BOLETÍN Nº66 MAY 2026

AEINSE
Asociación Española de Ingenieros de Seguridad

Critical Entities Resilience CER

ADI AXIS COMMUNICATIONS casmar alhua TECHNOLOGY DESICO DORLET FFV GEUTEBRÜCK IQSIGHT
Hanwha Vision HID Johnson Controls LANACCESS LEGIC Sicuralia SCATI VIGI by tp-link

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

Lo que sabemos que sabemos y lo que sabemos que no sabemos...

Ley de protección y resiliencia de las entidades críticas

El papel del ingeniero de seguridad

La Directiva (UE) 2022/2557 sobre la resiliencia de las entidades críticas (Critical Entities Resilience – CER) tiene como objetivo reforzar la capacidad de las entidades esenciales para prevenir, resistir, responder y recuperarse frente a incidentes graves como sabotajes, ciberataques, desastres naturales o fallos operativos.

Esta norma amplía el enfoque tradicional de protección de infraestructuras críticas, pasando de la protección exclusiva de la infraestructura física a la garantía de la continuidad operativa de toda la entidad crítica.

En España, su transposición se materializará mediante la Ley de Protección y Resiliencia de Entidades Críticas que, de momento, es un Proyecto de Ley aprobado por el Consejo de Ministros en marzo 2026, pero pendiente de aprobación por el Congreso. La Ley sustituirá progresivamente el marco anterior establecido por la Ley 8/2011 de Protección de Infraestructuras Críticas.

¿Qué sabemos del Proyecto de Ley?

De acuerdo con el Proyecto de Ley de Protección y Resiliencia de Entidades Críticas, en adelante el "Proyecto" podrán instalar sistemas antidrones y sistemas de reconocimiento biométrico en el control de acceso a sus instalaciones.

Pero lo más relevante de la futura ley, es que producirá un cambio significativo en el marco jurídico. Su futuro desarrollo reglamentario incorporará aspectos como los riesgos operacionales con impacto significativo en el suministro del servicio esencial, el desarrollo de planes de resiliencia, la continuidad de negocio y una mayor coordinación público-privada.

Por riesgos operacionales con impacto significativo en el suministro del servicio esencial debemos entender una parte de los riesgos relacionados con la interrupción del negocio.

Estos riesgos pueden tener su origen en errores humanos, fallos técnicos, deficiencias de proceso, accidentes, interrupciones en la cadena de suministro, fenómenos naturales o acciones deliberadas, tanto en el ámbito de la seguridad física como en el de la ciberseguridad.

¿Qué no sabemos del Proyecto de Ley?
En general, las empresas gestionan sus riesgos con mayor o menor rigor y profundidad en función de su tamaño, sector y obligaciones de cumplimiento normativo. Por ejemplo:

- Las empresas cotizadas en Bolsa deben disponer de un sistema de gestión de riesgos que contemple aquellos que puedan afectar a los objetivos de la organización.
- El gestor de una pyme suele tener identificados los riesgos que amenazan la continuidad del suministro y las medidas necesarias para mitigarlos.

Una parte de los riesgos de continuidad de negocio de una empresa puede coincidir con los riesgos de continuidad del suministro.

¿Es válida la clasificación de los riesgos de continuidad de negocio para gestionar también los riesgos de continuidad del suministro? Entendemos que sí, en la medida en que el impacto sobre la continuidad de negocio exija su tratamiento cuando también exista impacto sobre la continuidad del suministro, y viceversa. No obstante, dejará de ser válida cuando no exista esa correspondencia.

Uno de los aspectos más complejos en el desarrollo y aplicación del nuevo marco jurídico será establecer las métricas que permitan determinar en qué casos los riesgos para la continuidad del suministro requieren tratamiento. Dicho de otra forma: será necesario definir la tolerancia al riesgo de interrupción del servicio esencial.

Esta tolerancia al riesgo puede variar según el sector o subsector, aunque deberá existir un criterio común que aporte coherencia al nuevo sistema de protección de entidades críticas. Por ejemplo:

- La tolerancia al riesgo en la interrupción del servicio de distribución eléctrica es mucho menor que en la distribución de agua.
- La tolerancia al riesgo en la interrupción del servicio de metro puede ser inferior a la del aeropuerto.

Pero surge una cuestión relevante: ¿cómo comparar la tolerancia al riesgo entre sectores distintos? Por ejemplo, ¿tolera mejor una ciudad como Madrid una interrupción de cuatro horas en el sistema de distribución de agua o en la actividad aeroportuaria? ¿Cuál es el papel del ingeniero de seguridad?

En el ámbito de las infraestructuras críticas, este cambio normativo implica pasar de un sistema centrado en la protección a un enfoque mucho más amplio basado en la resiliencia: prevención, protección, respuesta, resistencia, mitigación, absorción, adaptación y recuperación ante incidentes.

El desarrollo reglamentario de la Ley establecerá previsiblemente una estrategia de mejora basada en el análisis de riesgos, posiblemente acompañada de guías para la elaboración de un Plan de Resiliencia —donde podrían integrarse los actuales PSO y PPE—, así como un esquema nacional de certificación.

Estas certificaciones no serán emitidas directamente por la Administración, sino por entidades privadas de certificación previamente acreditadas por la Entidad Nacional de Acreditación (ENAC). Se incorpora así un nuevo rol de supervisión y certificación independiente tanto del Operador Crítico como de la propia Administración.

Esto abre una nueva oportunidad profesional para la ingeniería de seguridad, más allá del actual desempeño en los departamentos de seguridad.

Si entendemos la protección de infraestructuras críticas como un proyecto integral, los ingenieros de seguridad podrán desempeñar funciones en algunas de las siguientes responsabilidades:

- En la elaboración del Plan de Resiliencia, en colaboración con áreas de la empresa hasta ahora no vinculadas a la seguridad tal como se entiende en el PSO y PPE. En la implantación del Plan de Resiliencia, mediante la implantación y mantenimiento de medidas de seguridad, ya sea desde una empresa instaladora o desde el equipo técnico del propio Operador Crítico.

- En la asistencia a procesos de consultoría, que tradicionalmente se limitaban al ámbito de la seguridad física y la ciberseguridad, pero que ahora se amplían al ámbito de la continuidad operativa.

¿Cuál será el papel de AEINSE?
Es evidente que este nuevo enfoque exigirá una ampliación de las competencias de los profesionales de la seguridad.

En este contexto, AEINSE ha incorporado en su grupo de expertos del área de Gestión de Riesgos una nueva línea de trabajo orientada al desarrollo de las competencias del Ingeniero de Seguridad dentro de este nuevo marco legal.

Esta línea de trabajo pretende desarrollar herramientas, criterios y recursos que permitan a los miembros de AEINSE dar una respuesta adecuada al rol que les corresponda desempeñar en sus respectivas organizaciones.

Conclusiones:

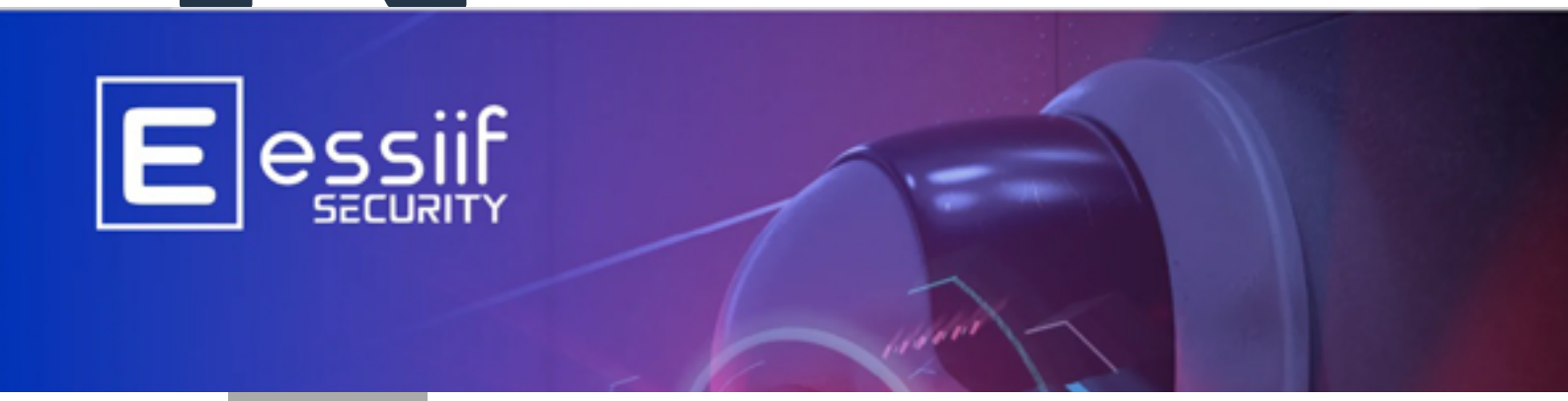
La futura Ley de Protección y Resiliencia de las Entidades Críticas no supone únicamente una actualización normativa, sino un cambio de paradigma en la forma de entender la seguridad de los servicios esenciales.

Pasamos de un modelo centrado principalmente en la protección de infraestructuras físicas a otro orientado a garantizar la continuidad operativa de toda la organización frente a amenazas cada vez más complejas, interdependientes y cambiantes.

Este nuevo escenario exige profesionales capaces de integrar la seguridad física, la ciberseguridad, la gestión de riesgos, la continuidad de negocio y la resiliencia organizacional en una visión única y coherente.

El ingeniero de seguridad se sitúa, por tanto, en una posición estratégica, no solo como especialista técnico, sino como actor clave en la toma de decisiones que afectan a la estabilidad de los servicios esenciales y a la protección de la sociedad.

El verdadero reto no será únicamente cumplir con la nueva Ley, sino desarrollar una cultura de resiliencia capaz de anticiparse a la incertidumbre y garantizar la continuidad allí donde una interrupción no es una opción. En ese camino, AEINSE debe desempeñar un papel fundamental como punto de encuentro, desarrollo de conocimiento y fortalecimiento profesional de quienes tendrán la responsabilidad de construir esa nueva seguridad.



