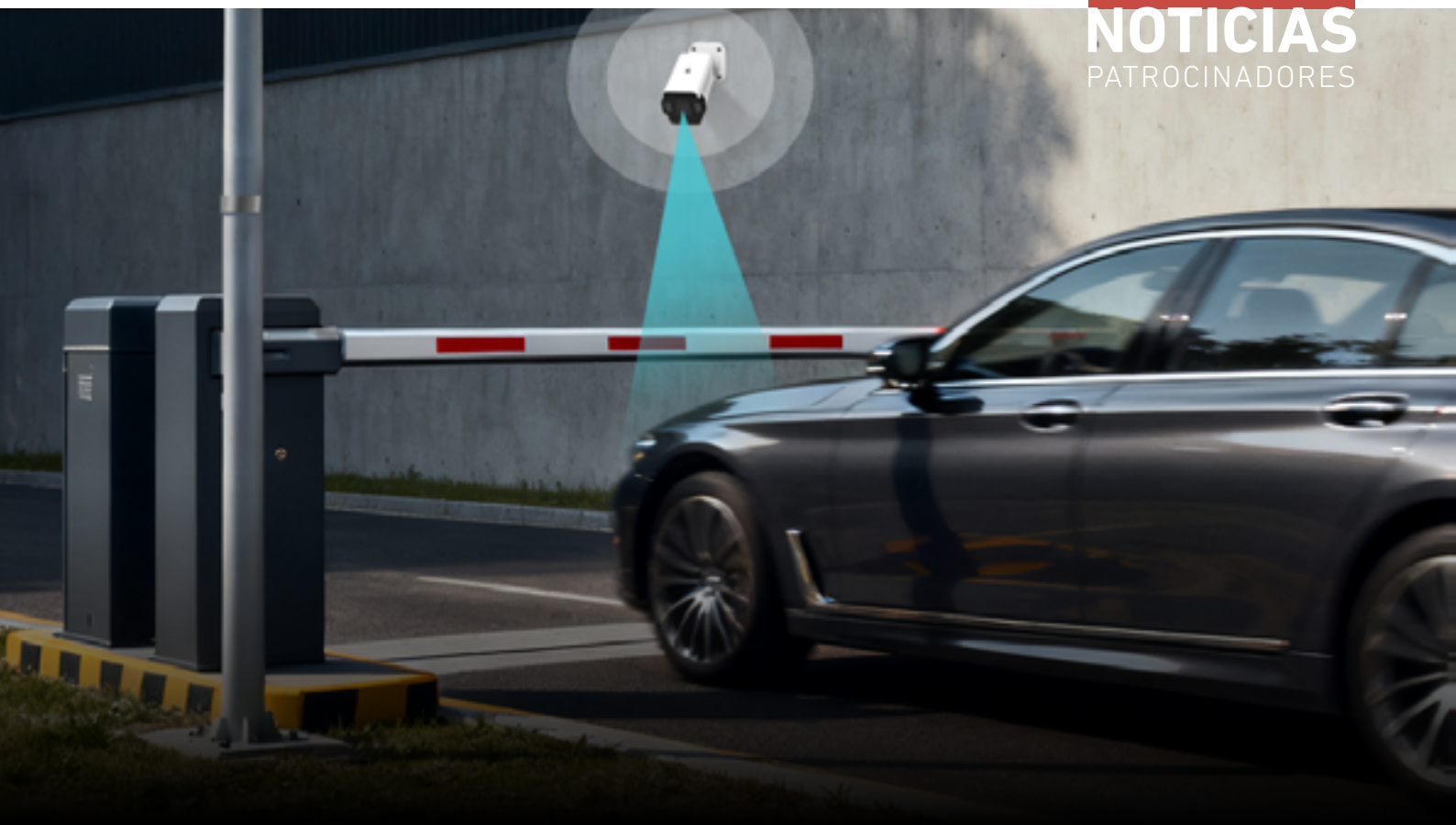
Además, el diseño físico del vallado está pensado para la disuasión. Su malla especial anti-escalada, fabricada con celdas compactas de 12,7 x 76,2 mm, reduce al mínimo los puntos de apoyo.

Esta configuración dificulta y ralentiza cualquier intento de escalado manual o con herramientas, proporcionando un tiempo de respuesta fundamental a los equipos de intervención.

Diseñado para soportar las exigencias de los entornos más sensibles y estratégicos, el **vallado sensor VPA** cumple con los estrictos estándares de los **Centros de Procesamiento de Datos (CPDs)**, proporcionando una solución robusta que neutraliza las amenazas perimetrales antes de que comprometan el interior de la instalación.

[+información](#) 





Control de Accesos Inteligente con Cámaras de Lectura de Matrículas de VIGI by TP-Link

Las cámaras de lectura de matrículas (LPR o ANPR) son un producto diseñado para automatizar el control de accesos y reforzar la seguridad en entornos como empresas, parkings, comunidades de propietarios e instalaciones logísticas. Mediante reconocimiento óptico de caracteres (OCR) e inteligencia artificial, identifican matrículas en tiempo real con gran precisión.

