BOLETÍN Nº63 OCT 2025

AEINSE
Asociación Española de Ingenieros de Seguridad

III Congreso Ingeniería de Seguridad AEINSE

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

III Congreso Ingeniería y Seguridad

¡No podemos estar más contentos!

El III Congreso de Ingeniería de Seguridad de nuestra asociación ha sido todo un éxito, reuniendo a más de 130 profesionales del sector en una jornada repleta de aprendizaje, intercambio de ideas y, sobre todo, mucha pasión por la ingeniería de seguridad.

Durante el congreso disfrutamos de ponencias de altísimo nivel, que pusieron sobre la mesa los grandes temas que están marcando el presente y el futuro de nuestra profesión; la Inteligencia Artificial, los desafíos de la Ingeniería de Seguridad, la Ciberseguridad y la Protección Perimetral, amenizando el Congreso con una micro charla: *"De la colmena a la mesa, el fascinante mundo de la miel"* para romper con nuestro día a día y que fue muy apreciada por los presentes.

Los ponentes compartieron su experiencia y conocimientos de una forma cercana y práctica, haciendo que cada charla aportara un valor real a todos los asistentes.

Uno de los aspectos más destacados fue el ambiente participativo y colaborativo que se vivió en todo momento. Se notaba que los asistentes tenían ganas de compartir, debatir y aprender juntos. Esa energía positiva y ese espíritu de comunidad son, sin duda, parte del éxito de este congreso.

Desde **AEINSE** queremos dar las gracias a todos los que formasteis parte de esta edición: a los asistentes por su interés y entusiasmo, a los ponentes por el esfuerzo y la calidad de sus intervenciones, y a los patrocinadores, cuyo apoyo hace posible que sigamos impulsando encuentros como este.

También queremos hacer una mención especial a **Seguritecnia**, que una vez más ha demostrado su profesionalidad y dedicación en la organización del evento. ¡Gracias por hacerlo todo tan fácil!

Este tercer congreso ha sido una gran oportunidad para seguir aprendiendo y creciendo juntos como comunidad profesional. Nos llevamos muchas ideas, nuevos contactos y, sobre todo, la motivación de seguir trabajando por una ingeniería de seguridad más innovadora, colaborativa y preparada para los desafíos del futuro.

Y, por supuesto, ya estamos pensando en la próxima edición. Si esta ha sido buena, prometemos que la siguiente será todavía mejor.

¡Nos vemos en el próximo Congreso de Ingeniería de Seguridad de **AEINSE**!

NOTICIAS AEINSE

III Congreso de Ingeniería de Seguridad AEINSE

07 OCT 2025

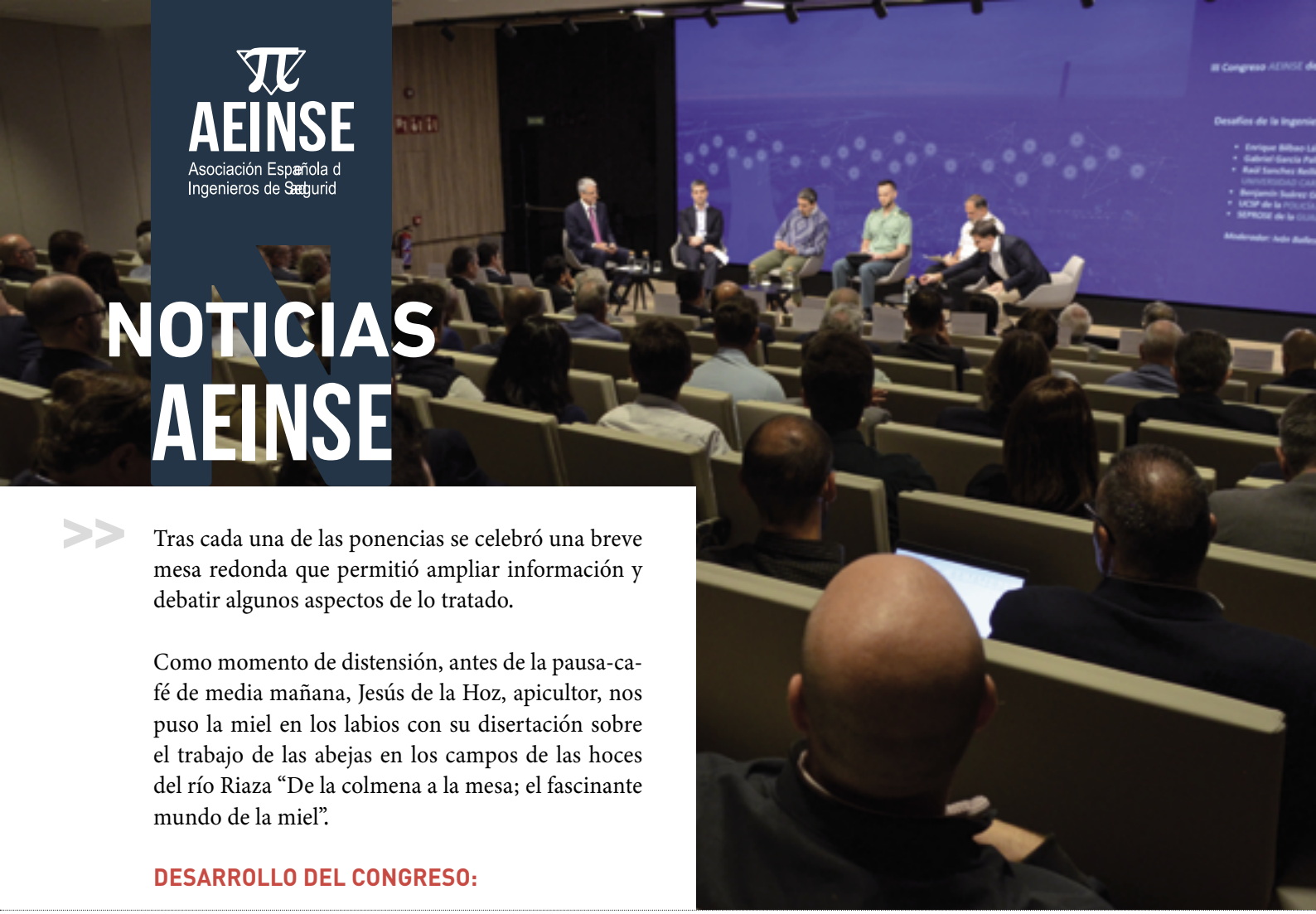
El pasado día 7 de octubre se celebró nuestro III Congreso de Ingeniería de Seguridad. El evento tuvo lugar en el auditorio Cecabank en Madrid y fue organizado con la colaboración de Seguritecnia.

Contó con **más de 130 asistentes** que siguieron con interés y expectación las ponencias y mesas redondas que tuvieron lugar.

Agradecemos el patrocinio de **Bosch, Casmar, Dahua, Desico, Dorlet, Grupo On Seguridad, Hanwha Vision, Lanaccess** y **Sicuralia Systems** que contribuyeron a hacer posible el evento.

Tras la bienvenida a los asistentes que realizaron nuestro presidente **Juan Manuel de Diego** y **Ana Borredá** de **Seguritecnia**, se cumplió el programa tal y como estaba previsto. Abordando las temáticas relativas a la utilización de la inteligencia artificial, los desafíos de la ingeniería de seguridad, la ciberseguridad en los sistemas de seguridad y las tecnologías de protección perimetral.

>>



Tras cada una de las ponencias se celebró una breve mesa redonda que permitió ampliar información y debatir algunos aspectos de lo tratado.

Como momento de distensión, antes de la pausa-café de media mañana, Jesús de la Hoz, apicultor, nos puso la miel en los labios con su disertación sobre el trabajo de las abejas en los campos de las hoces del río Riaza "De la colmena a la mesa; el fascinante mundo de la miel".

DESARROLLO DEL CONGRESO:

BLOQUE 1:
"Inteligencia artificial aplicada a la Seguridad"

Participantes:

Xavier Oliva,
Senior Key Account Manager en LANACCESS,
PONENCIA:
"Cómo diseñar un videograbador con IA"

Antonio Amegide,
PreSales Manager en DAHUA,
PONENCIA:
"Modelos de IA a gran escala-Visión"

Pablo A. Soto Pastén,
PreSales & Technical Manager en HANWHA VISION EUROPE,
PONENCIA:
"El impacto de la IA en el uso de cámaras de seguridad"

MESA REDONDA CON LOS PONENTES.

Moderador:
Juan José Hernández de la Encina
Miembro de la Junta Directiva de AEINSE.

BLOQUE 2:
PONENCIA Y MESA REDONDA
"Desafíos de Ingeniería de Seguridad"

Enrique Bilbao,
Director adjunto de DESICO,
PONENCIA:
"La necesidad de cerrar el ciclo de mejora continua de la ingeniería de seguridad"

MESA REDONDA:

Enrique Bilbao,
Director adjunto de DESICO,
Gabriel García Palermo,
Gerente de AB SEGURIDAD,
Benjamín Suárez González,
Dirección Corporativa de Seguridad en MAPFRE,
Representante de la UCSP de la Policía Nacional y
Representante del SEPROSE.

Moderador:
Iván Ballesteros
Miembro de la Junta Directiva de AEINSE.

BLOQUE 3:
PONENCIA
"La ciberseguridad en los sistemas de seguridad"

Participantes:

Ignacio Rojo,
Director de la unidad de negocio de DORLET SECURITY,
PONENCIA:
"DORLET en el Catálogo CPSTIC: fortaleciendo el ENS y anticipando los retos de NIS2 y CER"
Álvaro Retana,
Responsable de ingenierías y consultoras en BOSCH VIEDEO SYSTEMS,
PONENCIA:
"Cybersecurity in Video Surveillance Systems"
Manuel Carpio,
Creador y fundador de Armatum,
PONENCIA:
"Seguridad... ¿Cuánta es suficiente?"

MESA REDONDA CON LOS PONENTES.

Moderador:
Raúl Aguilera
Miembro de la Junta Directiva de AEINSE.

BLOQUE 4:
PONENCIA
"Protección perimetral"

Participantes:

Jordi Alonso,
Director de innovación y tecnología de CASMAR SECURITY,
PONENCIA:
"Soluciones de protección perimetral"
Antonio Pereira,
Director de Ingeniería de SICURALIA,
PONENCIA:
"Tecnología LIDAR en protección perimetral"
José Ramón Becerra,
Gerente de Grupo ON Seguridad y Presidente de AESCRA,
PONENCIA:
"De la detección perimetral a la eficiencia operativa: El papel de los diferentes actores en la eficiencia de la labor de la CRA"

MESA REDONDA CON LOS PONENTES.

Moderador:
Carlos Martínez
Miembro de la Junta Directiva de AEINSE.

NOTICIAS AEINSE

>> SINOPSIS DE LAS PONENCIAS Y MESA REDONDA

BLOQUE 1:

"Cómo diseñar un videograbador con IA"

La inteligencia artificial se ha convertido en un elemento clave en los sistemas de videovigilancia. El entrenamiento de modelos se realiza en servidores, pero la ejecución está alojada en los dispositivos —cámaras y videograbadores—, lo que mejora la eficiencia, reduce el ancho de banda y refuerza la seguridad. Además, permite búsquedas inteligentes y análisis estadísticos para inteligencia de negocio.
Los videograbadores deben dar servicio en entornos a menudo exigentes. Por ello, su diseño debe priorizar la eficiencia térmica, la durabilidad y la ciberseguridad, evitando el uso de componentes mecánicos como los ventiladores.