04 MAY 2026

AEINSE en los cursos de formación en seguridad de ESSIIF

Fruto de la colaboración entre ambas entidades, ya ha comenzado este año el programa de formación on line con la programación de siete cursos, algunos de ellos son impartidos por socios de AEINSE y que cuentan con el respaldo de la Universidad Isabel I y la Universidad Tecnológica Atlántico Mediterráneo.

El primero de ellos, **Curso de especialización en sistemas de videovigilancia y CCTV**, se desarrolló durante los meses de marzo y abril. Con 60 horas lectivas fue impartido por nuestro compañero **Gabriel García.**

El 4 de mayo se ha iniciado el **Curso de especialización en sistemas de control de accesos**, impartido por **Iván Ballesteros**, nuestro actual presidente, con 60 horas lectivas.

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

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

+INFORMACIÓN

ADI
AXIS COMMUNICATIONS
casmar
alhua TECHNOLOGY
DESICO
DORLET
FFV GEUTEBRÜCK
HID
IQSIGHT
Hanwha Vision
Johnson Controls
LANACCESS 30
LEGIC
Sicuralia
VIGI by tp-link
SCATI

Sistemas de grabación Geutebrück: seguridad, fiabilidad y rendimiento para entornos críticos

En el ámbito de la seguridad, contar con sistemas de grabación robustos es esencial para garantizar la protección y eficiencia de cualquier instalación. Los grabadores Geutebrück destacan además, por su compatibilidad con cámaras con analíticas de inteligencia artificial y su capacidad de integración con soluciones de terceros, adaptándose a proyectos de diversa complejidad y escala.

VIDEOSISTEMAS FFV GEUTEBRÜCK

Los sistemas de grabación Geutebrück se caracterizan por ofrecer:

Máxima seguridad:
Cuentan con certificación ISO 27001, garantizando un sistema de gestión de la seguridad de la información conforme a estándares internacionales de confidencialidad, integridad y disponibilidad. Incorporan múltiples capas de protección, como cifrado AES-256 y TLS, almacenamiento seguro y protección avanzada de credenciales.

Máxima fiabilidad
La solución hardware garantiza rendimiento y operación continua en entornos exigentes. Integra placa base industrial de ciclo extendido y chipset Intel, optimizado para ofrecer un procesamiento eficiente y mejorar la capacidad de respuesta del sistema. Su funcionamiento 24/7 garantizan su operatividad ininterrumpida en entornos críticos.

Máximas prestaciones
Permiten gestionar vídeo de alta resolución con eficiencia y escalabilidad, soportando H.265 y H.264. Admiten cámaras de hasta 32 MPX a 120 IPS, interoperabilidad ONVIF, hasta 128 canales y 450 TB de base de datos. Incluyen sistemas Failover y configuraciones RAID 1, 5 y 6 para mayor seguridad y disponibilidad.

+información

IVA Pro Context

Intelligent Video Analytics (IVA) Pro Context es un software de análisis de vídeo basado en tecnología de modelos de lenguaje natural a gran escala, diseñado para la comprensión avanzada de escenas y aplicaciones de vigilancia inteligente.

Alcanza niveles sin precedentes de conocimiento contextual para **detectar situaciones complejas, anomalías e infracciones de seguridad.**

El sistema combina la detección de objetos tradicional con una sofisticada comprensión del lenguaje natural mediante un **motor de procesamiento de Inteligencia Artificial Generativa (GenAI) basado en la nube**, pasa obtener información contextual y detallada sobre las escenas monitorizadas.

Los datos recopilados se pueden presentar al usuario en tres formatos distintos: mediante señales de alarma en formato binario, en formato de descripción detallada, o extrayendo caracteres alfanuméricos.

Todo ello permite elaborar información útil para **mejorar la seguridad y la eficiencia operativa en diversos entornos**, como almacenes, locales comerciales e instalaciones industriales.

Sus robustos sistemas de gestión y moderación garantizan un funcionamiento fiable y conforme a la normativa.

BLAZE VMS

Hanwha Vision, amplía su ecosistema de video con BLAZE VMS, un sistema híbrido de gestión de vídeo diseñado para simplificar el despliegue del sistema, las acciones impulsadas por Inteligencia Artificial y la gestión de múltiples ubicaciones y sedes.

BLAZE ofrece compatibilidad total, nativa, con cámaras y dispositivos de Hanwha, y combina el rendimiento de sistemas locales con gestión en nube y administración unificada de usuarios. Esta arquitectura híbrida permite a las organizaciones gestionar de forma eficiente múltiples ubicaciones de forma segura, con una arquitectura escalable y un control centralizado de usuarios. Además, detecta automáticamente los dispositivos conectados y aplica configuraciones optimizadas, lo que permite a los integradores desplegar sistemas más rápidamente con una configuración manual mínima.

BLAZE funciona de forma integrada con WiseAI de Hanwha, facilitando búsquedas forenses más ágiles. La función Similarit Search utiliza Inteligencia Artificial para localizar apariciones similares de una persona en distintas cámaras, lo que ayuda a los operadores a seguir rápidamente su recorrido a través de grandes instalaciones o múltiples ubicaciones.

Los sistemas **BLAZE** también incorporan Semantic Search, impulsado por Inteligencia Artificial generativa, permitiendo a los operadores utilizar consultas en lenguaje natural para localizar eventos.

BLAZE también estará disponible con dispositivos dedicados (Appliances), optimizados específicamente para la plataforma. Estos equipos se suministran con licencias preinstaladas, listos para funcionar desde el primer momento.

+ información BLAZE VMS

Johnson Controls Security Products lanza una nueva herramienta para facilitar la gestión eficaz de incidentes que es un elemento clave en la operativa diaria de las organizaciones que deben garantizar altos niveles de seguridad, trazabilidad y cumplimiento normativo.

C•CURE IQ Incident Management:

control y eficiencia ante cualquier incidente

C•CURE IQ Incident Management responde a esta necesidad con una solución nativa que estructura todo el ciclo del incidente, desde su detección hasta su completa resolución y documentación.

Integrado directamente en la plataforma **C•CURE IQ**, el sistema permite crear incidentes de forma automática a partir de eventos o alarmas, vinculándolos al contexto operativo y a las evidencias disponibles, como vídeo en tiempo real o grabado.

A partir de ese momento, el operador es guiado mediante flujos de trabajo que aseguran la correcta recogida de datos, la aplicación de los procedimientos definidos y una actuación rápida y coherente.

Se facilita la adaptación de los procesos a distintos tipos de incidentes, requisitos regulatorios o normas corporativas, mediante el uso de flujos de trabajo configurables y un diseñador visual. Además, cuenta con una herramienta para la generación de informes claros y exportables simplificando auditorías internas y externas.

Con este enfoque, **C•CURE IQ Incident Management** estandariza los procesos, mejora la calidad de la información registrada y refuerza la capacidad de los equipos de seguridad para actuar con precisión, consistencia y confianza.

Lanaccess consigue la certificación de la Directiva NIS 2

Lanaccess ha obtenido la certificación de la Directiva NIS 2, reforzando su apuesta por una videovigilancia cibersegura.

La **NIS2** afecta a entidades que operan en la Unión Europea en sectores críticos (energía, transporte, banca, salud, telecomunicaciones, centros de datos, etc.). Exige gestionar riesgos de ciberseguridad y reportar incidentes con plazos definidos, con sanciones que, según la categoría, pueden alcanzar 10 M€ o el 2 % de la facturación global anual.

Como directiva, **NIS2** no se aplica directamente como un reglamento: necesita trasposición para desplegar el régimen nacional completo (autoridades, procedimiento sancionador, obligaciones concretas y cómo se exigen). En el país, aún no hay una trasposición aprobada y en vigor.

La estrategia de la compañía pasa por consolidar nuestro compromiso con la ciberseguridad a través de las certificaciones internacionales más rigurosas.

- **Certificación del ENS (Esquema Nacional de Seguridad), Nivel Alto:** esta certificación garantiza que una organización cumple con los requisitos más estrictos establecidos por el marco legal español para la protección de sistemas de información que manejan datos sensibles o críticos. Expedida por el CCN (Centro Criptológico Nacional).

- **La ISO27001:** normativa internacional que obliga a proteger la confidencialidad, integridad y disponibilidad de los datos.

+información

LEGIC
Presente en ISC West Las Vegas

En ISC West 2026, LEGIC tuvo una presencia sólida y destacada, caracterizada por un gran número de reuniones y un diálogo significativo con el sector. El evento confirmó el impulso continuo de la innovación en materia de acceso seguro y la colaboración en el ecosistema.

Uno de los aspectos más destacados fue el anuncio de **LEGIC** sobre su estrategia de integración de **Aliro** (Protocolo de comunicación estandarizado entre lectores de acceso y dispositivos de usuario, tales como smartphones) destinada a permitir la interoperabilidad de última generación entre las tecnologías de acceso.

La empresa está avanzando en la compatibilidad entre su serie 6000 y su futura cartera de lectores, con rutas de actualización de firmware que permiten a muchas instalaciones existentes adoptar **Aliro** sin necesidad de sustituir el hardware.

La solución ya se está mostrando a socios seleccionados, y su disponibilidad inicial está prevista para septiembre de 2026, sujeta a la validación final y la aceptación por parte de los clientes. Más allá del recinto ferial, **LEGIC** reforzó sus relaciones con el sector como patrocinador del evento Wine & Security, fomentando un valioso intercambio en un entorno más informal.

Otro hito notable fue la implementación visible de la tecnología de **LEGIC** en **Resorts World Las Vegas**, donde sus soluciones protegen el acceso a más de 3000 habitaciones de hotel, demostrando su escalabilidad en un entorno real.

La semana concluyó con claras señales de progreso, colaboración y preparación para una adopción más amplia.

Sicuralia Systems

FORTE

La revolución en seguridad perimetral por fibra óptica

Sicuralia presenta FORTE, un innovador sistema de seguridad perimetral, basado en tecnología de fibra óptica, diseñado para ofrecer una vigilancia continua y fiable. Este sensor avanzado utiliza un principio de detección interferométrica que permite identificar y clasificar con precisión diversos intentos de intrusión, como escalada, corte o levantamiento de mallas.

Una de las ventajas más destacadas es su **Tecnología Cross Point**, capaz de localizar el punto de la intrusión con una precisión de hasta 4 metros. Además, al ser una tecnología 100% óptica, el sistema es totalmente inmune a las interferencias electromagnéticas y a los fenómenos atmosféricos, garantizando estabilidad en cualquier condición ambiental.

