BOLETÍN Nº64 DIC 2025

AEINSE

Asociación Española de Ingenieros de Seguridad

Despedida del año... y bienvenido 2026!!

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

Despedida del año...

Y mirada hacia un *futuro ingenieril*

Con la llegada del final de 2025, nuestra asociación se detiene un momento para reflexionar sobre los logros alcanzados y proyectar con ilusión los retos que nos esperan en el próximo año. Ha sido un periodo intenso, marcado por el fortalecimiento de la comunidad profesional y la celebración de eventos que han reafirmado nuestro compromiso con la excelencia en la ingeniería de seguridad.

Uno de los hitos más relevantes fue el Congreso de Ingeniería de Seguridad, que reunió a expertos y profesionales en un espacio de intercambio de conocimiento y experiencias. El congreso se convirtió en un foro de referencia donde se abordaron los desafíos actuales del sector, desde la innovación tecnológica hasta la adaptación normativa, pasando por la importancia de la formación continua. La alta participación y el nivel de las ponencias confirmaron que la ingeniería de seguridad en España avanza con paso firme hacia un futuro más seguro y sostenible.

Durante este año también se alcanzaron objetivos estratégicos de gran valor: se ampliaron las redes de colaboración con instituciones nacionales, se impulsaron programas de capacitación para ingenieros y se reforzó la presencia de AEINSE en eventos sobre seguridad. Estos logros reflejan el esfuerzo colectivo de la asociación y el compromiso de sus miembros por situar la ingeniería de seguridad en el lugar que merece dentro de la sociedad.

Al mismo tiempo, miramos hacia 2026 con entusiasmo. El próximo año estará marcado por dos acontecimientos de especial relevancia. En primer lugar, se celebrarán elecciones en la asociación, al concluir el periodo de dos años de la actual junta directiva.

Este proceso democrático permitirá renovar energías y continuar construyendo una AEINSE abierta, participativa y orientada al futuro. En segundo lugar, nuestra asociación tendrá una destacada participación en SICUR. Será una oportunidad única para mostrar el talento de nuestros profesionales y reforzar la visibilidad de la ingeniería de seguridad en un contexto global.

En estas fechas tan señaladas, queremos desear a todos nuestros socios, colaboradores y amigos una Feliz Navidad y un próspero Año Ingenieril 2026.

Que el nuevo año nos encuentre unidos, con proyectos renovados y con la convicción de que la ingeniería de seguridad seguirá siendo motor de progreso y garantía de bienestar para nuestra sociedad.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

Asamblea General Ordinaria Elección Junta Directiva AEINSE

23 FEB 2026

El día 23 del próximo mes de febrero, día anterior al inicio de SICUR 2026, celebraremos nuestra Asamblea General Ordinaria (AGO). Como en años anteriores, se hace coincidir con la fecha de inicio de SICUR para facilitar los desplazamientos de nuestr@s que no residen en Madrid.

Con antelación suficiente se nos comunicará la hora y el lugar de celebración. Como es tradición, estará seguida de la **Cena de Hermandad**, en la que tendremos oportunidad de conversar y conocernos mejor.

Por otra parte, en 2026 corresponde la elección de la **Nueva Junta Directiva**, lo que se hará dentro de la propia **AGO**.

Ya se ha enviado a los socios la información sobre el Proceso electoral, con la Conformación de la Junta Electoral, información relativa a la Presentación de candidaturas y posterior confirmación de las mismas.

Desde estas líneas os animamos a presentar candidaturas.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

AEINSE estará presente en SICUR 2026 con un stand de representación

Por gentileza de la Organización de SICUR, como en la pasada edición, tendremos un stand de representación de nuestra asociación en este prestigioso evento internacional que el próximo año tendrá lugar en IFEMMA entre los días 24 y 27 de febrero.