"Modelos de IA a gran escala - Visión"

La ponencia expone la evolución de la inteligencia artificial en videovigilancia, destacando los modelos Xinghan de gran escala. Estos modelos mejoran la detección de personas, vehículos y objetos en entornos complejos, reduciendo falsas alarmas y permitiendo búsquedas y alarmas personalizadas mediante texto e imagen.

Se presentan tres líneas principales:
Modelos de visión, multimodales y de lenguaje, que facilitan la configuración automática; la comprensión de escenas y la interacción avanzada.

Las aplicaciones abarcan seguridad, tráfico, industria y gestión urbana, optimizando la eficiencia y adaptabilidad en múltiples sectores.

"El impacto de la IA en el uso de cámaras de seguridad"

El objetivo es presentar las capacidades de las cámaras con inteligencia artificial, sus beneficios y su cumplimiento con la normativa europea (RGPD) y española (AI Act y LOPDGDD-España). Las cámaras con IA no solo graban, sino que "analizan lo que ven en tiempo real" usando algoritmos de inteligencia artificial para detectar objetos, personas, comportamientos y atributos.

Las cámaras tradicionales solo detectan movimiento y esto genera falsas alarmas, las cámaras con IA reconocen lo que hay en la escena proporcionando alertas precisas y más valor operativo. Sus funcionalidades claves son la detección de personas, vehículos, animales, paquetes y el análisis de atributos como género, edad estimada, color de ropa, uso de mascarilla, dirección de movimiento.

Entre sus beneficios cabe citar: Reducción de falsas alarmas, respuesta más rápida ante incidentes, ahorro de costes operativos, integración con sistemas de seguridad existentes, mejora de la eficiencia en retail, industria, transporte y smart cities.

En cuanto a legislación debe cumplirse en AI ACT de la UE y respecto a España la LOPDGDD, EIPD, AEPD y lo establecido por Autoridad competente para supervisar el AI Act.

Mesa redonda
Los ponentes dieron sus opiniones sobre tres cuestiones que propuso el moderador.

A la pregunta de:
¿Cuales son los principales retos para la explotación de la IA en los sistemas de videovigilancia?
La conclusión es que la legislación y regulación tiene una gran influencia y bastantes problemas derivados de la interpretación de cada país; por ejemplo protección de datos que, a pesar de la normativa unificada, en cada país hay matices que pueden ser diferentes. La falta de concreción en algunos puntos vitales. Un problema añadido es que la tecnología avanza más rápido que la regulación.

En cuanto a los modelos a gran escala, ¿cómo pueden influir en los sistemas?
El salto hacia el futuro es muy grande: tenemos analíticas complejas, Explotación de los datos, Búsquedas forenses más rápidas, alta precisión, y todo ello, en gran medida, con los mismos equipos

¿Cuál será el desarrollo futuro a corto plazo de la IA?
Se consolida la tendencia de incorporación de la IA en las cámaras, la utilización de tarjetas IA de terceros, ejemplo Nvidia.

¿Creéis que la IA es el mayor cambio tecnológico que ha habido en la seguridad?
Es uno de los mayores. Los grabadores digitales ya fueros un gran cabio, la tecnología IP, la analítica de vídeo también lo fue. La IA es un gran cambio a nivel sociedad, es un cambio de era. Hay que manejarla, encuadrarla, legislarla y ahí queda mucho por hacer

BLOQUE 2:

La necesidad de cerrar el ciclo de mejora continua de la ingeniería de seguridad.

"La ponencia reflexiona sobre cómo la ingeniería de seguridad debe evolucionar ante los nuevos riesgos, las exigencias normativas y los cambios tecnológicos. Destaca que la clave está en aplicar una cultura de mejora continua que conecte la estrategia con la práctica diaria. Señala la necesidad de unir y adaptar las actividades actuales de consultoría e ingeniería para lograr soluciones eficaces y adaptadas al entorno empresarial.

En particular, resalta la importancia de integrar los medios organizativos y humanos de la empresa en los sistemas técnicos tipo PSIM, destacando la necesidad de convertir los procedimientos en instrucciones, que el PSIM guíe a los operadores y la definición de los informes generados ante eventos ocurridos para que sirvan el negocio y la mejora continua.

En conclusión, propone entender la seguridad como un proceso dinámico, medible y esencial para la sostenibilidad de las organizaciones."

Mesa redonda
El punto de partida de esta mesa fue una definición compartida de ingeniería de seguridad: una disciplina que aplica principios técnicos, organizativos y humanos para identificar, analizar, controlar y reducir los riesgos de security que pueden afectar a las personas, los bienes o las infraestructuras.

No se limita al diseño de sistemas o medidas, sino que busca integrar la seguridad en todo el ciclo de vida de un proyecto.

NOTICIAS AEINSE

Durante la sesión se abordaron los principales retos de la ingeniería de seguridad. Para ello, se identificaron seis desafíos y se conformó una mesa con profesionales de perfiles muy diversos del sector, con el objetivo de conocer su opinión y perspectivas sobre cada uno de ellos.

Los participantes argumentaron cuáles consideraban los tres desafíos más relevantes desde su punto de vista. Todos los desafíos recibieron apoyos, aunque ninguno obtuvo consenso absoluto.

Si se priorizan los desafíos según la cantidad de argumentos aportados durante la mesa, el resultado fue el siguiente:

1. **Integrar las medidas humanas y organizativas.**
2. **Cerrar la brecha entre la ingeniería y la evolución tecnológica.**
3. **Contar con profesionales en ingeniería de seguridad con experiencia y conocimiento.**
4. **Implementar medidas de seguridad adecuadas al riesgo.**
5. **Disponer de requerimientos reconocidos por el cliente y las partes interesadas.**
6. **Alinear los sistemas con la función de seguridad requerida.**

Como datos curiosos destacan dos aspectos especialmente relevantes en los resultados:

Los tres primeros desafíos fueron identificados por la mayoría de los participantes como áreas prioritarias de mejora en la ingeniería de seguridad, lo que puede interpretarse como un objetivo compartido por el conjunto del sector.

Los tres últimos desafíos, con alguna excepción, fueron señalados principalmente por representantes de las CCFFSS, lo que sugiere que, aunque los ingenieros no los percibimos como los retos más urgentes (porque existe conocimiento técnico suficiente para abordarlos), desde la experiencia operativa de las CCFFSS aún queda trabajo por hacer en su aplicación práctica.

BLOQUE 3:

DORLET en el Catálogo CPSTIC: fortaleciendo el ENS y anticipando los retos de NIS2 y CER:

La presentación analiza el marco normativo español en ciberseguridad, destacando el Esquema Nacional de Seguridad (ENS) y su alineación con las directivas europeas NIS2 y CER. Explica su aplicación a entidades esenciales, importantes y críticas, y la necesidad de gestionar la seguridad física y lógica mediante controles de acceso, cifrado y certificaciones.

Subraya la importancia de adoptar sistemas certificados para garantizar cumplimiento real, mejorar la resiliencia, superar auditorías y reducir riesgos, sanciones y costes operativos.

Cybersecurity in Video Surveillance Systems:
La presentación aborda la ciberseguridad en sistemas de videovigilancia, destacando amenazas como malware, ataques DDoS, robo de datos o intrusión de privacidad.

Propone un enfoque integral en cuatro fases —captura, almacenamiento, visualización y gestión que garantiza confianza mediante elementos seguros, cifrado avanzado, control de acceso y auditorías.

La importancia del cumplimiento con estándares internacionales como IEC 62443, UL 2900 y GDPR, y la inclusión de 10 medidas integradas para proteger datos e infraestructura IoT mediante una mejora continua de la seguridad.

Seguridad...¿Cuánta es suficiente?:
La cuantificación económica del riesgo tecnológico es hoy una realidad gracias a metodologías como los grafos de ataque e impacto o el modelo FAIR, que emplean simulaciones Monte Carlo.

Estas herramientas permiten estimar tanto la probabilidad de que ocurran incidentes como la magnitud de las pérdidas asociadas, utilizando modelos probabilísticos que pueden ajustarse fácilmente a partir del criterio de expertos.

Además, una evaluación responsable de las inversiones en ciberseguridad debería considerar el nivel óptimo de inversión y los retornos esperados de dichas decisiones.

Mesa redonda
Raúl Aguilera, moderador de la sesión, propuso a **Ignacio Rojo** que aterrizara de forma más tangible los conceptos expuestos en su ponencia sobre las certificaciones CPSTIC, CSPN, Grado 4, entre otras.

Ignacio Rojo explicó que, por ejemplo, en el cumplimiento del Grado 4, la entidad certificadora verifica que los equipos conectados cuenten con supervisión continua, que toda alarma disponga de trazabilidad en su seguimiento, y que exista un control periódico del correcto funcionamiento de los sistemas. También destacó la importancia de la generación de señales de coacción, como puede ser el caso en un control de accesos, y de garantizar la seguridad de las comunicaciones.

En materia de ciberseguridad, subrayó que el cliente debe ser el creador y único conocedor de las credenciales de los sistemas.

Ante la pregunta ***¿Cómo afectan la inteligencia artificial y los nuevos métodos de computación a la ciberseguridad?*** **Álvaro Retana** señaló que la IA está haciendo evolucionar las amenazas, volviéndolas más eficientes y difíciles de detectar. Sin embargo, también destacó que la propia IA contribuye a entrenar mejor los sistemas de defensa, aumentando su capacidad de detección.

Respecto a la computación cuántica, advirtió que representa una amenaza directa a los métodos de cifrado actuales.

Finalmente, **Raúl Aguilera**, en relación con la cuantificación de la seguridad y el uso de métodos estadísticos basados en la ocurrencia y la trascendencia como herramienta de medición, planteó a Manuel Carpio la siguiente cuestión:

¿Cómo se ven afectados estos modelos cuando existe escasez de datos?
Manuel Carpio explicó que, dado que en el ámbito cibernético existe poco histórico de incidentes, es necesario recurrir a la experiencia de los expertos operativos para estimar la frecuencia de ocurrencia y el impacto potencial en el negocio.

Según los estudios actuales, la inversión en protección cibernética debería situarse entre el 25% y el 37% del mayor daño económico esperable, siendo desaconsejable descender por debajo de ese umbral.

Como conclusión, se destacaron varias recomendaciones:

- Apostar por el cumplimiento normativo certificado de los productos.
- Cuantificar las posibles pérdidas y trasladarlas a los comités económicos para fomentar el compromiso de inversión.
- Realizar una evaluación económica de riesgos, que permita valorar de forma objetiva la relación entre coste y beneficio de las medidas de protección.

BLOQUE 4:

Soluciones de protección perimetral:
El anillo exterior es la primera línea de defensa. Las diferentes soluciones y tecnologías disponibles, que pueden funcionar de forma independiente o de forma complementaria, permiten la detección de intrusos en su fase más temprana y permiten adecuar una pronta respuesta.

Se muestran algunas de las soluciones más innovadoras utilizadas para la protección de perímetros, explicando los puntos clave de cada una de ellas en base a sus prestaciones y limitaciones. Tratando soluciones como el análisis de vídeo utilizando IA, radares, cable en Vallado , detección geosísmica, detección por presión, detectores Laser, Drones y la integración de los sistemas

Tecnología LIDAR en protección perimetral:
Ponencia técnica que desglosa la tecnología LIDAR desde sus fundamentos hasta su aplicación avanzada en seguridad perimetral.

Analiza cómo los principios básicos de la detección por pulsos de luz han evolucionado desde los sistemas iniciales de escaneo 2D hasta las soluciones modernas de mapeo 3D. Cómo la tecnología actual está sustituyendo las partes mecánicas por chips.