FORTE ofrece una eficiencia operativa superior, ya que el cable sensor es pasivo y no requiere alimentación eléctrica en el campo, lo que reduce significativamente los costes de instalación y mantenimiento. Mediante algoritmos de procesamiento de señales (FFT), el sistema distingue con éxito entre amenazas reales y ruidos ambientales, minimizando drásticamente las falsas alarmas.

Disponible en configuraciones que cubren hasta 800 metros por analizador, lo que permite la protección de hasta 1600m de vallado desde un único punto de alimentación y comunicaciones.

FORTE es una solución potente, escalable y discreta, ideal para la protección de infraestructuras críticas. Su capacidad para integrarse fácilmente en sistemas de seguridad y gestión más habituales como **Octave Coda, Milestone** o **Genetec**.

+información

VIGI by tp-link

Videovigilancia autónoma en cualquier lugar sin infraestructura

En un contexto donde la seguridad debe adaptarse a entornos cada vez más diversos, surgen soluciones capaces de superar las limitaciones tradicionales de infraestructura. La videovigilancia evoluciona hacia sistemas autónomos, flexibles y fáciles de desplegar, incluso en ubicaciones sin acceso a red eléctrica o cableado.

La solución de **Energía Solar 4G de VIGI by TP-Link** responde a esta necesidad, combinando alimentación mediante panel solar y conectividad 4G para ofrecer un sistema completamente independiente.

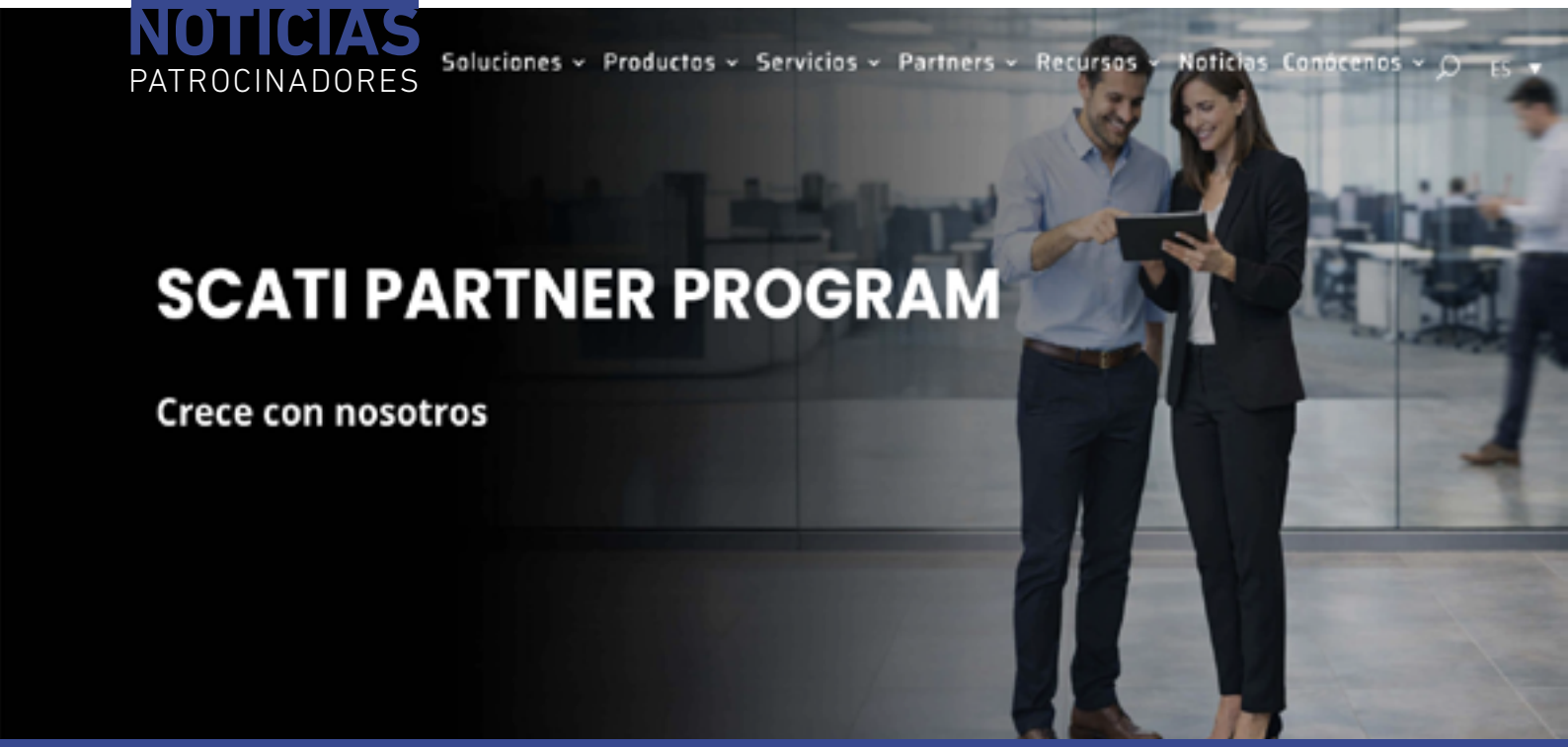
Esto permite implementar videovigilancia en cualquier lugar, reduciendo tiempos, costes y complejidad de instalación. Además, la gestión remota a través de plataformas como **VIGI Cloud VMS, Omada Central** o la **APP VIGI** facilita la monitorización en tiempo real, el envío de alertas y el mantenimiento sin desplazamientos. Dentro de esta solución destaca la cámara 4G de **VIGI**, diseñada para exteriores y con una característica diferencial clave: su función como router 4G.

Gracias a sus tres puertos LAN, permite conectar simultáneamente varios dispositivos, como cámaras adicionales u otros equipos, proporcionando conectividad directa sin necesidad de infraestructura adicional e incluso dando servicio al propio sistema del panel solar para su gestión.

Esta capacidad la convierte en una solución especialmente versátil, ampliando el alcance del sistema y simplificando el despliegue en entornos remotos o temporales.

+información

SCATI



SCATI impulsa el crecimiento de su red de socios con su nuevo Partner Program

SCATI refuerza su apuesta por el canal con el lanzamiento de su nuevo SCATI Partner Program, una iniciativa pensada para que integradores, distribuidores y empresas del sector accedan a más oportunidades de negocio, mayor respaldo comercial y mejores herramientas para crecer.

Formar parte del programa permite a los partners proteger sus oportunidades comerciales, contar con mayor visibilidad sobre su actividad y proyectos a través del **SCATI Partner Portal**, y trabajar con planes de negocio personalizados alineados con sus objetivos de crecimiento.

Además, las empresas obtienen acceso a formación y certificaciones técnicas y comerciales, así como a soporte continuo en todas las fases del ciclo comercial, desde la preventa hasta el cierre de proyectos. Todo ello les ayuda a mejorar su posicionamiento, reforzar sus capacidades y abordar nuevas oportunidades con más garantías.

Con esta iniciativa, **SCATI** consolida un modelo de colaboración orientado a generar valor real, impulsar la competitividad de sus socios y acompañarlos en un mercado cada vez más exigente.

"Queremos que nuestros partners no solo vendan nuestras soluciones, sino que crezcan con nosotros", destaca **Miguel Ángel Gimeno**, Marketing & BD Director de **SCATI**.

+información

AV1, AXIS ARTPEC 9 y overlays inteligentes:
más eficiencia y control en el vídeo de seguridad

La eficiencia en el uso del vídeo y la capacidad de extraer valor operativo de cada flujo son aspectos clave para los profesionales de la seguridad. En este contexto, el códec AV1 se consolida como un estándar abierto que permite reducir significativamente el consumo de ancho de banda y almacenamiento, manteniendo una alta calidad de imagen, especialmente relevante en despliegues a gran escala o multi sede.

Axis ha incorporado estas capacidades en su chip propio **ARTPEC 9**. Este procesador integra funciones avanzadas de codificación, ciberseguridad y analítica en el edge, permitiendo un procesamiento eficiente directamente en el dispositivo.

Una de las novedades más destacadas es la incorporación de overlays conmutables en flujos AV1. Estos overlays permiten mostrar información adicional —como datos de analítica, metadatos o alertas— sin modificar el vídeo grabado, pudiendo activarse o desactivarse según las necesidades operativas.

Además, estos eventos y metadatos pueden publicarse mediante **MQTT**, un protocolo ligero ampliamente utilizado en entornos IoT. Esto facilita la integración del vídeo con plataformas externas y sistemas de automatización, convirtiendo la cámara en una fuente de datos en tiempo real.

En conjunto, **AV1, ARTPEC 9 y los nuevos overlays** refuerzan un enfoque más abierto, eficiente e integrable del vídeo en los sistemas de seguridad modernos.

Impacto de la Ley de Protección de Entidades Críticas en Seguridad Privada

La reciente publicación del Proyecto de Ley de Protección y Resiliencia de Entidades Críticas marca un hito en España. Esta norma, que adapta la directiva europea CER, otorga por fin a la seguridad privada el estatus de sector estratégico, clave para proteger servicios vitales como la energía, el transporte o la sanidad.

Bajo la supervisión del **CNPREC**, no solo las infraestructuras serán vigiladas; las propias empresas de seguridad (CRA, vigilancia o mantenimiento) podrán ser catalogadas como entidades críticas. Esto implica nuevas responsabilidades: diseñar planes de resiliencia integrales, designar responsables de seguridad y gestionar incidentes con estándares europeos.

El proyecto introduce novedades tecnológicas y operativas que transformarán el día a día del sector:

- **Idoneidad del personal:** Control riguroso de antecedentes para quienes accedan a zonas sensibles.
- **Tecnología avanzada:** Uso de biometría y sistemas de detección de drones.
- **Cultura de resiliencia:** El enfoque pasa de la "protección estática" a la capacidad de recuperación inmediata.

Para **Casmar**, la resiliencia no es solo una obligación normativa: es una oportunidad para crear entornos más seguros y preparados. Ofrecemos soluciones tecnológicas y asesoramiento especializado para que nuestros clientes lideren este cambio. La seguridad ya no es solo proteger, es garantizar que todo siga funcionando, pase lo que pase.