Será un lugar de encuentro de los socios y patrocinadores y también un medio para dar a conocer nuestra asociación y su actividad a los visitantes de la feria y, en especial, a los ingenieros del sector

También tenemos prevista la colaboración en alguna de las actividades divulgativas que tendrán lugar durante la feria y que será anunciada en el momento que esté concretada.

sicur Salón Internacional de la Seguridad
24 - 27 FEB **2026**

Os esperamos en SICUR!

Pabellón 10
Stand A13

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

Foro Social sobre Ingenierías

Organiza · Colabora · Con el apoyo técnico

El Consejo Social de la Universidad de Córdoba y la Diputación Provincial de Córdoba celebraron el pasado 13 de noviembre el Foro Social sobre Ingenierías para la Innovación y Desarrollo de la Provincia, un espacio institucional cuyo objetivo es reforzar la conexión entre la universidad pública, el tejido productivo y los agentes sociales para avanzar en una estrategia provincial común en materia de innovación, talento y desarrollo socioeconómico.

El encuentro se celebró en el Campus de Rabanales con la colaboración técnica de **Fundecor** y asistencia de profesores, investigadores y estudiantes de las tres **Escuelas de Ingeniería de la Universidad de Córdoba (UCO).** El evento contó con dos conferencias magistrales:

"Ingeniería basada en el riesgo"
por **Iván Ballesteros,** vicepresidente de la Asociación Española de Ingenieros de Seguridad (AEINSE).

"Evolución de las tecnologías duales: oportunidades y retos en formación"
por **Dr. Gonzalo León Serrano**, Catedrático Emérito de Ingeniería Telemática de la Universidad Politécnica de Madrid.

En la exposición, **Ivan Ballesteros** explicó el riesgo como factor impulsor de la ingeniería en general, y de la ingeniería de seguridad en particular, así como el marco para identificar oportunidades a partir de la gestión del riesgo.

Dejamos aquí constancia del agradecimiento de **AEINSE** al **Consejo Social de la Universidad de Córdoba** por invitarnos a participar en este evento.

+información

Inteligencia avanzada para la gestión de seguridad

Johnson Controls presenta el módulo C·CURE IQ Security Intelligence, una solución que complementa su actual sistemas de gestión de alarmas y que optimiza la seguridad empresarial mediante análisis inteligente y con visualización en tiempo real.

PRINCIPALES CARACTERÍSTICAS:

Alarm Intelligence (inteligencia en alarmas):

- Motor de reglas personalizable para reducir ruido de alarmas.
- Priorización dinámica con *Risk Score* (índice de riesgo) adaptativo según contexto.
- Identificación y eliminación de falsos positivos (ej. accesos autorizados tras alarma).

Cuadros de mandos integrales:

- Vista global de alarmas activas, automatización y localización crítica.
- Seguimiento de categorías, tipos y ubicaciones de alarmas.

Spatial Intelligence (inteligencia espacial):

- *Last Known Location* (última ubicación conocida) para rastreo en tiempo real.
- *Virtual Headcount* o recuento en puntos de reunión en evacuaciones.
- Métricas de acceso y cuadros de mandos de ocupación y asistencia para optimizar recursos.

Automatización y eficiencia:

- Reducción de alarmas redundantes.
- Escalado automático de eventos críticos.

Con estas capacidades, **C·CURE IQ** no solo mejora la respuesta ante incidentes, sino que también aporta datos estratégicos para optimizar espacios y reforzar la seguridad corporativa.

LANACCESS
Discover the power of video.

Soluciones de videovigilancia de Lanaccess
(videograbadores, VMS, analítica basada en IA, dispositivos de display y cámaras IP)

Lanaccess obtiene la certificación ENS en Categoría Alta

Lanaccess da un paso más en su apuesta por la ciberseguridad y consigue la certificación del Esquema Nacional de Seguridad (ENS) en Categoría Alta. Al estar sujeta a la validación del Centro Criptológico Nacional (CCN), se trata del mayor nivel de reconocimiento en ciberseguridad a nivel estatal.

El **ENS** establece los requisitos de protección de la información que deben cumplir tanto la Administración Pública como las empresas que trabajan con ella.