Explora las métricas clave, las arquitecturas de hardware y el procesamiento de datos que permiten una detección de objetos precisa y fiable mediante la posibilidad de definir con gran precisión la zona a proteger. El objetivo es proporcionar una comprensión completa de la tecnología y su relevancia en la protección de infraestructuras, incluidas las consideradas críticas.

De la detección perimetral a la eficiencia operativa: El papel de los diferentes actores en la eficiencia de la labor de la CRA:
La detección perimetral constituye un elemento crítico en la arquitectura de seguridad física. Su eficacia se mide no solo por la capacidad de detección temprana, sino por la reducción de la tasa de falsas alarmas sin sacrificar sensibilidad. Está aumentando el uso de detección perimetral, fundamentalmente video análisis y cámaras con IA, pero también están aumentando las falsas alarmas.

Analiza por qué no se está logrando mayor eficacia operativa, enumerando los fallos habituales de los principales actores: La tecnología, el diseño e ingeniería del proyecto, el cliente, el instalador, el mantenedor y el contexto legal.

El reto principal es equilibrar precisión y fiabilidad en proyectos integrados con Centrales Receptoras de Alarmas (CRA). La evolución hacia tecnologías avanzadas obliga a definir políticas claras que optimicen la gestión.

La IA será de gran ayuda a los operadores de CRA en las labores de verificación.

AEINSE
Asociación Española d
Ingenieros de Seguridad

NOTICIAS AEINSE

Mesa Redonda:

Esta última mesa, estando ya fuera de tiempo, solo dio lugar a unas reflexiones sobre la pregunta ***¿Cuales serían para vosotros los tres principios básicos para diseñar una protección perimetral eficaz?*** Llegando a las siguientes conclusiones como bases determinantes:

- Necesidad de realizar un análisis del entorno para determinar la tecnología más adecuada.
- La coordinación entre todos los actores desde el proyecto a la operación de CRA, pasando por mantenimiento durante todo el ciclo de vida de la instalación.
- La tecnología actual necesita personal y técnicos con conocimientos informáticos

Conclusiones del Congreso:

- De la parte de la inteligencia artificial, está redefiniendo no solo la vida, sino también toda la ingeniería de seguridad y tenemos que plantearnos trabajar con criterio, conociendo la normativa que ya hemos tenido el lío que tenemos entre unos sitios y otros y tenemos que formarnos en toda la normativa que venga, tampoco sabemos dónde nos va a llevar todo esto de lA.
- Respecto a los desafíos de la ingeniería ls tecnología sigue avanzando y, o estamos al día en la formación o nos quedamos atrás.
- Lo mismo sucede con la normativa.
- Respecto a la ciber hay que centrarse enla certificaciones, utilizar productos certificados, con garantía y no usar cualquier cosa del mercado.
- Respecto a la seguridad perimetral, tenemos que estar al día y estar al tanto de todo el ciclo: instalación, puesta en marcha, mantenimiento.
- Respecto a la CRA, debemos intervenir como ingenieros en esta etapa de la seguridad de las instalaciones.

CLAUSURA

Cerró el Congreso **Juan Manuel de Diego** aportando las siguientes conclusiones:

- **La IA redefine la vida y la tecnología: Debemos trabajar con criterio, cumplimiento de normativa y formación sobre su aplicación.**
- **Ante el avance de la tecnología, la formación actualizada de los ingenieros es fundamental**
- **Estar en todo el ciclo de vida equipos y sistemas; desde el proyecto al mantenimiento.**

Y dando las gracias a Patrocinadores, Seguritecnia y asistentes.

Tras el aperitivo y *networking* entre todos los asistentes, nos fuimos a casa con nuestro tarrito de miel, elaborada en Maderuelo, como Caperucita a casa de su abuelita...

III Congreso AEINSE de Ingeniería de Seguridad - Seguritecnia (YouTube)
+información

Artículo de Iván Ballesteros en el número 515 de Seguritecnia con el título "Claves del tercer Congreso AEINSE de Ingeniería de Seguridad"
+información

Artículo en el número 515 de Seguritecnia sobre el Congreso con el título: "Formación, regulación y tecnología: claves del futuro de la ingeniería de seguridad"
+información

Cómo fabricar un grabador con IA

LANACCESS
Discover the power of video.

El siguiente artículo es un fragmento de la ponencia que dio Xavier Oliva, socio de AEINSE y Key Account Manager en Lanaccess, en el III Congreso AEINSE de Ingeniería de Seguridad.

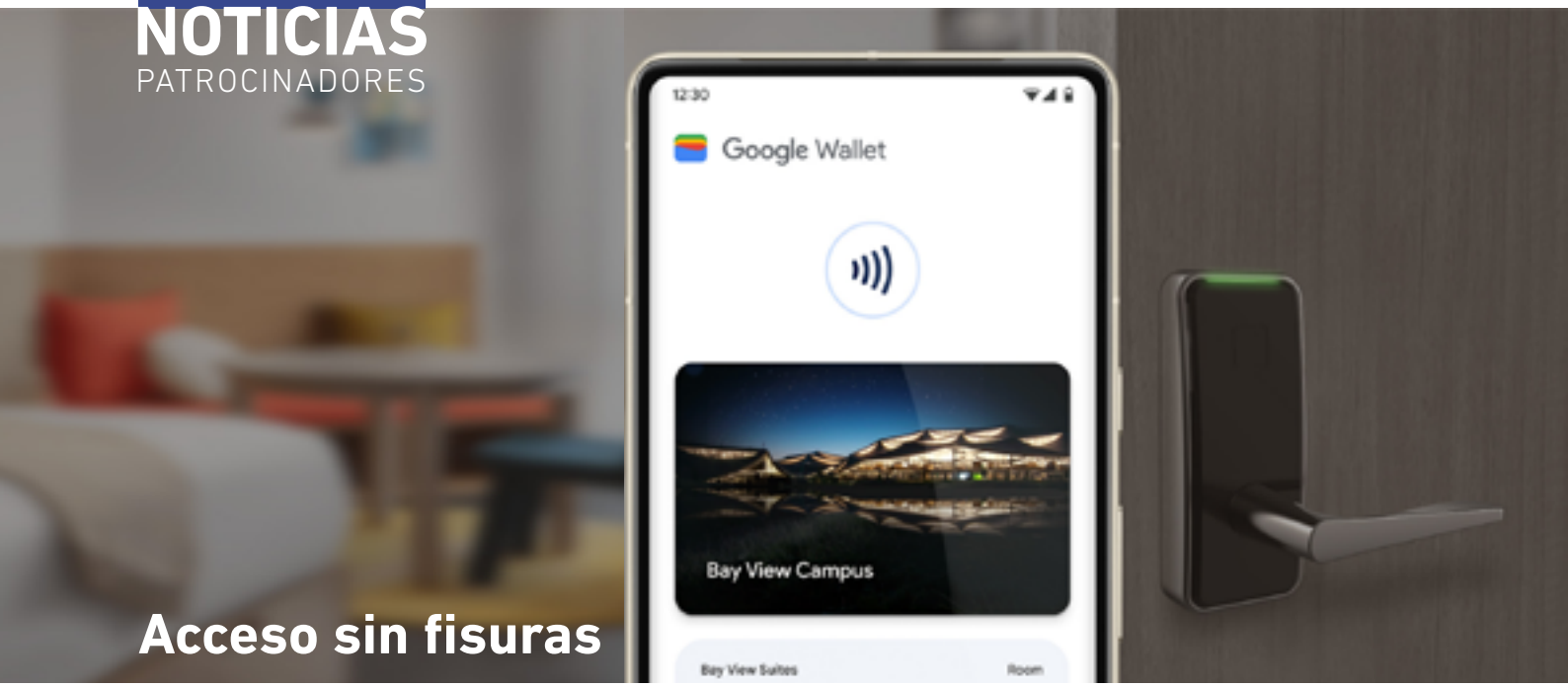
La inteligencia artificial se ha convertido en un elemento clave en los sistemas de videovigilancia modernos. Mientras el entrenamiento de modelos continúa pasando en centros de datos y en servidores, la ejecución de la IA se realiza directamente en los dispositivos —cámaras y videograbadores—, lo que mejora la eficiencia, reduce el ancho de banda necesario y refuerza la seguridad de las instalaciones.

La IA permite, además, búsquedas inteligentes y análisis estadísticos que aportan valor operativo más allá de la seguridad. Sin embargo, la identificación facial continúa sujeta a limitaciones legales derivadas de la normativa europea vigente.

En cualquier caso, el sector de la videoseguridad presenta retos específicos. Los grabadores deben dar servicio en entornos exigentes y ofrecer un alto nivel de fiabilidad que asegure su funcionamiento permanente. Por ello, el diseño de estos equipos debe priorizar la eficiencia térmica, la durabilidad y la ciberseguridad, evitando –en la medida que sea posible– la necesidad de usar componentes mecánicos como los ventiladores.

+información

LEGIC



Las credenciales LEGIC para móviles ahora en Google Wallet

Según informamos en el boletín anterior, ahora LEGIC Connect funciona también a través del Google Wallet, transformando la forma de gestionar las credenciales de acceso.

Con **LEGIC Connect** añadido a **Google Wallet**, los usuarios pueden llevar cómodamente sus credenciales móviles, como las tarjetas de identificación de empleados, directamente en sus dispositivos móviles. Ahora los empleados pueden acceder a sus lugares de trabajo sin esfuerzo con credenciales móviles basadas en el **Google Wallet**, sin necesidad de descargar una aplicación.

Oficinas, hoteles y apartamentos multifamiliares pueden ofrecer este servicio de credenciales móviles sin fisuras, proporcionando entrada sin contacto y una sencilla experiencia. Esto aumenta la eficiencia operativa, mejora la satisfacción de los empleados y huéspedes del hotel, y reduce los costes asociados a la gestión de tarjetas físicas.

Gracias a **LEGIC Connect** para **Google Wallet** podrá:

- Distribuir, gestionar o eliminar credenciales móviles de forma instantánea y remota en caso de pérdida del dispositivo o rotación de empleados
- Gestionar sin esfuerzo las credenciales de acceso en varios dispositivos móviles, garantizando una integración fluida
- Proporcionar a los usuarios las credenciales de **Wallet** a través de su aplicación,corporativa o de hotel, existente o directamente a través de una página web, garantizando una experiencia de usuario óptima.

Descubra cómo LEGIC Connect para Google Wallet transforma su gestión de accesos, haciéndola eficiente, cómoda y segura.

+información

El Nuevo radar inteligente de Seguridad Perimetral

Predator Radar AI

Sicuralia, presenta el sensor PREDATOR RADAR AI, una solución que redefine la protección de grandes áreas. Este sistema compacto "todo en uno" combina tecnología radar de última generación con una cámara PTZ de alta resolución.

PREDATOR RADAR AI ofrece una detección y seguimiento de 360º con un alcance de hasta 400 metros, midiendo con precisión la velocidad, el tamaño y la distancia de cualquier intruso. Sus nuevos algoritmos avanzados de Inteligencia Artificial que, junto con su software de auto-reconocimiento, eliminan las falsas alarmas provocadas por el clima adverso, garantizando una fiabilidad excepcional.

La cámara **Predator** integrada, incorpora imagen visible 4K, imagen térmica 640, iluminación luz IR e iluminación luz blanca, con distancias de hasta 550m

El equipo permite definir hasta 16 zonas de alarma programables. Además, ha sido diseñado para una integración digital con las mayores plataformas de gestión de vídeo y seguridad (VMS/PSIM) del mercado, incluyendo **Hexagon dC3, Milestone XProtect, Genetec Security Center** y **Vigiplus**.