TechXperience 2026:
el compromiso de Dahua con la formación y la innovación

Durante el primer semestre de 2026, Dahua Iberia está desarrollando una nueva edición de TechXperience, una gira tecnológica orientada a acercar la innovación al mercado español y reforzar la capacitación de clientes y profesionales del sector.

La iniciativa recorrerá distintas ciudades de España con jornadas presenciales centradas en la formación, la presentación de soluciones y el networking profesional.

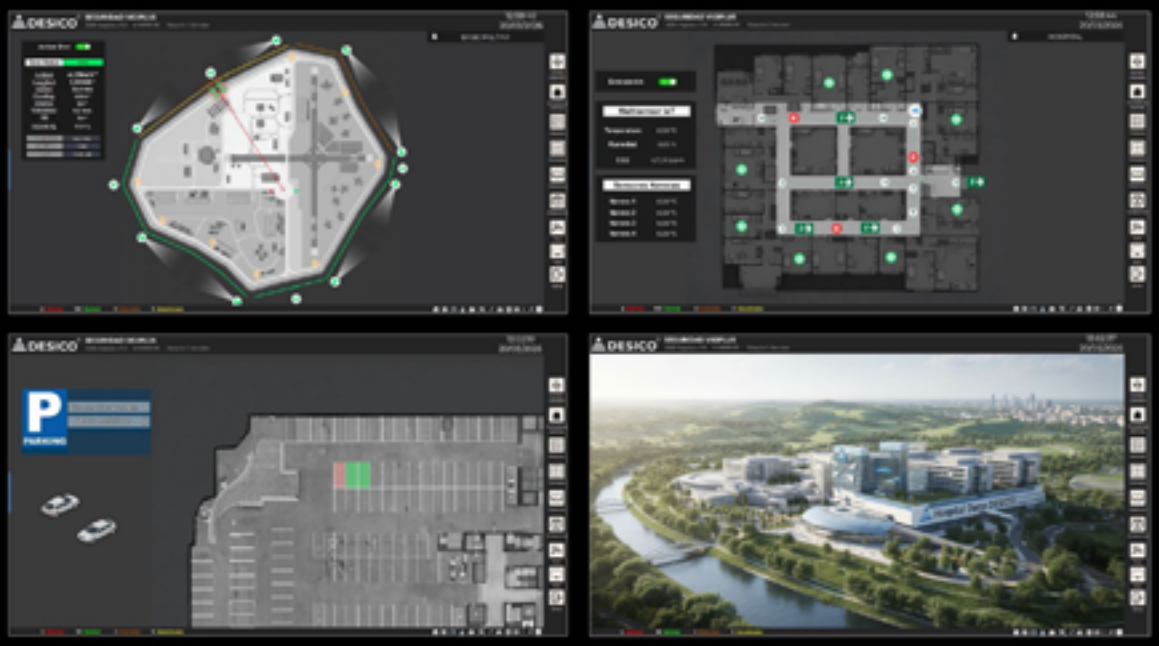
El objetivo de esta roadshow es ofrecer a los asistentes una experiencia útil y práctica, con sesiones formativas impartidas por especialistas de **Dahua** y contenidos enfocados en las nuevas tendencias tecnológicas del sector.

Durante las jornadas, los participantes pueden profundizar en diferentes soluciones y aplicaciones, así como conocer de primera mano las últimas novedades de la compañía en ámbitos como la videovigilancia inteligente, las soluciones inalámbricas, el tráfico y parking, el retail y la gestión tecnológica avanzada.

Además de su componente técnico, **TechXperience** también busca fortalecer la relación con clientes y partners, creando un espacio para compartir conocimiento, intercambiar experiencias y seguir impulsando la profesionalización del sector.

A través de este formato cercano y dinámico, **Dahua** reafirma su compromiso con la formación, la innovación y el acompañamiento a sus colaboradores en España.

+información



Proyectos personalizados con Desico

Saca todo el rendimiento a Vigiplus

DESICO®

El centro de control es el escaparate del departamento de Seguridad. Desico dispone de servicios profesionales que permiten personalizar y convertir tu centro de control en el elemento clave, en el punto neurálgico donde operar eficientemente y desde el que conectar con el resto del negocio.

Las tecnologías, los técnicos, los operadores y los procedimientos convergen en el centro de control. En él, la calidad de los planos, el desarrollo de las automatizaciones o la implantación de procedimientos son clave para sacar todo el rendimiento a los equipos y tecnologías de Seguridad.

Por eso, desde **Desico** estamos convencidos de la importancia de trabajar con nuestros clientes, de manera personalizada, en el desarrollo y mantenimiento de sus proyectos de centros de control.

Desico lleva más de 30 años ofreciendo a sus clientes unos servicios profesionales expertos en la integración de tecnologías y en el desarrollo de proyectos de Seguridad.

Desico dispone en España de más de 25 técnicos expertos en soporte al cliente, actualizaciones tecnológicas, integración de señales y procesos de mejora continua. Damos soporte antes, durante y después de la implantación, desarrollando proyectos personalizados, únicos y con la máxima calidad y eficiencia.

Si quieres implantar o mejorar tu centro de control, habla con nosotros. Somo los líderes en España en centros de control de Seguridad.

Optimiza tu centro de Control con **Desico**.
Conecta la Seguridad con el negocio:
comercial@desico.com |
(+34) 93 589 28 16

Lo primero es la salud... y la seguridad

La seguridad en los centros hospitalarios no es algo secundario. En estos espacios es esencial garantizar la continuidad asistencial, proteger tanto a pacientes como a profesionales y gestionar correctamente las áreas sensibles.

Estas infraestructuras esenciales presentan necesidades específicas: control de la rotación constante de personal y turnos, trazabilidad de movimientos, protección de áreas críticas como quirófanos o laboratorios y gestión segura de grandes flujos de personas, incluidos visitantes.

De forma paralela, es preciso monitorizar el resto de los sistemas de seguridad de forma centralizada: CCAA, VMS, intrusión, incendios, megafonía... Todo este ecosistema ha de cumplir una premisa clara: la seguridad nunca debe entorpecer la labor del personal ya que miles de vidas dependen de ello.

En **DORLET** lo sabemos, por eso, no solo ofrecemos productos y soluciones diseñadas específicamente para los centros sanitarios, sino que además actuamos como un guardián invisible se integra con la operativa diaria del hospital sin interferir en la actividad asistencial.

En este ámbito, contamos con una amplia experiencia y con referencias muy significativas como el Hospital de Cruces (Osakidetza), Hospital Clinic BCN (Catsalut), Hospital Virgen del Rocío (SAS) o el Hospital de Álvaro Cunqueiro (SERGAS), entre otros muchos otros centros sanitarios tanto a nivel nacional como internacional.

ACTUALIZACIÓN DE LA NORMA

UNE-EN IEC 62676-4:2025

EVOLUCIÓN DEL DISEÑO DE SISTEMAS DE VIDEOVIGILANCIA

Alberto Alonso

Responsable del programa de ingeniería y arquitectura, ciberseguridad y compliance de AXIS
alberto.alonso@axis.com

LA NORMA IEC 62676-4:2025, PUBLICADA POR LA COMISIÓN ELECTROTÉCNICA INTERNACIONAL (IEC) EN OCTUBRE DE 2025 Y RATIFICADA POR LA ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR) EN ENERO DE 2026, INTRODUCE UNA REVISIÓN PROFUNDA DE LAS DIRECTRICES DE APLICACIÓN PARA SISTEMAS DE VIDEOVIGILANCIA. ESTA ACTUALIZACIÓN SUSTITUYE LA EDICIÓN ANTERIOR (2014/2015), AMPLIAMENTE BASADA EN EL MODELO DORI (DETECT,OBSERVE, RECOGNIZE, IDENTIFY),, INCORPORANDO NUEVOS CRITERIOS TÉCNICOS ALINEADOS CON LA EVOLUCIÓN DE LAS CÁMARAS IP, LA ANALÍTICA DE VÍDEO Y LOS REQUISITOS ACTUALES DE SEGURIDAD FÍSICA Y CIBERSEGURIDAD.

Este artículo desarrolla un análisis técnico, integrando la evolución normativa desde la serie **EN 50132**, los cambios y diferencias con la versión anterior de la norma, su posible impacto en el diseño, instalación y mantenimiento de los sistemas de video vigilancia y su encaje en el marco regulatorio de Seguridad Privada español a través de la **Orden Ministerial INT/316/2011** y la incorporación de requisitos de ciberseguridad.

Evolución normativa internacional

La serie **EN 50132** constituyó durante décadas la referencia normativa en Europa para sistemas CCTV. No obstante, su enfoque resultaba limitado frente a los sistemas modernos, especialmente en entornos IP y de alta resolución.

ACTUALIZACIÓN DE LA NORMA UNE-EN62676-4:2025

La serie **IEC 62676** surge como evolución natural, adoptada posteriormente como **EN 62676** en el ámbito europeo y como **UNE-EN 62676** en España.

La transición desde la serie **EN 50132** hacia la serie **IEC 62676** no constituye únicamente una actualización técnica, sino un cambio conceptual profundo ya analizado en literatura sectorial previa. En este sentido, resulta especialmente interesante el análisis realizado por **Julio Pérez Carreño** en el boletín no. 61 (abril 2017) de la Asociación Española de Empresas de Seguridad.

En dicho trabajo se señala explícitamente la sustitución de la norma **EN 50132-1:2010** por la **UNE-EN 62676-1-1:2015,** marcando el inicio de la transición hacia un nuevo paradigma de sistemas de videovigilancia. Este cambio se acompaña de una redefinición conceptual, pasando de los tradicionales sistemas CCTV a los denominados Video Surveillance Systems (VSS), caracterizados por su naturaleza distribuida, su integración en redes IP y su capacidad de procesamiento avanzado.

Contexto y alcance de la norma

La **IEC 62676-4: 2025** establece rigurosos estándares de calidad que definen criterios medibles para la efectividad de los sistemas de videovigilancia (VSS) en aplicaciones de seguridad.