Este tipo de cámaras permite autorizar o denegar el acceso de vehículos de forma automática, registrar entradas y salidas, gestionar listas de matrículas autorizadas y generar alertas ante incidencias. Su integración con barreras, sistemas de videovigilancia y plataformas de gestión facilita la automatización de procesos y reduce la intervención manual.

Las **cámaras LPR de VIGI by TP-Link** destacan por su reconocimiento integrado de matrículas, alta resolución, visión nocturna y resistencia para uso exterior, garantizando un rendimiento fiable en distintas condiciones. Su uso contribuye a mejorar la trazabilidad de los accesos y optimizar la seguridad en instalaciones donde el control de vehículos es prioritario.

NOTICIAS

PATROCINADORES



PLATAFORMA COMPLETA EN LA NUBE

Videovigilancia, analítica y gestión de vídeo

-  Acceso remoto
-  Control centralizado
-  Grabación en la nube
-  Alertas inteligentes
-  Multiusuario
-  Escalable y flexible

www.scati.com



SCATI CLOUD

Plataforma de videovigilancia, analítica y gestión de vídeo

SCATI CLOUD es una plataforma de videovigilancia en la nube diseñada para centralizar la gestión de instalaciones, optimizar la supervisión y convertir el vídeo en información útil para la toma de decisiones. Permite monitorizar entornos multisede desde cualquier lugar, simplificando la operación y mejorando la eficiencia.

Gracias a sus capacidades de inteligencia artificial, **SCATI CLOUD** localiza eventos en segundos, reduce los tiempos de revisión y aporta información de valor para agilizar la respuesta ante incidencias.

Entre sus funcionalidades destacan el **reconocimiento automático de matrículas (LPR)**, el conteo y análisis del flujo de personas, la verificación del uso de **equipos de protección individual (EPIs)** y las búsquedas inteligentes de vídeo mediante filtros avanzados.

La plataforma se apoya en una arquitectura híbrida segura sobre **Amazon Web Services (AWS)**, con co-

municaciones cifradas y un modelo de suscripción escalable adaptado a las necesidades de cada proyecto.

A través de **SCATI CLOUD Bridge** se conectan de forma segura las cámaras de videovigilancia con **SCATI CLOUD** actuando como enlace inteligente entre la infraestructura local y el almacenamiento cloud sobre **Amazon Web Services (AWS)**, garantizando la continuidad operativa incluso ante incidencias de red. Accede a nuestra demo y descubre cómo **SCATI CLOUD** lleva la videovigilancia al siguiente nivel.

[+información](#) 





Drones DJI Enterprise transformando la seguridad pública

En seguridad pública, la información lo es todo. Saber qué está pasando, dónde y con qué intensidad es clave antes de actuar. La diferencia entre una intervención eficaz y una situación que se complica muchas veces depende de eso.

El problema es que obtener esa información con rapidez nunca ha sido fácil: el personal sobre el terreno tiene una visión parcial y el apoyo aéreo tradicional es caro y lento de desplegar.

Los **drones DJI Enterprise** están cambiando esa situación. Cámaras de alta resolución, sensores térmicos y capacidad de vuelo autónomo permiten tener una visión completa del escenario en tiempo real, de día o de noche, sin necesidad de exponer al personal. Eso significa llegar antes, decidir con datos reales y evitar riesgos innecesarios.

El resultado: tiempos de respuesta más cortos e intervenciones más seguras, tanto en una búsqueda en el litoral como en la gestión de un evento multitudinario o en la documentación de un accidente de tráfico.

Cada operativo es distinto, y la **gama DJI Enterprise** está pensada para eso: desde equipos compactos listos en minutos hasta plataformas de mayor autonomía para operaciones más exigentes.

En **Casmar** trabajamos para encontrar la solución que mejor encaja en cada caso.



Dahua Iberia inaugura su Innovation Center y refuerza su compromiso con la innovación en España



La inauguración del Innovation Center de Dahua Iberia supone un hito relevante en la estrategia de la compañía para impulsar la innovación, reforzar su presencia local y acercar sus soluciones tecnológicas a clientes, partners y profesionales del sector.

Este nuevo espacio ha sido concebido como un punto de encuentro entre tecnología, conocimiento y aplicación práctica.

A través de demostraciones, escenarios reales y soluciones integradas, el centro permitirá mostrar de forma directa cómo la tecnología puede responder a los retos actuales de distintos sectores, desde la seguridad y la gestión inteligente hasta la eficiencia operativa y la transformación digital.

Más que una sala de exposición, el Innovation Center se presenta como una plataforma de colaboración, diálogo y generación de nuevas oportunidades.

Su objetivo es ofrecer a cada visitante una experiencia útil, inspiradora y orientada a las necesidades reales de cada proyecto.

Con esta apertura, Dahua Iberia reafirma su apuesta por el mercado español y por un modelo de crecimiento basado en la cercanía, la innovación aplicada y la creación de valor junto a sus clientes y partners.



PYME INNOVADORA



 **DESICO**

Desico obtiene el sello Pyme Innovadora y refuerza su apuesta por la innovación tecnológica



Desico ha sido distinguida con el sello Pyme Innovadora, un reconocimiento otorgado por el Ministerio de Ciencia, Innovación y Universidades que acredita el compromiso de las empresas con la investigación, el desarrollo y la innovación como motores de crecimiento y competitividad.