Alcanzar la categoría Alta supone tener implantados controles reforzados para asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos.

La certificación se ha conseguido tras superar auditorías externas independientes que han evaluado los desarrollos de hardware, firmware y software de videovigilancia del centro de **I+D+i** de **Lanaccess** en Barcelona, abarcando todo el ciclo de vida de las soluciones de la compañía.

Certificación de conformidad con el ENS Categoría Alta

Este hito se suma a otras certificaciones y marcos normativos ya implantados (ISO 27001, NDAA, NIS 2, DORA y RGPD) y refuerza una trayectoria de 30 años apostando por el diseño y la fabricación de tecnología de videovigilancia cibersegura y resistente.

El desafío cuántico:
El Q-Day se acerca, ¿estás preparado?

Nuestro sector se basa fundamentalmente en criptografía. Cada autenticación de usuario, cada credencial móvil depende de la criptografía. Se prevé que los ordenadores cuánticos descifren los algoritmos asimétricos más utilizados en la actualidad en los próximos 5-10 años, lo que supone un cambio tecnológico inminente con consecuencias directas en cómo construimos sistemas de seguridad seguros y fiables.

LEGIC y El desafío cuántico

«Almacenar ahora, descifrar más tarde» es un riesgo real. Aunque los datos cifrados sigan estando protegidos hoy en día, la información interceptada podría ser legible en el momento en que maduren las capacidades cuánticas.

Por eso, es recomendable analizar de forma proactiva sus sistemas de seguridad, identificar los componentes vulnerables a la tecnología cuántica.

En **LEGIC**, apoyamos el sector de control de acceso en obtener resistencia cuántica. El diseño de nuestro sistema se basa en una **criptografía simétrica** sólida, que los expertos reconocen hoy en día como resistente a los ataques cuánticos.

En combinación con arquitecturas de seguridad híbridas y en capas y agilidad criptográfica, la plataforma de **LEGIC** está diseñada para evolucionar a medida que evolucionan las amenazas.

En **LEGIC**, seguiremos innovando y colaborando para garantizar que todas las autenticaciones, tanto ahora como en el futuro poscuántico, sigan siendo fiables.

Obtenga nuestra guía
sobre cómo obtener resistencia cuántica...
+información

Protección Perimetral Inalámbrica de Largo Alcance sin Cableado

TAKEX TXF

Sicuralia anuncia el lanzamiento de las nuevas barreras de infrarrojos TAKEX serie TXF. Unos sensores de haz cuádruple, alimentados por baterías y preparados para sistemas inalámbricos.

La **serie TXF** ha sido diseñada pensando en la flexibilidad y el ahorro. Al ser compatible con sistemas inalámbricos líderes, reduce drásticamente el tiempo y el costo de las instalaciones, ya que no requiere cableado ni obras de ingeniería civil. Utilizando baterías de litio de larga duración, los sensores ofrecen una impresionante vida útil de hasta 3 años de servicio.

La fiabilidad del producto es máxima gracias a la tecnología de **Doble Modulación**, que asegura la estabilidad y reduce la posibilidad de activaciones no deseadas causadas por la luz ambiental.

Los sensores pueden proteger distancias exteriores de hasta 100m, con rangos de operación desde los 20m. hasta los 100m. La versatilidad se extiende con 4 frecuencias de canal, lo que permite el uso de múltiples unidades en configuraciones lineales o apiladas sin riesgo de diafonía (crosstalk).

Para garantizar el rendimiento en casi cualquier entorno, las **TXF** cuentan con una carcasa **IP65** y un amplio ajuste óptico de aprox. 90° horizontal y 20° vertical, adaptándose a terrenos irregulares.

También está disponible la opción de cableado híbrido si una de las partes está cerca de una fuente de alimentación.

+información

SCATI obtiene la certificación ISO 27001

reforzando su compromiso con la seguridad de la información

SCATI, fabricante español de soluciones inteligentes de seguridad, ha obtenido la certificación **ISO 27001**, estándar internacional de seguridad de la información.