Esta parte 4 de la serie **IEC 62676** se centra específicamente en:

- Requisitos operativos del sistema
- Calidad de imagen y rendimiento visual
- Condiciones de instalación
- Verificación y mantenimiento

La versión 2025 surge como respuesta a la transición ya casi completa a sistemas IP de alta resolución, la necesidad de integración de los sistemas con otros subsistemas de seguridad, la creciente utilización de la analítica de vídeo y la IA en la videovigilancia y las nuevas exigencias regulatorias en materia de privacidad y ciberseguridad.

Limitaciones del modelo anterior (DORI)

La edición anterior se apoyaba en el **modelo DORI**, que todos tenemos asimilado y que está basado en densidades de píxeles por metro.

Sin embargo, presentaba algunas limitaciones, como la simplificación excesiva de los escenarios reales, la falta de consideración de factores como los niveles de compresión, la iluminación, el ruido en la imagen o las tecnologías de visión térmica.

Como resultado, la aplicación de la norma era poco fiable en condiciones operativas complejas

ACTUALIZACIÓN DE LA NORMA UNE-EN IEC 62676-4:2025

Nuevo marco conceptual: ampliación de requisitos operativos

Avances tecnológicos:

La norma ha evolucionado para abordar numerosos cambios tecnológicos, incluyendo avances en la tecnología de cámaras como:

- Tecnología de sensores
- Procesamiento de imágenes
- Capacidades de rendimiento en baja luz
- Mejoras en el rango dinámico

También incorpora directrices para análisis de vídeo, incluyendo análisis de vídeo impulsado por IA, aplicaciones de aprendizaje automático, reconocimiento de comportamientos y clasificación de objetos.

Mejoras en seguridad:

La norma actualizada responde a los requisitos de seguridad en evolución abordando nuevos desafíos como amenazas ciberfísicas, ataques coordinados, amenazas internas y riesgos de ingeniería social.

Refleja cambios en los requisitos del centro de operaciones de seguridad, los protocolos de respuesta a incidentes, los procedimientos de manejo de pruebas y la documentación de cumplimiento. Además, la norma incorpora nuevas normativas de protección de datos, requisitos de privacidad, estándares de control de acceso y mandatos de auditoría e informe.

Implementación y escalabilidad:

La norma revisada proporciona una guía mejorada para escenarios de implementación complejos, abordando requisitos para instalaciones urbanas vs. rurales, ambientes interiores vs. exteriores y condiciones de iluminación variables.

Ofrece soluciones para escenarios de despliegue complejos, ofrece recomendaciones para la escalabilidad del sistema e incluye directrices para instalaciones preparadas para el futuro.

La norma también aborda consideraciones de mantenimiento y actualización, asegurando que los sistemas sigan siendo efectivos durante todo su ciclo de vida operativo.

Cambios técnicos en IEC 62676-4:2025

La actualización introduce un modelo más granular que sustituye **DORI** por múltiples (7) niveles operativos:

- **Overview** (visión general/panorama)
- **Outline** (contorno/ perfilado)
- **Discern** (discernir/distinguir)
- **Perceive** (percibir)
- **Characterize** (caracterizar/reconocer)
- **Validate** (Validar/identificar)
- **Scrutinize/Examine** (examinar/forense)

Estas categorías de operación se dividen en dos grupos: Las tres primeras, como **LPDO (Low Pixel Density Objects)** que se entiende orientada a escenas de perímetro y exteriores y las restantes se agrupan como **HPDO (High Pixel Density Objects)** más enfocada a la observación de espacios próximos e interiores y con el objetivo de generar evidencias de uso forense.

Desafortunadamente, dado que ahora se presentan 7 letras iniciales y solo 2 son vocales, resulta mucho más difícil crear un acrónimo como **DORI** que tan práctico ha resultado durante estos 10 años. **OODPCVS** sería el nuevo acrónimo, pero sospecho que no tendrá la misma difusión y éxito que su predecesor.

No obstante, el nuevo modelo presenta algunas ventajas sobre el anterior, como una mayor precisión a la hora de definir los objetivos de las operaciones de vigilancia una adaptación más ajustada a escenarios complejos (urbano, transporte, retail, etc.) y una mejor alineación con las tareas reales del operador de videovigilancia haciendo distinción de aquellas otras automatizadas por el uso de analíticas de vídeo.

Métricas de rendimiento visual aclaradas, consideración de factores físicos y ópticos

La revisión ofrece recomendaciones actualizadas sobre la colocación de la cámara, las condiciones de iluminación y los factores ambientales. En este sentido, la nueva norma incorpora variables que antes no se trataban explícitamente:

- Iluminación (visible e infrarroja)
- Relación señal/ruido
- Compresión de vídeo
- Óptica y ángulo de visión
- Fotogramas por segundo (fps)

Esto permite un diseño del sistema más ajustado a la realidad. Del mismo modo se reconoce ahora el papel creciente de la IA con reconocimiento y clasificación de objetos y personas y la capacidad de analizar movimientos y comportamientos.

Una gran diferencia es que se establecen consideraciones técnicas diferentes según se plantee la vigilancia mediante la interpretación humana o que sea ejecutada por procesamiento automatizado (analíticas de vídeo).

Tabla comparativa de factores técnicos en **IEC 62676:2015** *vs* **2025.**

Factor	Norma 2015	Norma 2025	Impacto
Iluminación	Implícito	Explícito	Diseño real
Compresión	No	Sí	Calidad
FPS	No	Sí	Movimiento
WDR	No	Sí	Contraste
Ruido	No	Sí	Nitidez
Óptica	Parcial	Completa	Precisión

Tabla comparativa de niveles operativos en **IEC 62676:2015** *vs* **2025**

Norma 2015	Norma 2025	Operación
Detect	Overview	Detectar presencia y movimiento
	Outline	Distinguir perfil de los objetos y personas y dirección de movimiento
Observe	Discern	Apreciar características generales de objetos, personas y animales
	Perceive	Características definidas de personas y objetos en la escena
Recognize	Characterize	Identificar características específicas. Clasificación de vehículos y personas
Identify	Validate	Verificación de identidades y lectura de matrículas
—	Scrutinize	Identificación técnica de uso forense

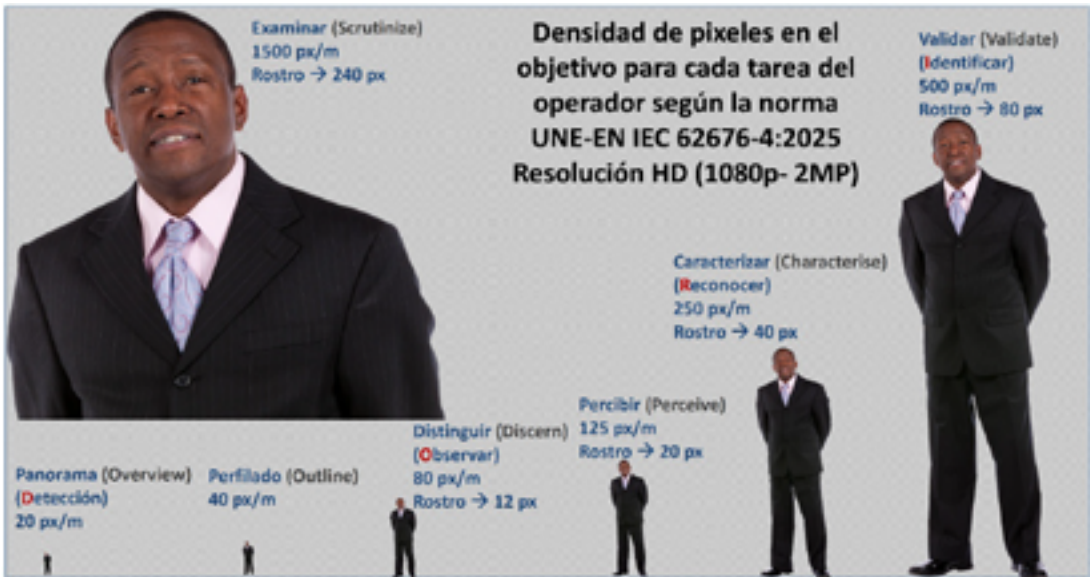
Revisión de la densidad de píxeles

Uno de los cambios más relevantes es la redefinición de los niveles de detalle, tratando de acompañar la evolución y mejora tecnológica de las cámaras que ofrecen ahora mayor resolución:

- Se incrementan los requisitos de píxeles por metro. Ejemplo: de ~250 px/m (identificación en DORI) a ~500 px/m (validar)
- Se introducen categorías **LPDO** y **HPDO** (baja/alta densidad de píxel en los objetos).
- Se mejora la representación matemática de la densidad de píxeles

Tabla comparativa de densidad de pixels en **IEC 62676:2015** *vs* **2025**

Nivel	**Norma 2015**	**Norma 2025**
Detección	25 px/m	20-80 px/m
Observación	63 px/m	80-250 px/m
Reconocimiento	125 px/m	250-500 px/m
Identificación	250 px/m	>500 px/m
Overview/panorama	—	20 px/m
Outline/contorno	—	40 px/m
Discern/discernir	—	80 px/m
Perceive/percibir	—	125 px/m
Characterize/caracterizar	—	250 px/m
Validate/validar	—	500 px/m
Scrutinize/examinar	—	1500 px/m



Importante: los requisitos operativos especificados son válidos en situaciones en que las imágenes de vídeo visuales son interpretadas por operadores humanos. En las aplicaciones de analítica de vídeo u otros sistemas en que el análisis de las imágenes se realiza mediante software, se aplican otras definiciones. En las imágenes térmicas (obtenidas con cámaras térmicas), los requisitos operativos también se definen de forma diferente.

Rendimiento visual no se refiere a "mejorar la calidad estética de la imagen", sino a optimizar la capacidad del sistema de videovigilancia para cumplir su objetivo operativo: detectar, observar, reconocer o identificar personas, objetos y eventos.

Rendimiento es la capacidad de una imagen de vídeo para permitir una tarea concreta de seguridad como, por ejemplo, detectar una persona, leer una matrícula o identificar un billete bancario.

Lo que la norma considera ahora es que no basta con que se vea "bien", sino que sea adecuado para la finalidad (operación) que se pretende, es decir, se refiere a la "usabilidad" de la imagen que la cámara proporciona.