Esta distinción pone en valor una forma de entender el negocio que ha acompañado a **Desico** desde sus inicios: desarrollar soluciones tecnológicas diferenciales capaces de responder a los retos de sectores donde la seguridad, la comunicación y la gestión inteligente son críticas.

La innovación en **Desico** va mucho más allá de sus áreas de I+D y Electrónica. Forma parte de la cultura de la compañía y se refleja tanto en el diseño de nuevos productos y servicios, como en la mejora continua de los procesos internos y en la manera de colaborar con clientes y socios tecnológicos.

Este enfoque, compartido con el **Grupo Casnova**, permite a la empresa anticiparse a las necesidades del mercado y ofrecer soluciones de alto valor añadido.

La obtención del sello Pyme Innovadora supone un importante respaldo al trabajo desarrollado por todo el equipo de **Desico** y refuerza el compromiso de la compañía con la excelencia tecnológica, la evolución constante y la creación de soluciones innovadoras que contribuyan a construir organizaciones más eficientes, conectadas y preparadas para el futuro.

Marc
Abella

Head of Customer Solutions & Product Strategy
TP-Link España

DE LA PLANIFICACIÓN A LA GESTIÓN EFICIENTE

REDES IP INTELIGENTES PARA VIDEOVIGILANCIA

EN LOS SISTEMAS DE SEGURIDAD ACTUALES, LA RED IP ES MUCHO MÁS QUE EL MEDIO POR EL QUE VIAJA EL VÍDEO. ES LA BASE QUE PERMITE QUE LAS CÁMARAS FUNCIONEN DE FORMA ESTABLE, QUE LAS GRABACIONES NO SE INTERRUMPAN Y QUE EL SISTEMA PUEDA GESTIONARSE CON FACILIDAD.

LA VIDEOVIGILANCIA YA NO CONSISTE ÚNICAMENTE EN INSTALAR CÁMARAS. CADA CÁMARA GENERA VÍDEO DE FORMA CONTINUA, Y ESE VÍDEO DEBE TRANSMITIRSE, PRIORIZARSE Y ALMACENARSE CORRECTAMENTE. SI LA RED NO ESTÁ BIEN DISEÑADA, PUEDEN APARECER CORTES, RETRASOS, PÉRDIDA DE CALIDAD O INCLUSO CÁMARAS DESCONECTADAS EN MOMENTOS CRÍTICOS.

Por eso, una red de videovigilancia profesional debe planificarse desde el inicio, teniendo en cuenta la ubicación de las cámaras, el ancho de banda necesario, la alimentación eléctrica, la seguridad y la gestión remota. A continuación, repasamos los puntos clave para diseñar una red de videovigilancia fiable, escalable y sencilla de mantener.

Diseño y planificación: evitar problemas antes de instalar

El éxito de una instalación de videovigilancia empieza antes de colocar la primera cámara. Una buena planificación permite evitar zonas sin cobertura, problemas de cableado, saturación de la red o costes adicionales por modificaciones posteriores.

Antes de instalar, es recomendable analizar el espacio donde se desplegarán las cámaras. Esto permite definir los puntos de grabación, los ángulos de visión, las zonas críticas y posibles obstáculos. Así se reducen las zonas ciegas y se evita tener que recolocar cámaras después.

También es importante calcular cuánta información generará cada cámara. No consume lo mismo una cámara básica que una cámara de alta resolución grabando muchas imágenes por segundo. Factores como la resolución, el códec de vídeo, la tasa de imágenes y el nivel de movimiento en la escena influyen directamente en el ancho de banda y en el almacenamiento necesario.

Este cálculo ayuda a dimensionar correctamente los switches, los enlaces principales y el sistema de grabación. Si no se hace bien, la red puede saturarse y provocar cortes, pixelación o pérdida de vídeo.



Además, la planificación debe contemplar el crecimiento futuro. Muchas instalaciones empiezan con un número reducido de cámaras y, con el tiempo, necesitan ampliar cobertura, mejorar resolución o añadir nuevos puntos de vigilancia. Diseñar la red pensando en esa evolución evita tener que rehacer la infraestructura más adelante.

Capa de acceso: donde realmente se sostiene la videovigilancia

Los switches donde se conectan las cámaras tienen un papel fundamental. No solo proporcionan conexión de red y alimentación, sino que también ayudan a mantener el tráfico ordenado, seguro y estable.

Una buena práctica es separar el tráfico de vídeo del resto de la red mediante una **VLAN dedicada para videovigilancia**. Esta segmentación evita que el tráfico habitual de oficina, como navegación web, descargas o impresoras, interfiera con las cámaras. Además, permite aplicar de forma más ordenada políticas como **QoS** (Calidad de Servicio), **Port Isolation** (Aislamiento de Puertos) o control de tráfico en los puertos donde se conectan los dispositivos de vídeo.