Esta compatibilidad total permite una gestión centralizada y el uso de analíticas avanzadas, marcando un hito en la protección eficaz y automatizada a larga distancia para infraestructuras críticas e instalaciones industriales.

+información

SCATI — AUDIO INTELIGENTE PARA CUALQUIER ENTORNO

SCATI CONNECT

Integra comunicación de audio en tu plataforma de seguridad

SCATI CONNECT es la solución de comunicación por audio IP que amplía las capacidades de la plataforma de seguridad SCATI SENTRY.

Gracias a su diseño robusto y escalable, permite gestionar de forma centralizada altavoces IP, mensajes automatizados y sistemas de comunicación, convirtiéndose en un aliado clave para sectores como la banca, el retail, la industria o las infraestructuras críticas.

Con **SCATI CONNECT**, los operadores pueden reproducir mensajes predefinidos, programar avisos, automatizar comunicaciones basadas en eventos o establecer llamadas bidireccionales en tiempo real con cualquier punto de la instalación.

Todo ello desde una interfaz única e integrada en **SCATI SENTRY,** lo que garantiza control total, mayor eficiencia y máxima seguridad. Nuestros altavoces IP, diseñados para entornos exigentes, se integran directamente en la plataforma, ofreciendo funcionalidades avanzadas como reproducción simultánea, mensajes automatizados ante accesos no autorizados o llamadas inmediatas para gestionar incidencias.

SCATI CONNECT no solo mejora la seguridad disuasoria, sino también la experiencia de clientes y empleados mediante información en tiempo real, asistencia remota o comunicaciones operativas programadas.

Con esta solución, la seguridad se vuelve más inteligente, la gestión más eficiente y la comunicación más efectiva.

+información

AXIS COMMUNICATIONS

Cómo una potente herramienta de diseño de sistemas puede mejorar la eficiencia...

Diseñar soluciones de seguridad puede ser complejo y lento. Desde evaluar necesidades hasta configurar un sistema óptimo, cada paso requiere tiempo. Una herramienta avanzada de diseño de sistemas, como AXIS Site Designer, integra todo el proceso, ahorrando esfuerzo y garantizando soluciones eficientes.

Permite seleccionar productos, estimar almacenamiento, visualizar cobertura de cámaras y ajustar diseños en tiempo real junto al cliente. También ofrece recomendaciones personalizadas según requisitos operativos, sostenibilidad y estética. Además, genera propuestas precisas y documentación actualizada automáticamente.

Facilita la instalación con instrucciones detalladas y asegura que cada componente esté correctamente especificado. En resumen, esta herramienta transforma el diseño de sistemas en un proceso ágil, preciso y colaborativo, adaptado a las necesidades específicas del cliente.

Además, esta herramienta fomenta la colaboración entre equipos técnicos y comerciales, al permitir una comunicación clara sobre especificaciones y expectativas. Esto agiliza la toma de decisiones y fortalece la alineación entre diseño, ventas e implementación. Su uso reduce errores humanos, optimiza recursos y acelera la entrega de proyectos.

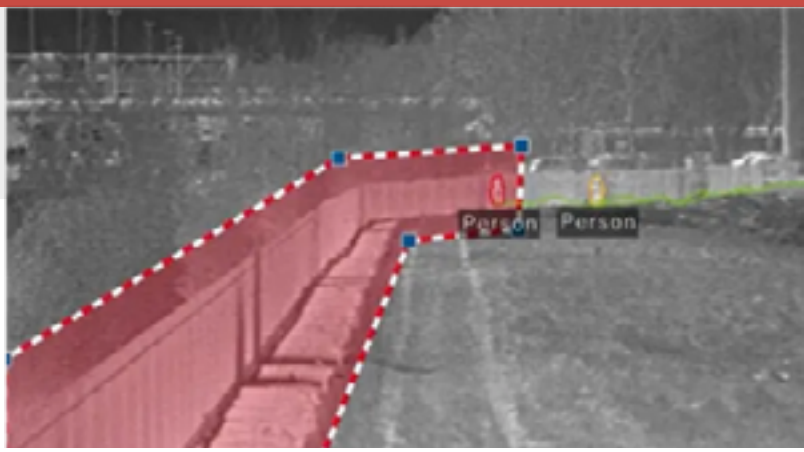
Cada diseño se adapta con precisión a los requisitos técnicos. El cliente recibe una solución robusta, eficiente y alineada con sus objetivos.

+información

DINION 8100i de BOSCH

Nuevas cámaras térmicas para ver "lo invisible"

BOSCH



La nueva cámara bullet térmica cuenta con tecnología de imagen térmica avanzada con IVA Pro Perimeter incorporado, que detecta personas de pie con precisión hasta a 586 m. de distancia y personas que reptan hasta a 327 m. de distancia, incluso en las condiciones más exigentes, lo que reduce la necesidad de usar varias cámaras y reduce los costes de instalación al tiempo que garantiza la seguridad total del perímetro.

IVA Pro Perimeter añade una capa de redes neuronales para minimizar las falsas alarmas y el tiempo de configuración, de modo que se reciban alertas cuando sea necesario.

Además, gracias a su función de **Autocalibración,** permite que la configuración inicial del dispositivo sea muy cómoda para el usuario, ya que la propia cámara establece los parámetros de forma automática basándose en datos consistentes y precisos obtenidos del entorno. Con su **diseño robusto, categorías IP66/IP67, resistencia a golpes NEMA TS-2 y resistencia a la corrosión según ISO 14993**, puede garantizar una vigilancia continua y fiable.

Además, se garantiza una sólida **ciberseguridad** con certificaciones como **IEC 62443-4-1** y **UL 2900-2-3 Nivel 3**. Nuestro **elemento seguro**, líder en el sector, está certificado según **Common Criteria EAL6+.**

+información

Casmar incorpora Gent de Honeywell

a su catálogo de protección contra incendios

Casmar refuerza su apuesta por la innovación en seguridad con la incorporación de Gent de Honeywell, una de las plataformas de detección y evacuación más avanzadas del mercado.

Esta nueva alianza permite a instaladores e ingenierías acceder a una solución reconocida internacionalmente por su fiabilidad, escalabilidad y eficiencia operativa.

Gent no es solo un sistema de detección, sino una plataforma integral que combina paneles de control, como Vigilon, con dispositivos multifunción S-Quad, capaces de integrar detección multitecnología (humo, calor y CO), señal acústica, avisador óptico y mensajes de voz en un único equipo. Esta arquitectura reduce el número de dispositivos y cableado, optimizando costes de instalación y mantenimiento sin comprometer la seguridad.

La solución está diseñada para adaptarse tanto a proyectos sencillos como a grandes instalaciones, como hospitales, hoteles, centros logísticos o edificios industriales.

Su compatibilidad con la plataforma en la nube CLSS (Connected Life Safety Services de Honeywell) facilita la supervisión remota, la generación automática de informes y el mantenimiento predictivo, funciones que aumentan la eficiencia y prolongan la vida útil de la instalación.

Con esta incorporación, **Casmar** ofrece al mercado una tecnología de última generación que aporta seguridad reforzada, gestión simplificada y preparación para el futuro.

+información

Modelos de IA a Gran Escala Xinghan
Dahua Technology

Dahua Technology, proveedor líder mundial de soluciones y servicios de AIoT centrados en video, ha lanzado oficialmente sus Modelos de IA a Gran Escala Xinghan, un sistema de nueva generación que combina inteligencia visual, multimodal y lingüística para abordar los desafíos de los entornos reales.

Inspirado en la palabra china "galaxia", **Xinghan** ofrece una arquitectura integral basada en la sinergia entre borde y nube, permitiendo una inteligencia escalable y adaptable en múltiples sectores. Entre sus principales líneas destacan los modelos de visión (V), con mejoras del 90% en precisión y detección avanzada de objetivos; y los modelos multimodales (M), capaces de procesar texto, imagen, audio y video para una comprensión semántica profunda.

Gracias a estas innovaciones, **Dahua** impulsa una nueva era de protección perimetral inteligente, búsqueda por lenguaje natural (WizSeek) y configuración automatizada mediante IA, optimizando la eficiencia operativa y la experiencia de usuario.

Dahua continuará evolucionando su modelo Xinghan AI para fomentar la transformación inteligente en seguridad pública, transporte, energía y entornos empresariales.

Para zonas públicas como salidas de incendios y vías de emergencia, **TiOC** también es una opción acertada, ya que puede vigilar y mantener zonas libres de obstáculos de forma eficaz.

+información

Vigiplus PSIM Mantenimiento

Tu seguridad, siempre a punto

DESICO®

En Desico, somos conscientes de que el mantenimiento adecuado es la clave para un sistema de Seguridad efectivo. Es por ello, por lo que Desico ha desarrollado un nuevo módulo de mantenimiento que permite la gestión de las tareas de mantenimiento utilizando el interfaz Vigiplus PSIM.

Centraliza y automatiza todas las tareas de mantenimiento desde el mismo entorno **Vigiplus PSIM**. Programa, ejecuta y audita revisiones en un único sistema –junto al resto de tu información de Seguridad– para ganar control, rapidez y trazabilidad.

Beneficios clave:

- **Toda la información en un solo lugar:** datos técnicos (fechas de instalación, IP, puertos, geolocalización, fotos) integrados con la operación de Seguridad.
- **Planificación inteligente:** crea grupos de mantenimiento, define periodicidades y recibe avisos automáticos de revisiones.
- **Actuación precisa**: gestiona elementos de forma agrupada (mantenimiento periódico) o individual (cuando requieren intervención específica).
- **Trazabilidad total:** historial por instalación y por elemento, con estados, incidencias y exportación a Excel o Power BI para un análisis completo.
- **Confianza demostrada.**

Muchos clientes ya confían en esta solución para gestionar el mantenimiento de sus instalaciones de seguridad.

Solicita una demostración y comprueba cómo simplificar el mantenimiento sin salir de Vigiplus PSIM a comercial@desico.com

Transforma y digitaliza tu mantenimiento: menos olvidos y más disponibilidad de tus sistemas.

dormakaba

Si gestionas un edificio —o varios—, resivo te ahorra tiempo y complicaciones. Es un sistema de gestión de accesos en la nube que sustituye llaves por credenciales digitales y te da control desde el móvil o el ordenador.

Su valor clave para ti: acceso remoto real. Abre puertas, autoriza entradas temporales o recurrentes y revoca permisos al instante, sin desplazarte y con trazabilidad.

Optimiza el día a día: crea permisos en lote para mudanzas o mantenimiento, da acceso puntual a repartidores, técnicos y contratistas, y define horarios por zonas. Si alguien pierde una llave... ya no es un incidente: desactiva su credencial y listo. Todo queda registrado para auditorías y cumplimiento.

resivo convive con tu infraestructura: empieza por puntos críticos y se amplía según necesidades, sin proyectos interminables. La app es intuitiva para inquilinos y el panel de administración ofrece vista global del edificio, alertas y control por perfiles. Menos entregas físicas, menos copias, menos urgencias de "ven a abrir". Más eficiencia operativa y mejor experiencia para quien vive y trabaja en el edificio.