La norma establece que esta usabilidad (rendimiento) no depende solo de la densidad de pixeles, sino de factores de configuración de la cámara como la compresión, el número de fotogramas por segundo, la velocidad del obturador, el procesado para mitigar la baja iluminación o los contraluces, y factores de instalación como la iluminación de la escena y la altura e inclinación de la cámara. En pocas palabras, que la imagen "sirva" para lo que se necesita.

Refuerzo de la ciberseguridad

Adicionalmente, y como no podía ser de otra manera en una actualización normativa de 2025 aplicable a dispositivos tecnológicos conectados a redes, se incorporan requisitos (básicos, pero al menos se incorporan) orientados a la protección del sistema de video vigilancia frente a ciberataques, contribuir a la seguridad de la red IP en la que opera, la gestión de los accesos a los dispositivos y la información que procesan y la integridad de los datos y evidencias que el sistema produce. Todo ello incluyendo consideraciones a lo largo de todo el ciclo de vida del sistema, lo que incide en el mantenimiento y gestión de este.

Por lo tanto, la norma amplía las directrices para garantizar y facilitar la escalabilidad del sistema y para adaptarse a entornos complejos (interior/exterior, urbano/rural). Igualmente hace mayor incidencia en el mantenimiento y actualización y en la interoperabilidad con los otros subsistemas de seguridad.

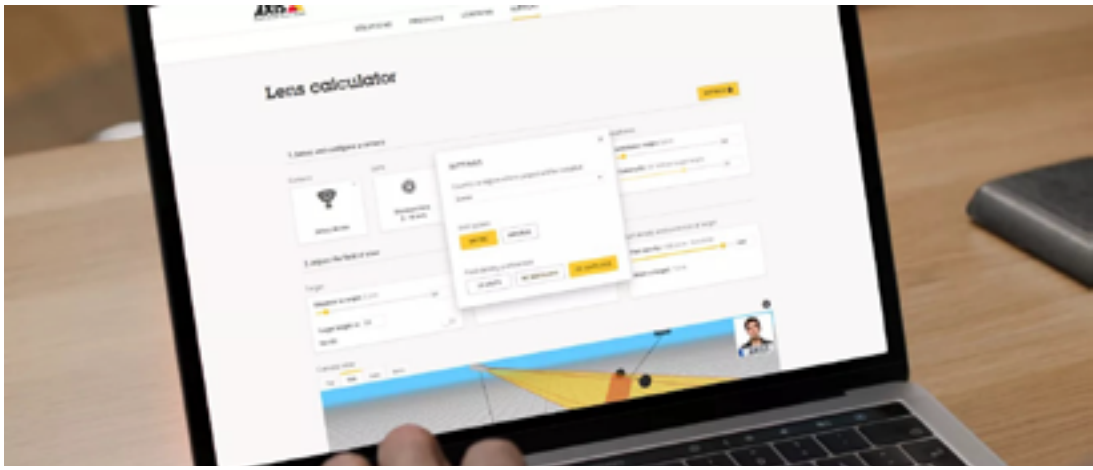
Tabla comparativa de Ciberseguridad en **IEC 62676:2015** *vs* **2025**

Elemento	**Norma 2015**	**Norma 2025**	**Impacto**
Autenticación	No	Sí	Acceso
Cifrado	No	Sí	Protección
Red	No	Segmentación	Seguridad
Firmware	No	Sí	Mantenimiento
Integridad	Implícita	Verificada	Legal/Forense

Impacto en el diseño de sistemas de videovigilancia

La nueva norma producirá algunos efectos en los diferentes actores de la industria. Para los ingenieros e integradores introduce la necesidad de rediseñar los criterios de cálculo (ya no basta DORI) incluyendo mayor resolución, incremento del almacenamiento y necesidades de red más exigentes, lo que puede conllevar el uso de herramientas avanzadas de planificación y mayor precisión en las especificaciones técnicas. Tendrán que detallar el propósito de cada cámara (OODPCVS) y la configuración y condiciones ambientales que deben producirse para que el equipamiento especificado ofrezca ese "rendimiento". Y obviamente cómo mantenerlo en el ciclo de vida del proyecto (revisiones, actualizaciones, recalibraciones, etc).

Para los fabricantes de equipamiento, que con seguridad deberán actualizar las fichas técnicas que ofrecen datos referidos a DORI, pero también tendrán que recalibrar las métricas de rendimiento y las herramientas de cálculo que ofrecen, así como tener en consideración (es de esperar que ya lo tuvieran) la integración de las analíticas y la ciberseguridad.



Para los usuarios finales lo esperable es que se vean beneficiados con mejores garantías de rendimiento (usabilidad de la imagen) en situaciones reales, que obtengan sistemas más fiables en escenarios críticos y que encuentren mayor facilidad para alinearse con los requisitos legales, especialmente de ciberseguridad y privacidad.

En definitiva, la norma evoluciona desde una guía orientativa hacia un marco técnico integral para el diseño avanzado de sistemas de videovigilancia.

Integración normativa en el ámbito de la Seguridad Privada: de EN 50132 a IEC 62676-4:2025 en el marco de la INT/316/2011

En España somos todos conscientes del anacronismo legislativo y regulatorio que supone estar sujetos a una Ley de Seguridad Privada del año 2014 que sin embargo no tuvo desarrollo reglamentario y que nos sitúa bajo el marco normativo de un reglamento del año 1994. No obstante, diversos Reales Decretos y Órdenes Ministeriales han venido a completar, actualizar y desarrollar aspectos normativos durante los pasados años. En concreto, para los sistemas de seguridad y alarma, la Orden Ministerial INT/316/2011 establece los requisitos para la instalación y mantenimiento de los sistemas de seguridad por parte de las empresas autorizadas.

Es lógico pensar que una OM publicada en 2011 adolecerá igualmente de obsolescencia y en especial en lo relativo a requisitos técnicos de sistemas y dispositivos, habida cuenta de la rápida evolución de estos. Sin embargo, el legislador, tuvo la precaución de redactar lo siguiente:

"Cualquier elemento o dispositivo que forme parte de un sistema de alarma de los recogidos por la normativa de seguridad privada, deberá cumplir, como mínimo, el grado y características establecidas en las Normas UNE-EN 50130, 50131, 50132, 50133, 50136 y en la Norma UNE CLC/TS 50398, o en aquellas otras llamadas a reemplazar a las citadas Normas, aplicables en cada caso y que estén en vigor"

Y se refuerza con su disposición adicional segunda:

> *"Disposición adicional segunda. Actualización normativa. La modificación o aprobación de cualquier nueva Norma UNE o UNE-EN sobre esta materia, de las contenidas en el anexo I de esta orden, será suficiente para su aplicación inmediata a las reformas de las instalaciones ya existentes y a las nuevas instalaciones, sin necesidad de ningún acto de incorporación normativa, desde el momento de su publicación por el organismo competente para ello."*

La clave de este texto está en *"en aquellas otras llamadas a reemplazar a las citadas Normas, aplicables en cada caso y que estén en vigor"*. Ese fragmento introduce una cláusula de actualización dinámica.

Esto significa que no se fija una norma concreta de forma estática, sino que se permite que el cumplimiento se adapte a normas más recientes. En ese sentido, la **INT/316/2011** fue concebida en un contexto analógico/IP temprano, por lo que no contempla amenazas modernas y no define requisitos de ciberseguridad detallados. Sin embargo, la **IEC 62676-4:2025** introduce la ciberseguridad como elemento estructural del sistema. Por la misma cláusula de sustitución la exigencia técnica evoluciona automáticamente.

Es decir, de acuerdo con la cláusula de actualización normativa recogida en la Orden **INT/316/2011**, las referencias a la serie **EN 50132** deben entenderse sustituidas por la serie **EN/IEC 62676** en vigor, aplicándose en este momento la **IEC 62676-4:2025** como estándar técnico actualizado para el diseño de sistemas de videovigilancia.

En términos de requisitos de ciberseguridad esto es importante, porque si bien otras regulaciones pueden ser aplicables a los sistemas de videovigilancia, tales como el **RGPD**, el **ENS** o la próxima trasposición de la directiva **NIS 2 (Ley de Coordinación y Gobernanza de la Ciberseguridad),** la estancada situación legislativa respecto a la Seguridad Privada nos podría hacer pensar que no existen requerimientos específicos de ciberseguridad que provengan de este ámbito regulatorio y de control.

Bien es cierto, que en virtud de lo matizado en la **INT/1504/2013**, la exigibilidad no será efectiva hasta pasados 30 meses de la aprobación de la norma, lo que sitúa la fecha de exigibilidad en junio de 2028:

> *Orden INT/1504/2013, de 30 de julio*
> *Artículo 4. Exigibilidad de Normas UNE o UNE-EN.*
>
> *3. En todo caso la exigibilidad de aplicación de la modificación o aprobación de cualquier Norma UNE o UNE-EN a las nuevas instalaciones o reformas no podrá ser inferior a los treinta meses posteriores a su fecha de publicación.*

Más aún, como ya apuntaba **Julio Pérez** en el citado artículo de 2017, queda la necesidad de concretar, cómo y quién debe certificar una instalación de videovigilancia, lo que sin duda convierte la obligatoriedad de cumplimiento en una utopía, y reduce la norma a una "guía de buenas prácticas". El alineamiento de la calificación de grado de seguridad entre **EN 50131-1** y **EN 62676-1** que en ese mismo artículo **Julio Pérez** reclamaba, me temo que queda también en "asuntos pendientes".

Líneas futuras esperables en la evolución de la norma

Se prevé que futuras revisiones profundicen en aspectos que cada día van tomando mayor importancia en la implantación y gestión de sistemas, tales como la integración con sistemas inteligentes de ciudades (Smart Cities), la evaluación automatizada del rendimiento visual y el alineamiento con las normas de ética en el uso de la IA y la privacidad.

Conclusión:

La incorporación de estos nuevos criterios y tablas de referencia convierte la **IEC 62676-4:202**5 en una herramienta mucho más precisa para el diseño de sistemas de videovigilancia modernos, alineados con las exigencias actuales de seguridad, analítica e interoperabilidad.

Como sucede con todas las actualizaciones normativas, llevará un tiempo acostumbrarse y ver de manera habitual el uso de las nuevas definiciones y requisitos tal y como lo hemos experimentado en los últimos 10 años con el "estándar" DORI. Sí debe hacernos reflexionar la inclusión de requisitos de ciberseguridad, puesto que representa un cambio de paradigma en el marco regulatorio, aunque su cumplimiento sea dudoso dada la falta de control de la obligatoriedad.