En algunos switches, esta configuración puede simplificarse mediante perfiles específicos para videovigilancia. Estos perfiles permiten agrupar en una misma configuración la VLAN de cámaras, la priorización del tráfico, el aislamiento de puertos y otras medidas de estabilidad. El objetivo es reducir errores de configuración y acelerar el despliegue, especialmente en instalaciones con muchas cámaras.

También es importante evitar errores físicos de conexión. En instalaciones con varios switches, una conexión incorrecta puede crear un bucle de red. Cuando esto ocurre, los datos empiezan a circular sin control y pueden saturar toda la infraestructura. Para prevenirlo, funciones como **Loop Detection** (Detección de bucle) permiten detectar estos bucles y actuar sobre el puerto afectado antes de que el problema impacte al sistema completo.

Otro aspecto clave es la priorización del vídeo. En una red compartida, no todo el tráfico tiene la misma importancia. El vídeo en directo necesita continuidad, especialmente en seguridad. Mediante **QoS**, la red puede dar prioridad al tráfico de vídeo frente a otros datos menos sensibles, ayudando a reducir retrasos, cortes o pixelación.

La seguridad también debe aplicarse desde el propio puerto de red. Con **Port Isolation**, una cámara conectada a un switch puede quedar aislada del resto de dispositivos y comunicarse solo con los equipos necesarios, como el grabador o el servidor de vídeo. Esto reduce riesgos si un dispositivo se comporta de forma anómala o se ve comprometido.

Además, funcionalidades como **Storm Control** ayudan a proteger la red frente a exceso de tráfico generado por errores, bucles o dispositivos defectuosos. En videovigilancia, esta protección es importante porque una tormenta de tráfico puede afectar a muchas cámaras al mismo tiempo.



Alimentación PoE: continuidad y recuperación automática

Muchas cámaras reciben alimentación eléctrica a través del propio cable de red mediante **PoE** (Alimentación a través de Ethernet). Esto simplifica mucho la instalación, pero también hace que el switch sea una parte crítica del sistema.

Por este motivo, es fundamental calcular correctamente la potencia PoE disponible. Cada cámara consume una cantidad determinada de energía, y algunas pueden requerir más potencia si tienen infrarrojos, calefactor, motor PTZ u otras funciones avanzadas. Si la potencia no está bien dimensionada, pueden aparecer reinicios, desconexiones o comportamientos inestables.

En instalaciones profesionales, funcionalidades como **Continuous PoE** aportan una ventaja importante. Permiten que las cámaras sigan recibiendo alimentación incluso durante ciertos reinicios o actualizaciones del switch. Esto ayuda a mantener la grabación activa y reduce interrupciones innecesarias.

Otra función especialmente útil es **PoE Recovery**. Esta característica permite supervisar si una cámara deja de responder y, en caso necesario, reiniciar automáticamente la alimentación del puerto PoE. En la práctica, si una cámara se bloquea, el sistema puede “apagar y encender” ese puerto sin que tenga que desplazarse un técnico.

Esto mejora la disponibilidad del sistema y reduce tiempos de intervención, algo especialmente valioso en instalaciones con muchas cámaras o ubicaciones remotas. También conviene tener en cuenta funcionalidades como **PoE Extend**, que permiten alcanzar distancias superiores a las habituales en determinados escenarios. Esto puede ser útil cuando una cámara está alejada del rack o del armario de comunicaciones, siempre que el diseño de red lo contemple correctamente.

Diagnóstico físico: detectar fallos sin desplazamientos innecesarios

En videovigilancia, muchos problemas no están en la cámara ni en el grabador, sino en el cableado. Un cable dañado, mal crimpado o demasiado largo puede provocar cortes intermitentes, pérdida de enlace o alimentación inestable.

Por eso, contar con herramientas como **Cable Test** facilita mucho el mantenimiento. Esta función permite comprobar el estado del cable desde la plataforma de gestión o desde el propio switch, ayudando a identificar si existe un problema físico antes de enviar a un técnico.

Esto reduce tiempos de diagnóstico y evita intervenciones innecesarias. En lugar de revisar manualmente todos los puntos, el administrador puede detectar con más rapidez si el problema está en el cable, en el puerto, en la alimentación o en la propia cámara.

Gestión centralizada y herramientas de análisis de problemas

Una instalación de videovigilancia no termina cuando las cámaras empiezan a grabar. Para que el sistema sea realmente eficiente, es necesario poder supervisarlos, diagnosticar incidencias y mantenerlos de forma sencilla.

La gestión centralizada permite ver el estado de switches, cámaras conectadas, puertos, consumo PoE, tráfico de red y eventos relevantes desde una única interfaz. Esto es especialmente útil en instalaciones con muchas cámaras, varios edificios o sedes distribuidas.

Cuando se produce una pérdida de vídeo, esta visibilidad permite identificar más rápido el origen del problema. Puede tratarse de una cámara bloqueada, un cable defectuoso, un puerto apagado, falta de alimentación PoE o saturación de tráfico. Sin una visión centralizada, el diagnóstico suele ser más lento y depende mucho más de desplazamientos físicos.

En este punto, las herramientas de análisis de problemas son especialmente importantes. Funciones como **Cable Test**, **Packet Capture**, registros de eventos, mapas de red y alertas ayudan a entender qué está ocurriendo en la instalación sin tener que estar físicamente delante del equipo.