Haz que tu gestión sea tan ágil como tu agenda con **resivo.**

+información

La importancia de centralizar los sistemas de seguridad para una protección integral

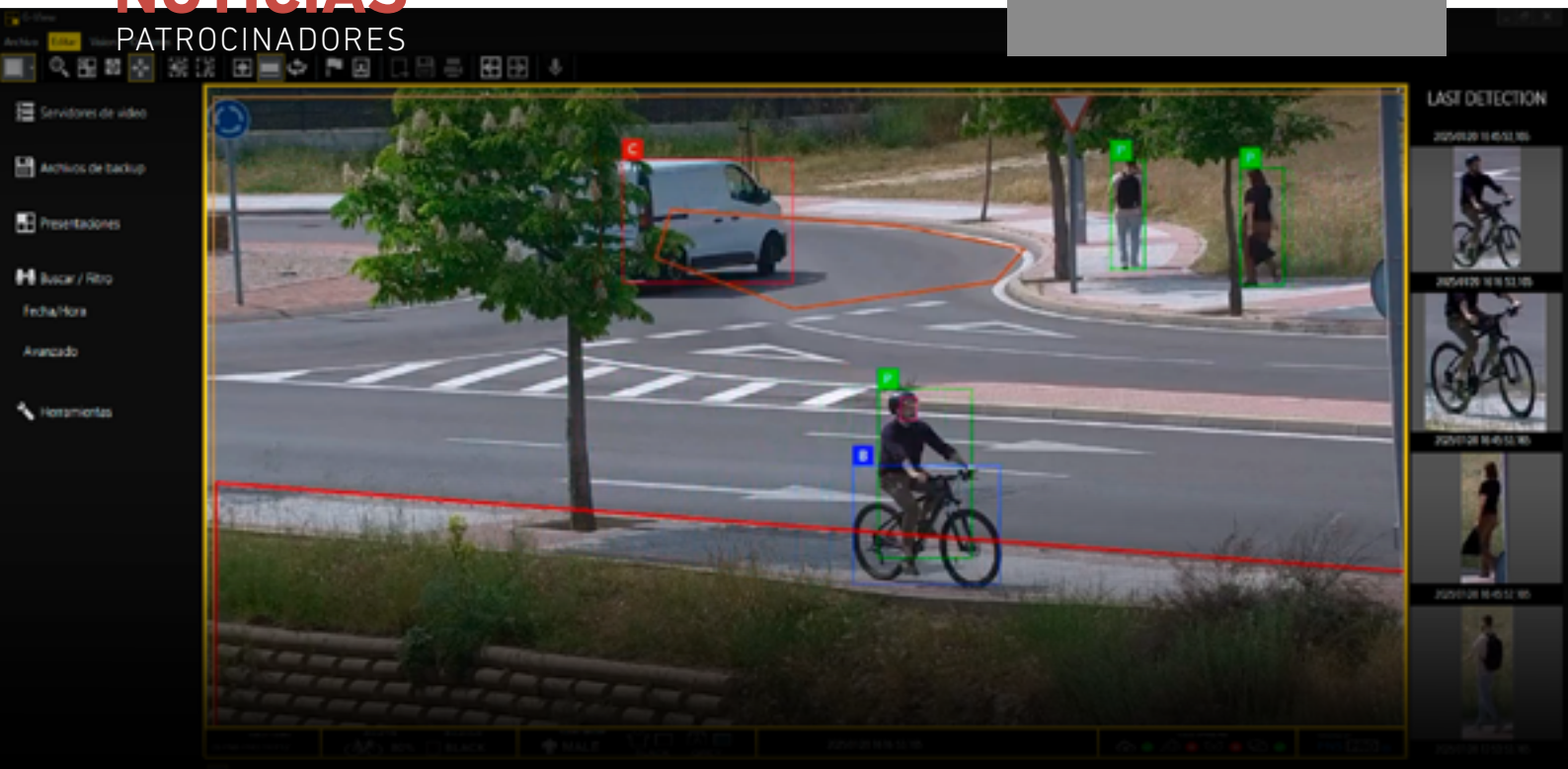
En un entorno donde cada segundo cuenta, disponer de un sistema de seguridad capaz de integrar y gestionar todos los subsistemas de manera centralizada es esencial para proteger infraestructuras críticas.

Sistemas como el control de accesos, el control por video VMS, las alarmas de intrusión y de incendios o la megafonía, por nombrar algunos, deben de operar de forma conjunta y coordinada para proporcional una respuesta ágil y efectiva ante cualquier situación de emergencia.

DASSnet®, la plataforma de gestión integral de **DORLET**®, se posiciona como una solución líder en este campo. Este software no solo permite integrar sus propios sistemas, sino que también se conecta con tecnologías de terceros, ofreciendo una visión global y detallada de toda la instalación. Su interfaz intuitiva y capacidad de análisis en tiempo real facilitan la toma de decisiones informadas, ya sea para activar protocolos de emergencia, gestionar accesos o realizar un seguimiento exhaustivo de los incidentes.

Optar por **DASSnet**® garantiza una mayor eficiencia operativa, mejora la coordinación entre equipos y minimiza los tiempos de reacción. Para las infraestructuras críticas, donde la protección de personas y recursos es primordial, esta solución representa un paso adelante hacia la seguridad integral y la resiliencia ante cualquier eventualidad.

VIDEOSISTEMAS FFV GEUTEBRÜCK



Cámaras PNS-PRO IA ULTRA SERIES

Donde la seguridad se une con la inteligencia artificial

Desde F.F.Videosistemas seguimos marcando la diferencia en el mundo de la videovigilancia con nuestras cámaras con Inteligencia Artificial Avanzada PNS-PRO ULTRA SERIES.

Hace cuatro años lanzamos esta línea revolucionaria que transformó la manera de proteger espacios, incorporando algoritmos Deep Learning capaces de analizar, clasificar y enviar alertas automáticas en cada escena.

Nuestras cámaras detectan y clasifican personas, bicicletas y vehículos identificando atributos como género, color de prendas, color de vehículo o bicicleta, y accesorios como mochilas o gafas.

Las analíticas avanzadas –como detección de pelea, persona caída, vehículo detenido, circulación en sentido contrario, conteo y velocidad de vehículos– ofrecen respuestas inmediatas, reducción de falsas alarmas y toma de decisiones en tiempo real, aumentando la eficiencia operativa y la prevención de incidentes.

Gracias a su flexibilidad, las cámaras **PNS-PRO IAULTRA SERIES** se aplican con éxito en ciudades inteligentes, infraestructuras críticas, hospitales, comercios, transporte y entidades financieras, adaptándose a cada necesidad.

En **F.F. Videosistemas**, seguimos evolucionando juanto a nuestros clientes.

Con las **cámaras IA Ultra Series**, la seguridad se vuelve simple, inteligente y confiable.

Hanwha Vision lanza su nueva generación de

Cámaras Térmicas QVGA con IA

Estas nuevas soluciones incorporan detección de objetos basada en Inteligencia Artificial, imagen térmica avanzada, con un NETD (Diferencia de Temperatura Equivalente al Ruido) inferior a 20 mK a 25°C, que permite detectar diferencias de apenas 0,02 °C, estas cámaras ultrasensibles ofrecen un contraste térmico excepcional.

Esto permite capturar imágenes más nítidas y detalladas incluso en entornos de bajo contraste (humedad, niebla, largas distancias). Además, la gama admite la detección de cambios de temperatura en tres áreas.

Se trata de una solución perimetral precisa y fiable, para uso en distintas condiciones atmosféricas y lumínicas, aplicable tanto a pequeños como a grandes perímetros.

La detección precisa de objetos mediante Inteligencia Artificial permite identificar en tiempo real personas y vehículos, reduciendo las falsas alarmas causadas por sombras, animales u objetos movidos por el viento. Los análisis de eventos (línea virtual, merodeo) facilitan una supervisión más proactiva.

La detección de movimiento basada en Inteligencia Artificial ayuda a los equipos a centrarse solo en los movimientos relevantes.

Las opciones de lentes (13 mm, 19 mm, 35 mm y 60 mm) disponibles en versiones de cámaras de 8 fps o 30 fps proporcionando una cobertura flexible para distintas distancias.

Otras características:

- **IP67, IK10 NEMA 4X, NEMA-TS 2, MIL-STD-810H.**
- **RJ-45 blindado**
- **Ciberseguridad FIPS 140-3 Nivel 3 CC-EAL6+**
- **Integración con Genetec, Milestone y Wisenet WAVE.**

Modelos 8fps TNO-C3042T / 52T / 62T / 82T
Modelos 30fps: TNO-C3040T / 50T / 60T / 80T

+información

Johnson Controls

Controladoras con Ciberseguridad de Última Generación iSTAR

Las controladoras de control de acceso son componentes esenciales en la seguridad física de cualquier instalación. Al gestionar la apertura y cierre de puertas, su compromiso puede poner en riesgo tanto la integridad del sistema como la información sensible que almacenan.

Por ello, es fundamental que estos dispositivos incorporen mecanismos avanzados de protección frente a ataques externos y garanticen la confidencialidad y disponibilidad de los datos.

Las controladoras iSTAR elevan el estándar de ciberseguridad en el sector. A diferencia de otras soluciones que se autodenominan "plataformas abiertas", iSTAR pueden utilizar el protocolo MQTT, realmente abierto y reconocido por su robustez y eficiencia. Desde su fabricación, integran Trusted Execution Environment (TEE), asegurando una cadena de confianza desde el inicio. Incorporan Secure Boot, autenticación de comandos y actualizaciones seguras. Además, ofrecen protección contra ataques DoS (Denegación de Servicio), comunicaciones cifradas con TLS 1.3 y AES256 con Certificación FIPS 140-2 (NIST No. 3389), almacenamiento seguro, autenticación de puertos 802.1X, firewalls integrados y detección de brechas.

Con capacidades como OSDP v2, gestión local de hasta un millón de tarjetas, doble tarjeta de red para redundancia y funciones avanzadas como anti-passback global, las controladoras iSTAR incorporan todo tipo de tecnologías y mecanismos, para estar preparados para los desafíos actuales en seguridad electrónica.

Claves técnicas para entender porqué, a veces, el cliente ve sus cámaras y la CRA no*

VISUALIZACIÓN DE IMÁGENES EN LAS CRA*

Óscar Castro

Ingeniero de Telecomunicaciones de Grupo On Seguridad

EN LA PRÁCTICA DIARIA DE LAS CENTRALES RECEPTORAS DE ALARMAS (CRA), ES HABITUAL QUE UN CLIENTE VISUALICE SIN PROBLEMAS SU SISTEMA DE CÁMARAS DE VIDEOVIGILANCIA (CCTV) DESDE LA APP O EL PC, MIENTRAS LA CRA A TRAVÉS DEL SOFTWARE DE GESTIÓN, MANITOU* EN NUESTRO CASO, NO LOGRA ABRIR ESOS MISMOS FLUJOS DE VISUALIZACIÓN EN TIEMPO Y FORMA.

El cliente, e incluso a veces sorprendentemente el propio instalador, se preguntan cómo es posible. El objetivo de este artículo es explicar de forma rigurosa el por qué sucede, cómo diagnosticar cada caso y qué buenas prácticas conviene implantar por parte del instalador para evitar que suceda.

Dos formas de ver cámaras... con objetivos distintos

1.Acceso del cliente.
Suele primar la comodidad. El cliente visualiza sus cámaras desde app, navegador PC o software cliente del fabricante.

- **IP privada* (LAN*):** En LAN no hay dependencia de puertos ni IP pública*, y la estabilidad suele ser máxima. Segura, no depende de Internet.