En definitiva, la **UNE-EN IEC 62676-4:2025** es la norma internacional y nacional de aplicación como guía para el diseño, implantación y mantenimiento de sistemas de videovigilancia, de modo que como profesionales debemos conocerla y adoptarla en el desempeño de nuestra actividad.

CONOCE A UN

SOCIO

Jaume Pomé Algueró

SOCIO Nº 167

Buenos días Jaume, aunque llevas años en el sector y muchos te conocemos profesionalmente, dinos algo sobre ti que nos ayude a conocer al Jaume persona.

Me llamo Jaume Pomé Algueró, ingeniero informático, toda mi trayectoria profesional ha estado vinculada al entorno de la seguridad, combinando tecnología, software e integración de sistemas aplicados tanto a entornos industriales como de seguridad física.

Quiero agradecer a AEINSE la oportunidad de poder presentarme a todo el colectivo y compartir, a través de esta entrevista, una visión personal y profesional forjada a lo largo de más de tres décadas de experiencia en el sector. Siempre he entendido la seguridad como un ámbito en constante evolución, en el que la tecnología, las personas y la colaboración entre profesionales juegan un papel clave.

¿Cuál es tu formación académica?

Licenciado en Informática por la Universitat Autònoma de Barcelona (UAB)

¿Has cursado alguna otra formación, aunque no sea académica, que te haya sido útil?

Más allá de la formación académica, mi aprendizaje ha estado siempre ligado a la evolución constante de las tecnologías informáticas desde los años noventa hasta la actualidad. A lo largo de este tiempo he realizado diversos cursos y formaciones técnicas, pero, sobre todo, he mantenido una actitud de aprendizaje continuo, imprescindible en un sector en permanente transformación.

He vivido de primera mano la evolución de las bases de datos, desde modelos más simples y cerrados hasta arquitecturas complejas, distribuidas y orientadas a grandes volúmenes de información, así como la transformación de las arquitecturas de software y los entornos de desarrollo. En paralelo, y muy especialmente en el ámbito que constituye la base de nuestra actividad, he acompañado la profunda evolución de los sistemas de seguridad física, desde los primeros sistemas de CCTV analógico, centrales de intrusión y control de accesos, hasta las actuales plataformas PSIM (Physical Security Information Management), basadas en integración software, que unifican CCTV, intrusión, control de accesos, PCI y otros sistemas de seguridad física.

En los últimos años, todo este proceso se ha visto reforzado por la creciente importancia de la ciberseguridad, que hoy es un elemento inseparable tanto de los sistemas informáticos como de las infraestructuras de seguridad física conectadas. En mi experiencia, esta capacidad de adaptación y actualización constante, basada en la práctica profesional y en proyectos reales, ha sido tan determinante como cualquier formación reglada a lo largo de mi carrera.

¿En qué empresas has desarrollado tu actividad profesional, qué tipo de trabajo has realizado y en qué puestos?

Inicié mi trayectoria profesional en Control y Aplicaciones, S.A. (CAE), grupo español de ingeniería e instrumentación industrial que fue una de las compañías de referencia en España a finales de los años ochenta en sistemas de control, automatización y mantenimiento de grandes instalaciones industriales.

En esta etapa desarrollé mi labor como Ingeniero de Sistemas, participando en proyectos tecnológicos de gran envergadura en entornos industriales y de seguridad.

Posteriormente, fui cofundador de DESICO, junto con Andrés Calvo, José Luis Jiménez y José Luis Martín, empresa en la que he desarrollado gran parte de mi carrera profesional. En DESICO he desempeñado el cargo de Director del Departamento de Software, participando en el diseño, desarrollo y evolución de soluciones de software y sistemas tecnológicos aplicados a entornos industriales y de seguridad.

De todos estos trabajos ¿Cuál dirías que te ha gratificado más?

Sin duda, la experiencia que más me ha gratificado ha sido la fundación y el crecimiento de DESICO. No solo por el reto técnico y empresarial que supuso crear el proyecto desde cero, sino, sobre todo, por haber podido construir a lo largo de los años un equipo humano sólido, comprometido y altamente cualificado.

Ver cómo una iniciativa impulsada inicialmente por unos pocos se ha transformado, con el tiempo, en una empresa consolidada, con casi 60 profesionales en la actualidad, y comprobar que muchas de esas personas han crecido junto al proyecto, es sin duda el aspecto más satisfactorio de toda mi trayectoria profesional.

Eres uno de los fundadores de DESICO y ahí seguís los cuatro socios 34 años. ¿Qué os llevó a fundar la Compañía?

La decisión de fundar DESICO surge en un momento de cambio natural de etapa, con movimientos de fusiones de empresas y la externalización de especialidades, entre ellas la tecnológica.

Intuimos que ese proceso implicaría cambios profundos y, como socios y profesionales con una marcada vocación técnica y emprendedora, entendimos que era el momento adecuado para iniciar un proyecto propio, en el que pudiésemos mantener una relación más directa con la tecnología, los proyectos y los clientes.

Con esa visión compartida, decidimos fundar DESICO, una decisión que con el tiempo hemos comprobado que fue acertada, tanto a nivel profesional como humano.

¿Cuál fue el primer producto que desarrollasteis y cómo era el estado de los sistemas de integración en los años 90?

En los primeros años tras la fundación de la empresa, desarrollamos una primera versión de software de integración que, en sus inicios, se conoció como VIGIA. En un contexto en el que los sistemas de seguridad eran fundamentalmente cerrados y aislados, VIGIA ya permitía integrar equipos de CCTV —entonces analógico—, centrales de intrusión y sistemas de control de accesos.

Con el paso de los años, este software fue evolucionando de forma continua, adaptándose a los cambios tecnológicos y a las nuevas necesidades del sector, hasta convertirse en lo que hoy es Vigiplus PSIM, una plataforma de integración avanzada que refleja esa evolución desde los primeros sistemas hasta los entornos actuales.

¿Cuáles fueron los principales obstáculos técnicos que encontrasteis?

Uno de los principales obstáculos técnicos fue, sin duda, la necesidad de crear software propio desde cero. En los inicios de DESICO no existían plataformas maduras que resolvieran de forma integrada las necesidades que teníamos, por lo que tuvimos que diseñar y desarrollar nuestras propias soluciones, tanto a nivel de arquitectura como de funcionalidad.

Este reto coincidió además con una etapa de rápida evolución tecnológica, que nos obligó a adaptarnos continuamente: la transición desde sistemas propietarios y cerrados hacia entornos abiertos e IP, la evolución de las bases de datos, las nuevas arquitecturas de software y, en paralelo, la profunda transformación de los sistemas de seguridad física.

Pasamos de soluciones aisladas –CCTV analógico, intrusión o control de accesos– a plataformas PSIM, capaces de integrar de forma unificada CCTV, PCI, control de accesos, analítica avanzada, así como una gran variedad de equipamiento utilizado en el entorno de la seguridad.

En los últimos años, a todo ello se ha sumado el auge de la inteligencia artificial, junto con la ciberseguridad, hoy un requisito crítico y transversal. Afrontar estos desafíos exige un esfuerzo constante de aprendizaje, diseño e innovación, y pone de manifiesto la capacidad de adaptación tecnológica que ha acompañado la evolución de DESICO a lo largo del tiempo.

En la actualidad, tenéis uno de los PSIM más reconocidos del mercado, ¿qué prestaciones son las más demandadas por los clientes y cuales las indispensables?

Más allá de las funcionalidades concretas, los clientes valoran especialmente que Vigiplus PSIM integre de forma transparente los distintos sistemas de seguridad. El objetivo es que el usuario final trabaje desde una única plataforma, sin preocuparse por fabricantes o tecnologías, gestionando de forma unificada CCTV, accesos, intrusión, PCI o drones. Para nosotros, esa simplicidad operativa es hoy una prestación indispensable en cualquier PSIM.

En tu opinión ¿Tienen las compañías instaladoras en general personal suficiente cualificado para instalar, mantener y sacar el máximo rendimiento a los desarrollados PSIM actuales?

Las compañías instaladoras disponen de profesionales muy cualificados en la instalación de sistemas de seguridad, pero los PSIM actuales exigen perfiles más híbridos, con conocimientos de software, integración, IT y ciberseguridad. El reto hoy no es tanto instalar la plataforma como explotarla al máximo, y ahí la formación continua y la colaboración entre fabricantes e integradores juegan un papel clave.

¿Qué opinas de la actual normativa y legislación que aplica al sector de la seguridad?

La normativa ha contribuido a ordenar y profesionalizar el sector de la seguridad, especialmente en aspectos como la protección de datos y la seguridad de la información. Sin embargo, la rápida evolución tecnológica hace necesario un marco regulatorio más flexible, capaz de acompañar la convergencia entre seguridad física, software y ciberseguridad sin frenar la innovación.

Además de la intensiva dedicación profesional, seguro que dejas huecos para tus aficiones personales. ¿Qué te gusta hacer? ¿Qué proyectos tienes en mente para el futuro próximo?

A lo largo de los años he dedicado muchas horas a la vida profesional, pero siempre he procurado reservar espacio para aquello que aporta equilibrio. Ante todo, valoro especialmente el tiempo compartido con la familia y los amigos, que considero fundamental. Junto a ello, la música, especialmente la lectura, la música clásica, así como el teatro y la ópera, forman parte de mis principales aficiones. También disfruto de los paseos, tanto por la playa como por la montaña.

En cuanto a los proyectos para el futuro próximo, me encuentro en un momento especial, ya que en unas semanas inicio una nueva etapa tras mi jubilación. La idea es poder dedicar más tiempo a estos ámbitos personales, disfrutándolos con mayor calma. Al mismo tiempo, seguiré vinculado a DESICO, acompañando su evolución desde una perspectiva más relajada.