Una funcionalidad especialmente útil es **Remote Access**. Permite acceder de forma remota a determinados dispositivos o interfaces de gestión de la red para revisar el estado del sistema, comprobar configuraciones o analizar una incidencia sin necesidad de desplazarse inicialmente a la instalación. En la práctica, esto permite al equipo técnico hacer un primer diagnóstico mucho más rápido y decidir si el problema puede resolverse en remoto o si realmente requiere una intervención presencial.

Esto tiene un impacto directo en el mantenimiento: se reducen tiempos de respuesta, se evitan desplazamientos innecesarios y se mejora la continuidad del servicio. En videovigilancia, donde una cámara fuera de servicio puede dejar una zona sin cobertura, poder actuar rápidamente marca una diferencia importante.

Además, la gestión puede adaptarse al tipo de instalación. En entornos donde no se desea depender de Internet, puede optarse por una gestión local. En proyectos donde se necesita supervisión remota, una gestión en la nube permite revisar el sistema desde cualquier ubicación y actuar con mayor rapidez.

Mantenimiento proactivo: anticiparse antes de que el sistema falle

Una red bien gestionada no solo sirve para resolver problemas cuando ya han ocurrido. También permite anticiparse.

Supervisar el consumo de ancho de banda, el uso de PoE, el estado de los enlaces y los eventos de red ayuda a detectar comportamientos anómalos. Por ejemplo, una cámara que empieza a consumir más energía de lo habitual, un puerto con errores o un enlace que se desconecta de forma intermitente pueden ser señales tempranas de una incidencia.

Este enfoque preventivo es especialmente importante en videovigilancia, porque el objetivo no es solo recuperar el servicio, sino evitar que deje de funcionar en momentos críticos.

Aquí cobran valor funciones como **PoE Recovery**, **Continuous PoE**, **Loop Detection**, **Storm Control**, **Cable Test**, **Packet Capture** y **Remote Access**. Combinadas, permiten no solo mantener las cámaras conectadas, sino también entender por qué se ha producido una incidencia y actuar con rapidez.

Por ejemplo, si una cámara deja de responder, **PoE Recovery** puede reiniciar automáticamente su alimentación. Si el problema está en el cableado, **Cable Test** ayuda a detectarlo. Si se sospecha de un problema de tráfico o comunicación, **Packet Capture** permite analizar qué está pasando en la red. Y si es necesario revisar la interfaz de un dispositivo o validar una configuración, **Remote Access** permite hacerlo sin desplazamiento inicial.

El resultado es una operación mucho más eficiente: menos tiempo de diagnóstico, menos visitas innecesarias y mayor disponibilidad del sistema de videovigilancia.



Conclusión

La videovigilancia profesional necesita una red fiable, ordenada y fácil de gestionar. Las cámaras son la parte más visible del sistema, pero la red es la base que permite que el vídeo llegue correctamente, se grabe sin interrupciones y pueda supervisarse de forma eficiente.

Planificar bien la instalación, separar el tráfico mediante una **VLAN dedicada para videovigilancia**, priorizar el vídeo con **QoS**, proteger la red con funciones como **Loop Detection**, **Port Isolation** y **Storm Control**, y mantener la continuidad mediante **Continuous PoE** y **PoE Recovery** permite construir sistemas mucho más estables.

Además, disponer de herramientas de diagnóstico como **Cable Test**, **Packet Capture** y **Remote Access** permite analizar incidencias de forma remota, reducir tiempos de respuesta y evitar desplazamientos innecesarios.

En definitiva, una buena red no solo conecta cámaras: garantiza continuidad, facilita el mantenimiento y aporta tranquilidad al usuario final.

Por último, es importante recordar que muchas de estas funcionalidades solo aportan todo su valor cuando el instalador cuenta con una formación adecuada en redes IP. Conceptos como VLAN, QoS, PoE, segmentación, aislamiento de puertos, diagnóstico de cableado o acceso remoto requieren una correcta planificación y configuración. Por ello, además de elegir equipos preparados para videovigilancia profesional, es fundamental que el instalador disponga de los conocimientos necesarios para diseñar, implementar y mantener la red de forma segura, estable y eficiente.

CONOCE A UNA **SOCIA**

Laura
Díaz
Enríquez

SOCIA N° 198



Buenos días, Laura. Lo primero que te pido es que te presentes a nuestros socios y lectores para que podamos empezar a conocerte.

Buenos días, ante todo agradecer esta oportunidad, que hayáis querido contar conmigo para esta sección de AEINSE y conocer un poco más de mí, de mi trayectoria profesional y de todo lo que me vincula a este mundo.

Soy Laura Díaz Enríquez, titulada en ingeniería de Diseño Industrial, y aunque mis inicios en el mundo laboral no tuvieron mucho que ver con la seguridad, llevo dedicándome a ello desde 2015 justo después de la entrega de mi proyecto fin de carrera. Desde entonces hasta la actualidad no he dejado de estar vinculada a este tipo de proyectos, en los que cada vez me siento más cómoda y a gusto.