El logro acredita la solidez de su sistema de gestión y sus medidas para proteger los datos frente a amenazas internas y externas, ofreciendo a clientes, partners y proveedores un entorno seguro y alineado con los más altos estándares.

Con esta certificación, **SCATI** reafirma su propósito de acompañar a las organizaciones en sus necesidades de seguridad con soluciones que no solo aportan eficiencia y control, sino que también cumplen con los máximos niveles de exigencia en materia de ciberseguridad y gestión de la información.

"La certificación ISO 27001 confirma algo que ya formaba parte del ADN de SCATI: nuestro firme compromiso con la seguridad de la información. Este hito avala que nuestros procesos, sistemas y metodologías cumplen con los más altos estándares internacionales, garantizando la confidencialidad, integridad y disponibilidad de los datos", afirma **Jorge Ibáñez**, IT & Maintenance Manager de **SCATI.**

SCATI continuará fortaleciendo sus controles y capacidad de respuesta ante nuevos riesgos para mantener y renovar la certificación y seguir ofreciendo soluciones tecnológicas con la máxima confianza.

AXIS COMMUNICATIONS

Del diseño a la operación: cómo convertir la videoseguridad en valor recurrente con herramientas inteligentes

Los clientes ya no compran cámaras; exigen soluciones completas con servicio continuo, costes predecibles y actualizaciones. Para cumplirlo, los integradores deben orquestar el ciclo de vida completo —diseño, implantación y operación— con herramientas que conecten cada fase y conviertan el proyecto en valor recurrente.

En diseño, **AXIS Site Designer** permite planificar cobertura sobre planos, calcular ancho de banda y almacenamiento, generar documentación y listas de materiales, e importar ajustes al sistema para reducir errores y horas en obra. Su informe de **TCO (Total Cost of Ownership – Coste Total de Propiedad)** incorpora energía y almacenamiento para decisiones más sostenibles, y su integración con **BIM** acelera la coordinación con *stakeholders*.

En implantación y operación, **AXIS Camera Station** estandariza la puesta en marcha y unifica vídeo y control de accesos en una red privada con conectividad opcional a la nube.

Para el servicio gestionado, **Axis Device Manager Extend** ofrece un panel centralizado multi sitio con estado, versiones de software, garantías/EoL y actualizaciones masivas, lo que habilita mantenimiento proactivo, menor tiempo de inactividad y cumplimiento de **SLA.**

El resultado: **implantaciones más rápidas, sistemas coherentes y seguros, y relaciones a largo plazo basadas en datos, eficiencia y transparencia**. Así, el integrador pasa de vender equipos a ofrecer valor medible y recurrente para el cliente.

+información

Ciberseguridad de los datos
para sistemas de vídeo

BOSCH
Video Systems

La inteligencia artificial está cambiando todos los aspectos de nuestras vidas. Las cámaras son sensores inteligentes que recopilan muchos más datos que las imágenes de video seguridad por sí solas. A medida que éstas se conectan al Internet de las Cosas (IoT), se necesitan más y mejores métodos de protección de los datos frente a ciber amenazas.

Los sistemas de video de **Bosch** cuentan con certificaciones críticas de ciberseguridad como la **UL-2900-2-3** o la **IEC 62443-4-1**, además de otras certificaciones y normativas locales.

Estas incluyen, entre otras, la **Directiva de Seguridad de las Redes y de la Información (NIS2)** de la Unión Europea y **la Ley de Ciberresiliencia (CRA)**, o la **Ley de Autorización de Defensa Nacional (NDAA)** y el **Acuerdo Federal de Adquisiciones sobre Acuerdos Comerciales (FAAR)** en los Estados Unidos.

Además de las certificaciones anteriores, también se incluyen coprocesadores criptográficos, protocolos de gestión de certificados, sistemas operativos cerrados y firmware firmado, además de otras medidas para conseguir un sistema fiable y seguro.