Afronto esta nueva etapa con la satisfacción de saber que el proyecto continúa con un equipo humano excepcional, que con los años se ha convertido casi en una familia, y que seguirá siendo el verdadero motor de DESICO. Ver cómo las personas que forman la compañía continúan haciendo crecer el proyecto es, sin duda, una de las mayores recompensas de todos estos años.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

ABR
2026

13º Congreso PRYC: Protección, Resiliencia y Seguridad

El 13º Congreso PRYC: Protección, Resiliencia y Seguridad se celebró en Madrid, los pasados 21y 22 de abril. Estando el primer día dedicado a la ciberseguridad y el segundo a la seguridad física. Dos fueron las cuestiones que levantaron más interés y debate: La seguridad de la cadena de suministro, el proyecto de Ley de Protección y Resiliencia de Entidades Críticas y el uso de la biometría en el control de accesos y sus derivadas legales.

Organizado por la **Fundación Borredá, Seguritecni**a y **Red Seguridad**, contó con la presencia en las mesas de debate y ponencias de directores de Seguridad Privada, CISOS, profesionales de la seguridad – entre ellos, nuestro socio **Raúl Porra**s- , organismos públicos y privados y fuerzas de seguridad del estado como el CNPIC y el SEPROSE de la Guardia Civil.

La apertura del Congreso corrió a cargo de **José Luís Pérez Pajuelo, director del CNPIC** y finalizó con un resumen de conclusiones por parte de **César Álvarez, coordinador de proyectos de la Fundación Borredá.**

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Global terrorism index 2016

index 2016

El Institut for Economics & Pece, publicó recientemente su informe anual sobre la medida del impacto del terrorismo "Global Terrorism Index 2026".

El informe contiene 4 capítulos: Resultados, Tendencias del terrorismo, Terrorismo y regiones fronterizas y Radicalización de los jóvenes

"El Índice de este año registró una caída sustancial del terrorismo en todo el mundo. Las muertes por terrorismo disminuyeron un 28%, hasta 5.582, mientras que el número de ataques se redujo casi un 22%, hasta 2.944. La mejora fue generalizada, con 81 países registrando avances. Solo 19 países se deterioraron, el menor número de deterioros en la historia del Índice. Sin embargo, hubo un aumento significativo del terrorismo en los países occidentales, que representaron siete de los 19 deterioros."

"El terrorismo sigue estando muy concentrado. Poco menos del 70 por ciento de las muertes por terrorismo ocurrieron en solo cinco países: Pakistán, Burkina Faso, Nigeria, Níger y la República Democrática del Congo (RDC). Seis de los diez países más afectados por el terrorismo se encuentran en el África subsahariana, ahora el epicentro mundial del terrorismo".

Leer informe completo

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Proyecto de Ley de Protección y Resiliencia de las Entidades Críticas


BOLETÍN OFICIAL
DE LAS CORTES GENERALES

CONGRESO DE LOS DIPUTADOS

XV LEGISLATURA

PROYECTO DE LEY

MAR
2026

El Consejo de Ministros ha aprobado en su reunión de pasado 17 de marzo, a propuesta del Ministerio del Interior, el proyecto de Ley de Protección y Resiliencia de Entidades Críticas.

Con ello se va dando cumplimiento, aunque con notable retraso, a la inclusión en la legislación española de la **Directiva CER** sobre la **resiliencia de las Entidades Críticas; instituciones y empresas, públicas o privadas, que prestan servicios esenciales en sectores estratégicos** y resultan indispensables para mantener las funciones sociales o las actividades económicas vitales no solo en el ámbito nacional, sino también en la Unión Europea.

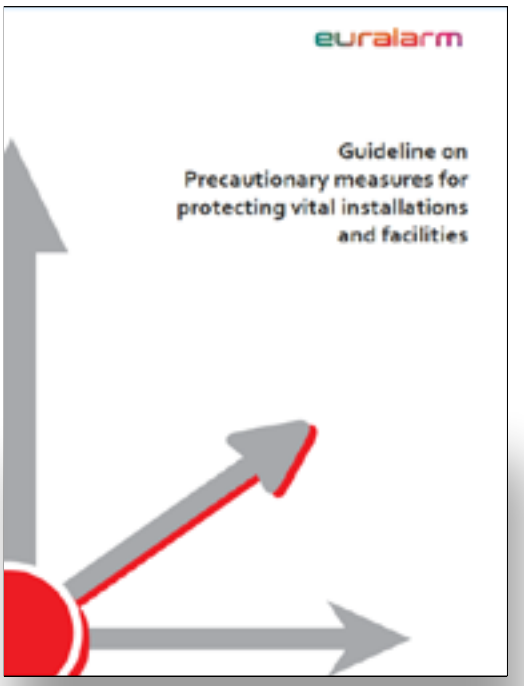
El proyecto de ley, que ha sido enviado a las Cortes Generales para su tramitación y aprobación parlamentaria, tiene como objetivo apoyar y garantizar el funcionamiento de las entidades públicas o privadas que explotan infraestructuras críticas en sectores estratégicos y deben tener capacidad de continuar prestando sus servicios ante impactos disruptivos.

Para ello adoptarán medidas de protección y recuperación tanto en el segmento ciber como en el físico.

Proyecto de Ley

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS



Directrices sobre medidas de precaución para proteger entidades e instalaciones vitales

EURALARM publicó a finales de pasado año esta guía en la que se destaca la importancia de la seguridad física y los requisitos básicos para la protección de las entidades críticas.

La Guía parte de la necesidad de realizar análisis de riesgos, la consideración de la normativa , el conocimiento de la operativa y el análisis de interdependencias, entre otros aspectos, para concluir con la afirmación de que la protección de infraestructuras vitales no es responsabilidad exclusiva de los operadores críticos, sino una tarea compartida con los sectores públicos y privados, así como una adaptación permanente a las amenazas permanentes.

En su introducción podemos leer:

"En un mundo cada vez más complejo e interconectado, en el que la interdependencia entre diferentes sectores es ubicua, la seguridad de las infraestructuras críticas es un elemento central de la estabilidad y el orden social". La protección de estas instalaciones y equipamientos vitales, desde el suministro de energía y agua hasta la atención sanitaria y los sistemas de comunicación y transporte, es de importancia central para el bienestar y la seguridad de la sociedad europea. Los desarrollos recientes y los escenarios de amenaza muestran cuán vulnerables son las infraestructuras europeas a ataques dirigidos, desastres naturales y fallos técnicos" .

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Securitas Direct pasa a ser Verisure

La compañía de alarmas Securitas Direct ha cambiado su marca en España para adoptar el nombre de Verisure con el que opera de manera global.

El cambio responde a sus experiencias previas en otros países que "han demostrado que operar bajo la misma marca fortalece la percepción de liderazgo, facilita la innovación compartida entre países y refuerza la confianza de clientes y grupos de interés", explican desde la compañía.

Este cambio no supone un cambio de estrategia ni del modelo de negocio, ni de la calidad del servicio de un compañía que lleva operando en España más de 30 años.

AEINSE
Asociación Española de Ingenieros de Seguridad

18º Seg2
Encuentro Seguridad Integral

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

JUN
2026

Soberanía Digital, Defensa y Ciberseguridad

El próximo 24 de junio, organizado por Seguritecnia y Red Seguridad con la colaboración de la Fundación Borredá, tendrá lugar en Madrid el evento, que estará dedicado al impacto del contexto geopolítico y la necesidad de reforzar la soberanía digital, la defensa y la ciberseguridad en España creando un escudo digital compartido y sostenido entre todos.

LEÍDO, VISTO Y OÍDO EN...

MANIAC

..."Bohr, Heisenberg, Dirac y Born, no podía Paul, sin embargo, evitar la sensación de que habían traspasado un límite fundamental, y que un demonio, o tal vez un genio, había anidado en el alma de la física, un genio al que ningún miembro de su generación podría devolver a su lámpara. Si uno aceptaba las nuevas reglas que gobernaban el reino interno de los átomos, el mundo entero dejaba de ser tan sólido y real como antes. ¡Seguramente hay una sección especial en el purgatorio para los profesores de mecánica cuántica!"

De la mano de John von Neumann, matemático húngaro de la primera mitad del siglo XX, Benjamin Labatut nos ofrece una novela en la que combina elementos biográficos de científicos y elementos de ficción para explorar el impacto de la inteligencia artificial, la teoría de juegos y el desarrollo de las primeras computadoras. Advirtiéndonos sobre los retos a los que nos tendremos que enfrentar a medida que nuestras creaciones tecnológicas adquieran cada vez mayor independencia. La obra concluye con la batalla entre un hombre y una máquina.

MANIAC.
Editorial Anagrama. ISBN 978-84-339-1100-1.
(Una obra muy adecuada a nuestro perfil de ingenieros).

Ecosistema de Seguridad

"Este número de **Red Seguridad** dedicado al ecosistema de Ciberseguridad incluye también a los principales organismos de la UE en esta materia, cuya coordinación con las entidades nacionales es fundamental para afrontar el presente y el futuro de la seguridad digital en el Viejo Continente"

La revista presenta un listado y breve resumen de su dependencia, jefatura y actividad de 48 organismos oficiales europeos, nacionales y autonómicos implicados en la ciberseguridad.

artículo completo

LEÍDO, VISTO Y OÍDO EN...

El Confidencial
EL DIARIO DE LOS LECTORES INFLUYENTES

EL FIN DE LA REALIDAD

Ingenieros crean la única tecnología realmente infalible para detener el caos del vídeo IA

Investigadores de la ETH Zúrich han creado un sensor que estampa un sello criptográfico de autenticidad en fotos y vídeos. Es la única manera de asegurarse de que un vídeo es real, pero los fabricantes tendrán que implementarlo

Imagen sintética de la falsa influencer Jessica Foster con Donald Trump. (Instagram)

"La verdad visual se está yendo al garete gracias a los nuevos modelos de IA generativa que produce contenido multimedia sintético con un aspecto indistinguible de la realidad..."

"Investigadores de la Escuela Politécnica Federal de Zúrich han creado un sensor que incorpora un sello de autenticidad en vídeo y fotos. Es la única manera de asegurarse de que un video es real, pero los fabricantes tendrán que implementarlo"

+información

PATROCINADORES

ADI
AXIS COMMUNICATIONS
casmar
alhua TECHNOLOGY
DESICO
DORLET
FFV VIDEOSISTEMAS GEUTEBRÜCK
HID
IQSIGHT
Hanwha Vision
Johnson Controls
LANACCESS 30 Años
LEGIC
Sicuralia
VIGI by tp-link
SCATI

AEINSE
Asociación Española de Ingenieros de Seguridad