Siempre he entendido la ingeniería como una profesión en constante evolución, por lo que la formación continua y la mejora de procesos han sido dos pilares fundamentales en mi desarrollo profesional. Me considero una persona comprometida, organizada y orientada a ofrecer soluciones que aporten valor tanto a los clientes como a los equipos con los que trabajo.

¿Cuál es tu formación académica?

Mi formación tiene una base técnica, como ya he comentado soy ingeniera especializada en diseño industrial. Posteriormente he ido complementando con formación especializada en distintas áreas relacionadas con la gestión de proyectos, la seguridad, la normativa y las nuevas tecnologías. Considero que la formación no termina con la obtención de un título, sino que debe mantenerse a lo largo de toda



la vida profesional para adaptarse a un entorno que evoluciona constantemente.

¿Cuáles estimas que son tus puntos fuertes en el terreno laboral?

Creo que uno de mis principales puntos fuertes es la capacidad de organización y planificación. Me gusta analizar los proyectos de forma global, anticipar posibles problemas y coordinar los distintos recursos para que todo funcione de forma eficiente.

También destacaría mi capacidad para trabajar en equipo, comunicarme con perfiles muy diferentes y mantener la calma ante situaciones complejas. Intento afrontar cada proyecto con responsabilidad, cercanía y una actitud orientada a la búsqueda de soluciones. En mi opinión es muy importante crear un entorno de confort en el que tanto cliente como instaladores, técnicos y personal directivo, puedan sentirse cómodos y motivados en crear las soluciones más adecuadas adaptadas a las necesidades que aparezcan durante el desarrollo del proyecto.

A la vista de tu currículum deduzco que eres una persona preocupada por tu formación. De los cursos realizados, ¿cuáles destacarías como los más útiles para tu desarrollo profesional?

Cada etapa profesional me ha requerido adquirir conocimientos diferentes, por lo que resulta difícil elegir unos pocos. Sin embargo, destacaría aquellos relacionados con la especialización de sistemas de videovigilancia y CCTV, y sistemas anti-intrusión en los que además se me facilitó el acceso a ellos a través de esta asociación a raíz del acuerdo de colaboración entre ESSIIF y AINSE.

La normativa aplicable a las instalaciones de seguridad y la formación en nuevas tecnologías y energías renovables lo considero algo crucial en cualquier trayectoria profesional. También considero muy valiosos los cursos centrados en habilidades de liderazgo y gestión de equipos, porque la parte técnica es esencial, pero saber coordinar personas y comunicar eficazmente también resulta determinante para el éxito de cualquier proyecto.

¿En qué empresas, sectores y puestos has desarrollado tu actividad profesional?

Inicialmente comencé mi trayectoria colaborando en proyectos de climatización para una empresa pequeña a través de una beca, aquí terminaron haciéndome mi primer contrato, pero llegó el momento en el que necesitaba seguir avanzando y estar allí no me lo permitía, por lo que terminé desvinculándome, gracias a

lo que en tan solo 2 meses me dio la oportunidad de adentrarme en este mundo de la seguridad.

La primera empresa en la que pude desarrollar mi actividad profesional en el ámbito de la seguridad fue Innovación Global de la Seguridad en la que estuve 6 años desempeñando varias funciones y adquiriendo conocimientos que me han permitido estar hoy donde estoy, agradecida a los compañeros y a todo el entorno que me rodeó durante esa etapa.

Posteriormente y sin descanso, me incorporé a la empresa INECO en la que llevé, como asistencia técnica e ingeniera de sistemas, el proyecto RS3 de RENFE en la zona Sur (Andalucía y Extremadura) durante 3 años y medio, y actualmente desde hace poco más de un año trabajo para la constructora Torrecamara como jefa de instalaciones, colaborando en un proyecto de rehabilitación de un centro Penitenciario Psiquiátrico en el que la seguridad es el factor más importante a tener en cuenta en todos los aspectos.

Esta diversidad de experiencias me ha permitido adquirir una visión amplia de las instalaciones y comprender que, aunque cada sector tenga sus particularidades, la planificación, la calidad y el compromiso con el cliente siempre son factores comunes.

Comenzaste trabajando en climatización ¿Qué te llevó a moverte al sector de la seguridad?

Fue una evolución natural motivada por la búsqueda de nuevos retos profesionales. El sector de la seguridad me llamó la atención porque combina ingeniería, tecnología e innovación de una forma muy dinámica.

Además, es un ámbito con una gran responsabilidad, ya que el trabajo que realizamos contribuye directamente a proteger personas, infraestructuras y organizaciones. Esa combinación de componente técnico e impacto real fue lo que terminó de convencerme.

Como Jefa de Instalaciones, que hay que atender a muchos palos, ¿qué labor consideras más importante para llevar a buen término un proyecto?

Sin duda, la planificación y la coordinación. Un proyecto puede contar con muy buenos profesionales y excelentes recursos, pero si no existe una planificación adecuada y una comunicación fluida entre todas las partes, es muy difícil alcanzar los objetivos previstos. También considero fundamental anticiparse a los posibles riesgos y mantener un seguimiento continuo de la ejecución para poder tomar decisiones a tiempo.