GLOSARIO DE TÉRMINOS*
Al final del artículo

- **Redirección de puertos con IP/DDNS*(WAN*):** Expone puertos (HTTP*/RTSP*/propietarios) y requiere DDNS si la IP es dinámica. Control directo, pero exige NAT* y expone red a Internet.
- **P2P* en la nube del fabricante:** Evita abrir puertos, pero depende de servidores externos y añade latencia.
- **VPN*:** La VPN es segura, aunque menos habitual en residencial y pymes por su complejidad. Más común en entornos profesionales.

2. Acceso de la CRA.
No se realiza con navegadores ni apps de usuario, sino mediante integraciones específicas del fabricante dentro del software de gestión. La trama* de conexión exige habitualmente parámetros obligatorios tales como dirección (IP, DNS, P2P), credenciales, puerto TCP* propietario, cámara asignada, stream* y la pregrabación* necesaria para verificar eventos con inmediatez. La apertura del clip de vídeo correspondiente debe ser automática al gestionar la alarma. En la gran mayoría de escenarios se requiere redirección de puertos hacia el grabador; algunos fabricantes incorporan acceso por P2P en sus plugins, si bien no es la vía preferente por su impacto en tiempos de acceso.

Conclusión:
El cliente prioriza flexibilidad. La CRA exige inmediatez, robustez y pregrabado. De ahí que la percepción "yo lo veo, la CRA no" sea perfectamente posible, ya que se trata de dos métodos de conexión distintos, con requisitos de red y de tiempos de respuesta también totalmente diferentes.

Causas por las cuales el cliente ve y la CRA no

1. Problemas de conectividad en la red del cliente
- Falta de redirección de puertos TCP propietarios (imprescindibles para la CRA, pero no obligatoriamente el cliente)
- Cambio/cierre de puertos tras actualización de router o cambio de ISP* (proveedor de internet).
- IP dinámica sin DDNS operativo
- CGNAT* del operador impide acceso entrante.
- Ancho de banda de subida insuficiente o conexión inestable
- Caídas del cloud del fabricante (afecta al P2P).

2. Problemas en el grabador del cliente
- Credenciales de usuario y contraseña erróneas
- Credenciales cambiadas y no comunicadas a CRA
- Cuentas bloqueadas por intentos fallidos.
- Límites de conexiones simultáneas (si el cliente está dentro, la CRA puede quedar fuera).
- Sesiones colgadas
- Discrepancias de stream. La CRA solicita substream* por ejemplo y está deshabilitado en configuración.
- Firmware desactualizado
- Bugs en la parte de integración.

3. **Problemas en la infraestructura del fabricante o de la CRA**
   - Plugin* del fabricante obsoleto o con fallos
   - Conflictos entre plugins de distintos fabricantes.
   - Desalineación entre versión de firmware del grabador y plugin del fabricante que se instala en la CRA.
     El fabricante debe notificar a la CRA
   - Incidencias puntuales de red de la CRA o del fabricante.
   - Errores humanos al dar de alta la trama (puerto, usuario, parámetros de pregrabación o stream).
     Con automatización estos errores tienden a desaparecer

Tramas y parámetros a configurar en la CRA: el detalle importa

Como comentamos anteriormente, una trama que permite visualizar en CRA el sistema de cámaras del cliente incluye varios parámetros obligatorios. Estos parámetros condicionan la apertura automática, la calidad y la fluidez del vídeo. Una sola incongruencia (cámara mal numerada, stream inexistente, puerto sin NAT) basta para que la CRA no muestre vídeo, aunque el cliente sí lo haga por otra vía.

Protocolo de diagnóstico

1. **Identificar el modo de acceso que usó el cliente y el que usó la CRA.**
   Ejemplo: el hecho de que el cliente vea por P2P no valida el acceso de la CRA si ésta necesita puerto propietario redirigido.
2. **Comprobar red desde la CRA:**
   Resolución de nombre (DDNS), conectividad a IP/puerto propietario.
   Verificar si hay CGNAT.
3. **Revisar grabador:**
   Estado de usuarios, límites de sesión, streams habilitados, firmware y sesiones colgadas.
4. **Auditar la trama en Manitou:**
   Usuario/clave, puerto, cámara, stream, segundos de pregrabación, parámetros especiales del plugin.
5. **Plugins:**
   Validar versión homologada por fabricante para ese firmware; descartar conflictos si conviven múltiples plugins.
6. **P2P:**
   Si el fabricante soporta P2P en su plugin, evaluar latencia y estabilidad, y asumir que no equivale a la experiencia del cliente (son flujos y rutas distintas).

Conclusión:

Que el cliente vea sus cámaras no garantiza que la CRA pueda verlas: usan caminos distintos. La clave es acordar y documentar con el instalador/mantenedor cómo accederá la CRA a las cámaras, probarlo y revisarlo cada vez que el cliente realice un cambio de red, de router u operador, de credenciales o cada vez que se actualice el equipo.

Con este acuerdo y un mantenimiento básico, el “cliente lo ve y la CRA no” dejará de ser un problema y pasará a ser previsible y evitable.

GLOSARIO

Definición y símil breve de los conceptos técnicos mencionados en el artículo:

IP pública:
Es la dirección que ve Internet (mundo exterior) para llegar a la red del cliente (casa del cliente). Con esa dirección, el "cartero" sabe a qué "edificio" ir.

IP dinámica:
El operador va cambiando aleatoriamente la IP del cliente. El edificio va cambiando de dirección; hay que mirar la guía cada vez (o usar DDNS).

IP fija:
El operador asigna siempre la misma IP al cliente. Dirección permanente del edificio.

IP Privada:
Es la dirección interna de los equipos del cliente (grabador, cámaras...). Número de piso/puerta dentro del edificio. Desde la calle no se ve, solo desde dentro.

LAN:
Es todo lo que está dentro de cada casa o empresa (habitaciones, pasillos, salones...). Se comunican entre ellas sin salir fuera del edificio. Las cámaras están en la LAN, en casa.

WAN:
Es todo lo que está fuera de cada casa o empresa (calle, ciudad). El router de un operador es el equipo que permite salir de casa a la calle. La CRA está en la WAN, en la calle.

ISP:
Operador de internet que te asigna una IP para identificarte en el mundo exterior. La compañía correos que te asigna la dirección del edificio.

HTTP:
Es el idioma que permite hablar con los servidores de cámaras. Cómo hablas con la consola del edificio.

TCP:
Un modo de comunicación con garantías entre dos equipos. Llamada con acuse de recibo: cada mensaje se confirma y llega en orden.

Manitou:
Software de gestión de alarmas desde donde la CRA visualiza las cámaras de un cliente. Central de control que, desde fuera, solicita a cada edificio su vídeo cuando hay una alarma.

CGNAT:
El operador coloca a muchos clientes detrás de una única IP pública, de ahí que no se pueda abrir puertos hacia dentro desde el router del cliente, ya que dicha IP es compartida por varios clientes. Urbanización con una sola dirección común y caseta del guarda: el cartero deja ahí el correo y no puede subir directo a tu portal.

P2P:
Método del fabricante por el que una cámara 'sale' a la nube del proveedor y el usuario accede a través de esa nube. Evita abrir puertos a internet. Mensajería con almacén central: llevas el paquete a una nave y el destinatario lo recoge allí (evita ir portal a portal).

DDNS:
Servicio que asocia un nombre de Internet a una IP pública dinámica. Permite conocer siempre la IP pública del cliente en tiempo real. Es como si un cliente cambiase de edifico constantemente y necesitas buscar por el nombre del cliente y la guía te da la dirección actual.

NAT:
Traducción de direcciones de red de equipos internos del cliente a una única IP pública que es la que se muestra a internet. Requiere redirección de puertos para acceso desde fuera. Conserje del edificio que recoge todo y lo saca a la calle con una única dirección del portal.

Redirección de puertos:
Regla en el router que permite conexiones entrantes en un puerto hacia un equipo interno en concreto, por ejemplo, al grabador. Encargo al conserje: "si llega al buzón 554, súbelo siempre al piso XXX (el grabador).

Upstream:
Ancho de banda de subida del cliente. Si es insuficiente o inestable, el vídeo se corta o no abre. Ancho de la rampa del garaje para sacar paquetes a la calle: si es estrecha o está atascada, los envíos (vídeo) salen mal.

Stream:
Flujo de vídeo principal/secundario que ofrece la cámara/NVR. La CRA suele usar el secundario para abrir más rápido. Tipo de envío: paquete grande (principal) o paquete ligero (secundario) según urgencia y capacidad de la rampa.

Substream:
Flujo secundario de menor resolución/bitrate para ahorrar ancho de banda. LA CRA no necesita calidad, necesita rapidez. Paquete ligero urgente: menos "peso", llega más fluido; la CRA prioriza rapidez sobre lujo del embalaje (resolución).

Plugin:
Programa de integración del fabricante que se instala dentro del software de la CRA (p. ej., Manitou) para visualizar cámaras. Llave compatible en la CRA para abrir el portal de ese edificio y hablar su "idioma".

Trama:
Ficha de conexión del abonado en la CRA: IP/DDNS, puerto, usuario/clave, cámara/stream y parámetros de pregrabación. Tarjeta de acceso + plano del edificio que dice al conserje a qué portal, buzón y piso llamar y qué vídeo pedir.

Pregrabación:
Segundos de vídeo previos al evento que se muestran al abrir una alarma. Cuando llegas al portal, ya puedes ver lo que pasó justo antes.

RTSP:
Protocolo de transporte de vídeo en directo usado por cámaras.

VPN:
Conexión cifrada y segura para acceder a una red de un cliente sin exponer puertos en Internet. Túnel privado bajo la ciudad: vas de tu central a ese edificio sin pasar por la calle abierta.

SDK:
Kit de desarrollo del fabricante para integrar cámaras con software de terceros que permiten la visualización desde la CRA, como con manitou por ejemplo. Manual del constructor para que la CRA pueda usar todas las llaves y funciones del edificio.

CONOCE A UN

SOCIO

Alfonso González Blázquez

SOCIO Nº 63

alfonso.gonzalez.blazquez@jci.com

Por favor, dinos algo sobre ti que permita a nuestros compañeros empezar a conocerte

Soy un profesional con más de 25 años de trayectoria profesional en el sector de la seguridad y he tenido la oportunidad de trabajar tanto en el ámbito público como en el privado. Actualmente desempeño el rol de responsable de Desarrollo de Negocio para el sur de Europa en la división de Security Products de Johnson Controls, anteriormente Tyco.

Mis primeros años estuvieron muy ligados a organismos públicos de gestión de emergencias como Policía, servicios 112, Bomberos, entre otros. En los últimos años, mi enfoque ha estado más orientado hacia soluciones de seguridad para infraestructuras críticas, grandes cuentas y clientes internacionales. Todo ello, ya sea desde el área técnica en mis inicios o más comercial ahora, siempre con una clara orientación tecnológica.

¿Cuál es tu formación académica?

Soy Ingeniero Técnico en Topografía por la Universidad Politécnica de Madrid. Me especialicé en Sistemas de Información Geográfica, lo que supuso mi primer punto de conexión con el mundo de la tecnología. A partir de ahí, completé mi formación con conocimientos en programación —Java, Visual Basic, Visual C++, desarrollo web, SQL, entre otros— que me permitieron ampliar mi perfil técnico y entender mejor la integración de sistemas.

Más adelante, al ir orientando mi carrera hacia roles más vinculados a ventas y desarrollo de negocio, decidí realizar un MBA con especialidad en marketing en la Universidad Camilo José Cela.

Me consta que además de la formación citada has asistido a cursos monográficos complementarios ¿Podrías citarnos algunos?

A nivel técnico, como comentaba, tengo conocimientos en varios lenguajes de programación como Java, Visual Basic, SQL, entre otros, además de experiencia en aspectos relacionados con infraestructuras de redes de comunicaciones.

A lo largo de mi carrera también he complementado mi perfil con formación en gestión de proyectos y liderazgo de equipos, así como cursos específicos en ventas y técnicas de negociación.

¿Cuáles consideras que son actualmente tus puntos fuertes?

Creo que tengo un buen equilibrio entre conocimientos técnicos y comerciales, respaldado por una amplia experiencia en proyectos de seguridad de todo tipo. Esta combinación me ha permitido desarrollar una visión más completa y estratégica, tanto en la definición de soluciones como en la relación con clientes y equipos.

Poder entender las necesidades desde el punto de vista técnico y, al mismo tiempo, saber cómo trasladarlas al ámbito comercial ha sido clave en los distintos roles que he desempeñado a lo largo de mi carrera.

Además de en la actual Johnson Controls Security Products ¿En qué empresas has desarrollado tu carrera profesional y con qué responsabilidades?

Tuve una primera etapa en Siemens, donde entré como estudiante en prácticas gracias a una beca de colaboración entre la Universidad Politécnica de Madrid y la compañía. Durante ese periodo desarrollé principalmente mi perfil técnico como analista programador, y terminé esta etapa como Jefe de Proyecto, liderando equipos y gestionando desarrollos tecnológicos. Fue una experiencia muy enriquecedora que me permitió crecer profesionalmente desde la base.

En una segunda etapa, me incorporé a Intergraph (hoy Hexagon), donde evolucioné hacia un rol más orientado al negocio, trabajando como Consultor Preventa. Allí apoyaba los procesos de venta en proyectos de seguridad, especialmente en el ámbito de la integración de sistemas, con un enfoque muy centrado en el sector público.

Finalmente, mi siguiente etapa comenzó en Tyco —hoy Johnson Controls—, donde estuve cinco años como Product Manager. Desde hace ya ocho años, desempeño el rol de responsable de Desarrollo de Negocio en el área de Security Products, combinando mi experiencia técnica con una visión estratégica y comercial para impulsar soluciones innovadoras y adaptadas a las necesidades del mercado.

Tu paso por Siemens pienso que han sido etapas decisivas en tu formación que habrás aplicado a los aspectos IT de los equipos y sistemas actuales. Háblanos de ello por favor.

Sí, totalmente. Fue una época en la que empezaban a surgir múltiples tecnologías emergentes en el mercado, como Internet o las comunicaciones móviles, entre otras. Esto hacía que los proyectos fueran auténticos retos tecnológicos, ya que muchas veces había que construir soluciones prácticamente desde cero, sin referencias previas ni estándares consolidados.

En ese momento, mi perfil era puramente técnico, centrado en el desarrollo de integraciones de sistemas muy diversos: CCTV, control de accesos, SIG, sensores, comunicaciones GPRS o por radio, entre otros. Fue una etapa muy enriquecedora, que me permitió adquirir una base sólida en tecnología aplicada y entender cómo conectar distintos mundos tecnológicos.

Sin duda, esa formación y experiencia han sido clave a lo largo de mi carrera. Me han permitido comprender en profundidad la tecnología actual y proponer soluciones con una base técnica robusta, alineadas con las necesidades reales de los proyectos.

Has acumulado experiencia en gestión comercial y también en equipos y soluciones técnicas. ¿Con cuál de los dos aspectos te sientes más identificado?

De la parte comercial, lo que más valoro son las relaciones personales que se van construyendo con el tiempo. Sin embargo, en nuestro sector, la base tecnológica es fundamental y debe estar siempre presente. Creo que me desenvuelvo con soltura en ambos ámbitos: por un lado, en la gestión de relaciones y desarrollo de negocio, y por otro, en el entendimiento técnico que me permite aportar valor real y diferenciado a los clientes.

Dado que trabajas en los mercados de España y del Sur de Europa ¿Qué diferencias y analogías encuentras entre los diferentes países?

Creo que en toda la cuenca mediterránea compartimos muchas similitudes en el ámbito social, especialmente en la forma en que entendemos y valoramos las relaciones personales dentro del entorno empresarial. En nuestra cultura, establecer vínculos de confianza es clave para hacer negocios, y muchas veces estas relaciones son tan importantes como la propia propuesta comercial.

Sin embargo, sí percibo algunas diferencias cuando comparo con otros países del sur de Europa. En general, son más abiertos a explorar nuevas soluciones y tecnologías, mostrando una mayor predisposición al cambio y a la innovación. En España, por el contrario, solemos ser más conservadores; nos cuesta salir de lo conocido y explorar alternativas distintas a las ya establecidas.

También gestionas seminarios web ¿Qué perfil de asistente es el que más acude a este tipo de formación

Especialmente destacaría los Ingenieros de Proyectos que suelen ser perfiles con una alta carga de trabajo, lo que lamentablemente les deja poco margen para visitar fabricantes o asistir a congresos y eventos del sector. Sin embargo, son precisamente quienes más necesitan estar al día en cuanto a novedades tecnológicas, tendencias y soluciones emergentes.

En ese sentido, los webinars se han convertido en una herramienta muy valiosa para ellos: permiten acceder a contenido actualizado de forma flexible, sin necesidad de desplazamientos ni grandes inversiones de tiempo. Esta modalidad les facilita mantenerse informados y seguir desarrollando su conocimiento técnico, algo esencial para tomar decisiones acertadas en sus proyectos.

Desde el punto de vista de la ingeniería ¿Cuál es tu opinión sobre el valor que da el cliente a la fase de proyecto y a la dirección de obra? ¿Sabemos "vender" su necesidad?

Lamentablemente, y en comparación con muchos otros países europeos, la fase de diseño de proyectos en España suele carecer, en demasiadas ocasiones, del nivel de definición técnico necesario. Esta falta de detalle técnico inicial provoca que durante la ejecución surjan sorpresas, improvisaciones y, en muchos casos, una mala implementación del proyecto.

Una parte importante de este problema recae en una mala planificación o simplemente en las prisas por obtener un presupuesto rápidamente, sin haber dedicado el tiempo suficiente a una toma de requerimientos adecuada ni a un diseño técnico sólido. Esta prisa por avanzar sin una base clara termina afectando la calidad del resultado.

En este contexto, me gustaría poner en valor el papel de las ingenierías de seguridad, que en España están poco presentes y, sin embargo, en otros países constituyen un sector especializado con gran relevancia.

Estas ingenierías aportan rigor técnico, visión integral y una metodología que permite anticipar problemas y asegurar una ejecución más eficiente y alineada con los objetivos del cliente. Fomentar su participación desde las fases iniciales del proyecto sería un paso importante hacia una mejora estructural en la forma en que se desarrollan los proyectos de seguridad en nuestro país.

¿Qué opinas de la utilización de la IA en la realización de proyectos de ingeniería de seguridad?

Creo que va a ser una herramienta de gran valor para el diseño y la redacción de proyectos. Especialmente porque permitirá agilizar tareas monótonas y repetitivas, liberando tiempo para que los Ingenieros de Seguridad podamos centrarnos en aspectos más

estratégicos, como el diseño conceptual y el cumplimiento de los requisitos técnicos y operativos. Esta optimización no solo mejorará la eficiencia del proceso, sino que creo que también elevará la calidad, al permitirnos dedicar más atención a lo que realmente aporta valor.

Espero que aparte de tu dedicación profesional, dispongas de tiempo para cultivar otras actividades y aficiones ¿Qué te gusta hacer?

Me encanta pasar tiempo con mi familia, ya sea viajando, esquiando o simplemente disfrutando juntos. También soy muy fan del senderismo, me gusta perderme por la montaña y desconectar un rato. Y cuando estoy en casa, el bricolaje es mi vía de escape: siempre tengo algún proyecto entre manos, arreglando cosas o montando algo nuevo.

Eres socio de AEINSE desde hace algún tiempo ¿Qué te llevó hasta nuestra asociación?

Además de que grandes amigos me animaron a hacerme socio, sentía que era muy importante dar visibilidad a un sector profesional que, aunque puede tener orígenes académicos muy diversos —ingenieros industriales, electrónicos, informáticos, de telecomunicaciones, o incluso como en mi caso, de topografía—, comparte una formación especializada y una experiencia común que nos convierte en un colectivo único. Y ese colectivo, en mi opinión, merecía tener más presencia y reconocimiento en la sociedad.

Es raro encontrar sectores tan especializados como el nuestro que no tengan una visibilidad clara ni en la etapa formativa ni en el entorno profesional. Por eso considero tan relevante el papel de la asociación: nos da voz, nos conecta y nos permite avanzar como grupo.

Lo que sí quiero destacar especialmente es el ambiente que se respira en la asociación. Para mí es un auténtico placer ver cómo, entre todos, vamos creciendo como colectivo. Hay una energía muy positiva, y cada uno aporta su granito de arena con ilusión y compromiso, todos en una misma dirección.

Finalmente ¿Tienes alguna sugerencia que nos ayude a mejorar la visibilidad de la Asociación y aportar mayor valor a los socios.

Seguir avanzando como lo estamos haciendo con la asociación me parece fundamental, pero si tuviera que destacar algo especialmente importante, serían las recomendaciones técnicas y las buenas prácticas. Creo que son clave para profesionalizar aún más nuestro sector, aportar valor real y marcar una diferencia en cómo se diseñan y ejecutan los proyectos.

Contar con guías claras, criterios compartidos y experiencias contrastadas nos ayuda no solo a mejorar la calidad del trabajo, sino también a generar confianza entre clientes, colaboradores y otros profesionales. Además, estas recomendaciones permiten que todos, independientemente de nuestro recorrido profesional, podamos alinearnos en una misma dirección y crecer como colectivo.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Nace el GRUPO

Casnova

casnova

"En Casnova queremos inspirar, transformar, impulsar al sector de la seguridad a un siguiente nivel a través de iniciativas novedosas y colaborativas. Guiados por nuestros valores –**compromiso, innovación, servicio excepcional y visión de futuro** –, preservaremos la independencia, esencia y excelencia de cada una de las empresas del grupo", afirma **Montse Castro Roca, presidenta del Grupo Casnova y CEO de** Casmar.

El objetivo del nuevo grupo empresarial Casnova se centra en **impulsar iniciativas innovadoras y colaborativas para y por el sector**, así como fomentar el crecimiento equilibrado y sostenible de sus empresas, **Casmar y Desico**, que si bien **cada una de ellas mantendrá su independencia.**

Montse Castro Roca continuará liderando Casmar, mientras que será en abril de 2026 cuando José Luis Martín Hurtado, fundador y CEO actual de Desico, con una gran trayectoria profesional y visión estratégica e innovadora, ceda el testigo a **Enrique Bilbao Lázaro**, actual director adjunto de Desico, quien **asumirá la dirección ejecutiva de la compañía**, garantizando continuidad y evolución.

Grupo Casnova: proyectos innovadores y colaborativos

Más de 130 profesionales formarán parte del grupo empresarial, que apuesta por un **crecimiento sostenible, independiente y colaborativo**. Casmar cuenta con más de 100 empleados entre España, Portugal y Chile, mientras que en Desico trabajan más de 30 empleados entre España y México. El plan estratégico de Casnova, que comenzará a desplegarse en el primer semestre de 2026, se centrará en proyectos innovadores y colaborativos que generen impacto tanto en el sector como en la sociedad.