¿Y cuál te parece la más incómoda y tediosa?

Probablemente la gestión administrativa y documental cuando se convierte en un proceso excesivamente burocrático. Es una parte imprescindible para garantizar la trazabilidad, la calidad y el cumplimiento normativo, pero en ocasiones consume un tiempo muy valioso que podría dedicarse a tareas más técnicas o de mayor valor añadido. Aun así, entiendo que forma parte de la responsabilidad del puesto y es necesario realizarla con el mismo rigor que el resto de las funciones.

Con el desarrollo tan rápido de la tecnología que estamos viviendo, ¿crees que el personal de instalación y puesta en marcha está, en términos generales, suficientemente capacitado o, por el contrario, necesita más formación?

Creo que el nivel profesional del personal técnico es cada vez mayor, pero la velocidad a la que evoluciona la tecnología hace que la formación continua sea imprescindible.

Hoy en día un instalador ya no solo debe conocer los sistemas físicos tradicionales, sino también redes de comunicaciones, integración de sistemas, software y conceptos básicos de ciberseguridad, y es aquí donde quizás sí existan más limitaciones. La formación debe entenderse como una inversión estratégica tanto para las empresas como para los propios profesionales.

El actual crecimiento de las ciberamenazas está llevando a las empresas a dedicar recursos, tanto humanos como económicos, para protegerse de las mismas. ¿Piensas que la ciberseguridad está desplazando a la seguridad física?

No creo que la esté desplazando; más bien considero que ambas disciplinas están convergiendo. Los sistemas de seguridad física actuales están cada vez más conectados y digitalizados, por lo que protegerlos también implica proteger su infraestructura tecnológica. La seguridad del futuro pasa por una visión integral en la que la seguridad física y la ciberseguridad trabajen de forma coordinada, compartiendo información y estrategias para ofrecer una protección más completa.

Aparte del trabajo diario, que seguro te absorbe gran parte del tiempo, ¿qué aficiones son tu válvula de escape y qué te gusta hacer?

Intento dedicar tiempo a actividades que me permitan desconectar y mantener un equilibrio entre la vida profesional y personal. Disfruto mucho haciendo deporte, viajando siempre que puedo y practican-

do actividades al aire libre, además me encanta pasar tiempo con mi familia y amigos. También me gusta leer y seguir aprendiendo sobre temas relacionados con la innovación y la tecnología, aunque procurando reservar espacios para desconectar completamente del trabajo.

¿Cómo conociste AINSE y qué te movió a asociarte?

Conocí AINSE a través de compañeros del sector y de diferentes encuentros profesionales. Lo que más me llamó la atención fue su papel como punto de encuentro para compartir conocimiento, experiencias y buenas prácticas entre profesionales de la seguridad. Considero que formar parte de una asociación permite mantenerse actualizado, ampliar la red de contactos y contribuir al crecimiento y profesionalización del sector.

¿Qué propondrías a la Asociación para mejorar y aportar más valor a los socios?

Creo que AINSE ya realiza una labor muy importante, pero siempre existen oportunidades para seguir creciendo. Apostaría por reforzar las actividades formativas sobre tecnologías emergentes, impulsar grupos de trabajo especializados y fomentar espacios de intercambio entre profesionales de diferentes generaciones y especialidades.

También considero interesante acercar aún más la Asociación a los jóvenes ingenieros y estudiantes, para despertar su interés por el sector de la seguridad y facilitar el relevo generacional.



Security Forum'26

**JUN
2026**

Los pasados días 3 y 4 de junio tuvo lugar en el recinto histórico de las Drassanes Reials de Barcelona la edición 13ª de Security Forum. El evento, organizado por Cuadernos de Seguridad, impulsado por Peldaño Media Group y con la colaboración del Ayuntamiento de Barcelona, tuvo como objetivo facilitar el diálogo profesional y activar nuevas oportunidades de negocio entre quienes lideran el presente y el futuro de la seguridad.

Más que un espacio expositivo, su misión es convertirse en el espacio donde confluyen las necesidades reales de las empresas y las soluciones más innovadoras del mercado. Por ello, estuvo organizado en tres espacios:

Business Hub: Reuniones agendadas entre clientes y proveedores.

THE LAB: Ponencias sobre las últimas tendencias en seguridad integral, destacando el uso de la IA, la ciberseguridad, la autenticación de imágenes y vídeos, el cibercrimen.

ZONA EXPO: En la que fue posible el contacto directo de más de 3.000 visitantes con las soluciones pioneras y los desarrollos más innovadores.

[+información](#)



Despedida de Manuel Yanguas, comisario jefe de la Unidad de Seguridad Privada



ABR
2026

El pasado 12 de abril, con motivo de su jubilación, Manuel Yanguas dejó su cargo en la UCSP. Unidad a la que estuvo ligado desde el año 2014. Siendo su jefe desde 2020 tras su ascenso a comisario principal, poco antes de la pandemia. Siendo su primer reto la gestión de las necesidades relacionadas con los servicios de seguridad durante la misma.