El **Grupo Casnova** surge con la misión de liderar la transformación del sector de la seguridad, combinando la experiencia consolidada de **Casmar** y **Desico** con la fuerza de la innovación tecnológica.

La creación del grupo es el siguiente paso a la adquisición de **Desico**, en 2024, por parte de los **hermanos Castro Roca**, tras el sólido legado que **Gonzalo Castro Mat**a, fundador de **Casmar**, deja a sus hijos, consolidando así un proyecto que une talento y visión de futuro bajo una marca común.

El Grupo Casnova se presentará oficialmente en febrero 2026 durante la feria de seguridad SICUR

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

ENERO-JUNIO 2025

Balance Trimestral Seguridad

Publicado por la Secretaría de Estado de Seguridad el balance Trimestral de Seguridad correspondiente al segundo trimestre del presente año.

El documento recoge la evolución de la criminalidad registrada en España durante los tres meses del año por la Policía Nacional, Guardia Civil, Ertzaintza, Mossos d'Esquadra, Policía Foral de Navarra, y también por aquellos Cuerpos de Policía Local que facilitan datos a las Fuerzas y Cuerpos de Seguridad del Estado.

En el período de enero a junio de 2025, y en comparación con igual período de 2024, la criminalidad total registrada policialmente en España ha decrecido un 0,9 por ciento.

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Security Forum'25

JUN
4 y 5

Los días 4 y 5 de junio pasado se celebró en Barcelona, en el escenario de Les Drassanes Reials, la duodécima edición de SECURITY FORUM organizado, un año más, por Cuadernos de Seguridad, con el impulso d Peldaño Media Group y el apoyo del Ayuntameinto de Barcelona.

Al evento acudieron más de 3.000 profesionales de la seguridad. A lo largo de las dos jornadas se sucedieron las ponencias y debates del programa "expert panel" se abordaron temas como PERSEO: aplicación para la gestión avanzada de casos policiales, el universo normativo y certificable actual en el sector TI y de la ciberseguridad, la detección de gases en servicios de bomberos de Barcelona, el modelo español de la Seguridad Privada, el reconocimiento o identificación, las imágenes videográficas comoprueba en un procedimiento judicial, etc.

+información

A partir de la página 44 del número 382 de Cuadernos de Seguridad se encuentra la información detallada del evento.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

7ª CONFERENCIA SECTORIAL

Seguridad de Puertos

Organizada por la Fundación Borredá en colaboaracíon con Puertos del Estado, Seguritecnia y Red Seguridad, el próximo 4 de noviembre, el Auditorio de Cecabank, Madrid, se celebrará la séptima edición de la Conferencia Sectorial de Seguridad en Puertos.

El evento se centrará en asuntos actualmente estratégicos como La evolución de la normativa en protección portuaria, lecciones aprendidas en su implementación y recomendaciones, retos y prioridades en la seguridad del sistema portuario, servicios de ciberseguridad aplicados al sector, la red global de sistemas antidrones, el crimen organizado en los puertos y soluciones tecnológicas avanzadas implantadas en puertos nacionales e internacionales.

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

La gestión del CISO:

Retos prácticos y normativos en un entorno en transformación

Con este lema, Cuadernos de seguridad organizó, en el mes de junio pasado, un encuentro que reunió a varios profesionales del sector con el fin de debatir sobre el papel del CISO ante un escenario en el que la ciberseguridad es un elemento estratégico.

Coordinado por la directora de Programas de Cuadernos de Seguridad, **Gemma G. Junaes** y moderado por **Iván Rubio**, director de Cuadernos de Seguridad, se debatió, entre otros aspectos, sobre el cambio de paradigma en el rol de Ciso, las competencias del **CISO** más allá de la ciberseguridad, la sobrecarga de normativa y el apoyo insuficiente, los riesgos emergentes..

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Feria Sicurezza 2025

INTERNATIONAL SECURITY & FIRE EXHIBITION

Los días 19 a 21 de noviembre tendrá lugar en Milán, en el recinto fieramilano, una nueva edición de SICUREZZA.

Una feria internacional dedicada a soluciones de seguridad y protección. El evento se concentra en la innovación en videovigilancia, control de accesos, anti-intrusión, detección y extinción de incendios, así como de las nuevas fronteras de la ciberseguridad y el uno de drones.

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Estrategia de Seguridad Aeroespacial Nacional

El Boletín Oficial del Estado ha publicado el pasado día 5 de agosto la segunda Estrategia de Seguridad Aeroespacial Nacional 2025 (ESAN), previamente aprobada el 14 de julio por el Consejo de Seguridad Nacional.

Desde la aprobación de la primera Estrategia, publicada en 2019, según el texto del documento, "los rápidos y significativos cambios en los dominios aéreo y espacial han tenido un impacto directo en el ámbito aeroespacial. Esta dinámica de cambio ha impulsado la necesidad de ampliar las previsiones existentes en la anterior ESAN para incorporar nuevos aspectos relacionados con la seguridad del espacio aéreo y ultraterrestre".

+información

LEÍDO, VISTO Y OÍDO EN...

Como indica en su introducción "La Guía Básica de la IA nace de la necesidad de proporcionar una base sólida de conocimientos sobre la Inteligencia Artificial a aquellos profesionales que desean entender cómo esta tecnología puede aplicarse en sus respectivos campos..."

Impulsada por el proyecto **Smart Digital** en la Comunidad Valenciana y elaborada con la colaboración de quince colegios profesionales y otros expertos en IA. En su redacción ha colaborado nuestro compañero en **AEINSE, Ramón Segarra**,

La guía desarrolla a lo largo de 496 páginas aspectos, entre otros, como los **Fundamentos, Desafíos, Ética, Regulación y Futuro de la IA,**

+información

Centro Nacional Ciberseguridad

Interesante artículo de **Elena de la Calle**, Consejera técnica en la Unidad de Ciberseguridad y Contra la Desinformación del Departamento de Seguridad Nacional.

"Una de las principales novedades que recoge el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad es el establecimiento de un Centro Nacional de Ciberseguridad, que deberá crearse en un plazo de 12 meses desde la entrada en vigor de la ley. Su creación se justifica por la necesidad de superar la actual dispersión competencial en materia de ciberseguridad. De esta manera, el Centro se constituiría en Autoridad nacional competente única para..."

artículo completo - pág 108

LEÍDO, VISTO Y OÍDO EN...

The future of Energy
is subatomic...

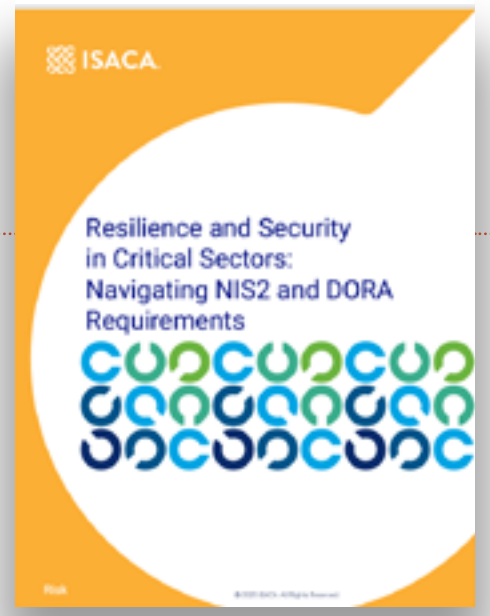
"A menudo, se confunden las dos tecnologías (fisión y fusión nuclear), lo cual es comprensible dado lo similares que parecen en la superficie. Pero la realidad es que, en muchos aspectos, la fisión y la fusión son opuestas. Conocer cómo funciona cada una—y por qué son diferentes—es fundamental para comprender los roles que desempeñarán en las próximas décadas..."

"La carrera por comercializar la energía de fusión se ha acelerado. Commonwealth Fusion Systems, una empresa que apoyo a través de Breakthrough Energy, es la que más avanzada está: están en camino de poner energía en la red a principios de la década de 2030..."

Bill Gates explica en este artículo las diferencias entre fisión y fusión nuclear como procesos para obtener energía eléctrica. Defendiendo las ventajas de esta última frente a la primera.

artículo completo

LEÍDO, VISTO Y OÍDO EN...



Informe técnico ISACA

Resiliencia y Seguridad en Sectores Críticos: Navegando por los requisitos de NIS2 y DORA

"Las empresas deben determinar si cumplen con NIS2 y/o DORA, ya que el incumplimiento podría generar grandes multas y posibles daños a la reputación.

También es importante tener en cuenta que las empresas que proporcionan sus productos o servicios a entidades financieras o entidades esenciales o importantes en la Unión Europea pueden tener obligaciones adicionales en virtud de NIS2 y/o DORA, por lo que es esencial estar familiarizado con los requisitos de la directiva y el reglamento".

+información

LEÍDO, VISTO Y OÍDO EN...


Manuel Sánchez Gómez-Merelo

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

Inicio Contacto English Mi experiencia Mi otra pasion Mis libros

Seguridad Global Corporativa. 10 nuevos paradigmas y retos para avanzar

1 Vote

La Seguridad Global Corporativa está experimentando una evolución hacia nuevos paradigmas que buscan una protección más efectiva, considerando la complejidad y la interconexión de los desafíos actuales. Estos nuevos paradigmas deben integrar la Seguridad con el desarrollo y los Derechos Humanos, promoviendo la participación ciudadana y teniendo como enfoque principal el uso de tecnologías emergentes para la prevención, protección y respuesta ante amenazas.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Nuevos Paradigmas de Seguridad Corporativa

Los nuevos paradigmas de Seguridad Corporativa enfatizan un enfoque integral que va más allá de la protección física, abarcando aspectos como la Seguridad de la Información y la Ciberseguridad, la Seguridad Ambiental y la Seguridad Humana. Este enfoque holístico considera la seguridad como una estrategia integrada que protege tanto los activos físicos como los intangibles de una organización, incluyendo sus datos, sistemas, personal y entorno de actividad.

Seguridad Global Corporativa

Manuel Sánchez Gómez-Merelo

"La Seguridad Global Corporativa está experimentando una evolución hacia nuevos paradigmas que buscan una protección más efectiva, considerando la complejidad y la interconexión de los desafíos actuales. Estos nuevos paradigmas deben integrar la Seguridad con el desarrollo y los Derechos Humanos, promoviendo la participación ciudadana y teniendo como enfoque principal el uso de tecnologías emergentes para la prevención, protección y respuesta ante amenazas".

+información

Tecnología: ¿amenaza o solución?

Artículo de Oriol Verdura, vocal de ADSI

"Ya os adelanto la respuesta a la pregunta del titular: la tecnología es tanto una amenaza como su solución. La seguridad empresarial está viviendo una revolución sin precedentes, impulsada por tecnologías disruptivas que redefinen tanto los riesgos como las oportunidades del sector. Inteligencia artificial, automatización, integración ciber-física..."

artículo completo

LEÍDO, VISTO Y OÍDO EN...

¿Es cierto que la IA te espía en los chats de WhatsApp?

red seguridad

"Estos días circula por redes un mensaje viral contando que si no activas una supuesta *configuración avanzada de privacidad*"...

La IA de Whatsapp puede acceder a todos tus mensajes, tanto individuales como en los chats de grupos, además de leer los números de teléfono y los datos personales almacenados en los dispositivos. Según este mensaje, si no activas la opción exponnes toda tu información y la de las personas a las que hayas incluido en chats grupales.

Sin embargo, esta afirmación es...

Leer el artículo completo: aquí

AEINSE
Asociación Española de Ingenieros de Seguridad