En una carta abierta al sector, expresó su agradecimiento a los profesionales de seguridad privada en la que manifiesta *"A lo largo de estos años he vivido innumerables experiencias colectivas y personales que han dejado una huella profunda en mi trayectoria profesional y, sobre todo, en lo personal. He tenido la suerte de compartir numerosas ocasiones con grandes profesionales, personas comprometidas, responsables y, sobre todo, con un fuerte sentido del deber"*

Desde **AEINSE** le agradecemos su proximidad y disponibilidad para tratar diferentes cuestiones relativas a las funciones de nuestro colectivo y a la colaboración entre los ámbitos público y privado de la seguridad.

Seg2

18º Encuentro Seguridad Integral



**JUN
2026**

El pasado 24 de junio se celebró en Madrid el evento anual Seguridad Integral. Organizado por las revistas Red Seguridad y Seguritecnia y bajo el lema “Soberanía digital, Defensa y Seguridad España, varios expertos en la materia abordaron los retos a los que actualmente hace frente el sector en un contexto internacional convulso.

En las distintas ponencias se trataron, entre otros, aspectos relativos al nuevo paradigma marcado por la IA, la dependencia de española en cuestión tecnológica y las nuevas herramientas desarrolladas en España, la soberanía digital y la resiliencia”.

[+ información](#) 

LEÍDO, VISTO Y OÍDO EN...



Cuadernos de seguridad

Revista nº 386 - pág. 48

Artículo de **José Ramón Becerra**, Presidente de la Asociación española de Centrales Receptoras de Alarma (ASCRA), que bajo el título **“Centrales Receptoras de Alarmas. Futuro muy condicionado por el presente”**, analiza la presumible evolución de las CRAs desde cuatro puntos de vista: Especialidades operativas, Profesionalización de las empresas, Mejorar la calidad del servicio y el contexto legal.

[Leer artículo](#)



LEÍDO, VISTO Y OÍDO EN...



Blog INCIBE

“Una pyme puede atender una llamada aparentemente normal y encontrarse ante un fraude, recibiendo, por ejemplo, una llamada falsa que busca engañar a sus empleados. Pero también puede ocurrir lo contrario, que sus clientes reciban llamadas falsas en las que aparece el número real de la empresa. En ambos casos, el problema es el mismo: spoofing telefónico o suplantación del identificador de llamada.”

Interesante artículo que explica en qué consiste y como funciona este fraude basado en suplantación de identidad por parte del delincuente

[Leer artículo](#)



LEÍDO, VISTO Y OÍDO EN...



El valor de un centro de control

Seguritecnia nº 518 - pág. 58

“El valor de un centro de control ya no se mide por cuantos operadores o pantallas incluye, cuántos sistemas concentra o cuantos eventos procesa. La cuestión es otra: consiste en saber si ese centro ayuda a la organización a anticiparse, a entender mejor lo que ocurre y a tomar decisiones con más contexto”.

Artículo de nuestro compañero **Enrique Bilbao** que nos habla del **Centro de control que viene: de monitorización a “hub” de inteligencia operativa**.

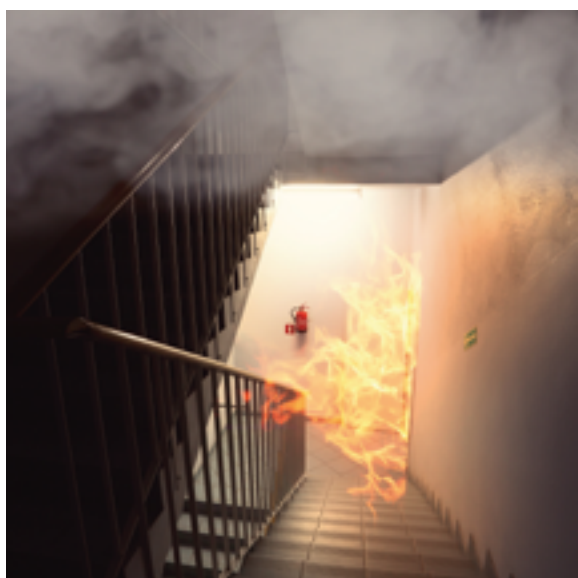


LEÍDO, VISTO Y OÍDO EN...



**Fundación
mapfre**

Informe Víctimas de incendios en España 2024 de la Fundación MAPFRE



“De nuevo, malas noticias: las terceras peores cifras de fallecidos por incendios y explosiones en España desde el año 2010. Si hay una conclusión que se repite año tras año en este informe, es que hay que instalar detectores de incendios en las viviendas. Los detectores de incendios reducen a la mitad el riesgo de morir en nuestros hogares por incendio. Alrededor de 85 personas que salvarían su vida cada año en España con esta medida”

[+información](#) 

PATROCINADORES

ADI

AXIS
COMMUNICATIONS

Casmar
Compromiso con la seguridad

ahua
TECHNOLOGY

DESICO

DORLET

ff FFV
GEUTEBRÜCK

HID

IQSIGHT

Hanwha Vision

Johnson Controls

LANACCESS 30 años

LEGIC

Sicuralia
Sistemas

VIGI
by tp-link

SCATI

ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD
BOLETÍN N°67 JULIO 2026

AEINSE
Asociación Española de
Ingenieros de Seguridad