En definitiva, los sistemas de video de **Bosch** son sistemas ciberseguros y en cumplimiento con los estándares actuales para ofrecer el mayor nivel de seguridad de los datos.

Casmar acerca la innovación de DEA Security a los profesionales

La seguridad de puertas y ventanas evoluciona con soluciones cada vez más inteligentes y discretas. El detector SN-SPCP-FRC(M) de DEA Security combina un diseño ultrafino y compacto con tecnología avanzada, integrándose dentro de las estructuras sin alterar la estética del entorno. Es ideal para viviendas, comercios o espacios donde la discreción es esencial.

Como distribuidor especializado, **Casmar** acerca este dispositivo a los profesionales del sector, facilitando el acceso a una solución que une eficacia, fiabilidad y facilidad de instalación. Gracias a la **tecnología DEA Sensor Fusion (DSF)**, el detector distingue con precisión golpes, vibraciones, perforaciones o aperturas forzadas, minimizando falsas alarmas. La versión "M" incorpora un sensor magnético para ampliar la protección.

Su instalación es rápida, sin necesidad de controladoras externas, y permite ajustar la sensibilidad mediante siete modos predefinidos o personalizables, adaptándose a diferentes materiales y estructuras. Además, protege frente a sabotajes, identificando interferencias magnéticas, movimientos, alteraciones térmicas y supervisando su propio funcionamiento mediante autodiagnóstico continuo.

Con el **SN-SPCP-FRC(M)**, **Casmar** refuerza su papel como proveedor de soluciones avanzadas, acercando a los profesionales un dispositivo que combina innovación, discreción y seguridad certificada, listo para integrarse en cualquier proyecto sin comprometer el diseño del espacio.

+información

Dahua Infinity 2025

encuentro de cierre de año y visión hacia 2026

El pasado 11 de diciembre, Dahua Iberia celebró en Madrid la primera edición de Dahua Infinity, su evento anual dirigido a sus partners del sector. La compañía organizó este encuentro con el objetivo de compartir los principales avances tecnológicos del año, reforzar la colaboración con su ecosistema de partners y agradecer la confianza recibida en este ejercicio.

Durante la jornada, los asistentes pudieron conocer las novedades presentadas en 2025, así como diversos proyectos desarrollados junto a diferentes partners en ámbitos como la seguridad, la movilidad y la gestión inteligente de entornos. La compañía destacó que este año ha supuesto un periodo de crecimiento y consolidación, por lo que **Infinity** sirvió también como espacio de reconocimiento al esfuerzo y compromiso de sus partners.

Dahua aprovechó igualmente el encuentro para proyectar sus líneas de trabajo de cara a 2026, un año en el que prevé seguir impulsando soluciones basadas en inteligencia artificial, mayor interoperabilidad y modelos más sostenibles, con el fin de aportar un valor añadido creciente a todo su ecosistema.

DESICO refuerza su presencia en Madrid
con nuevas oficinas y una sala de demostraciones

La compañía, como parte de su estrategia de crecimiento, inaugura nueva sede en la capital con una sala de demostraciones que recrea un centro de control de seguridad.

La empresa **DESICO** ha dado un paso estratégico en su consolidación en el mercado nacional con la apertura de sus nuevas oficinas en Madrid. El traslado a esta nueva sede responde al notable crecimiento experimentado por la compañía en los últimos años y a su voluntad de seguir impulsando su expansión, reforzando al mismo tiempo la relación y la proximidad con sus clientes.

Las nuevas instalaciones de **DESICO** no solo ofrecen un mayor espacio y mejores prestaciones para su equipo, sino que incorporan uno de los elementos más distintivos del proyecto: una sala de demostraciones diseñada para reproducir con máxima fidelidad el entorno operativo de un centro de control real, integrando sistemas avanzados de monitorización, gestión de incidentes, integración de todo tipo de señales y análisis en tiempo real. De este modo, clientes y colaboradores pueden experimentar de primera mano cómo funcionan las soluciones de **DESICO** en un entorno similar al que utilizan en su día a día.

Con esta apuesta por instalaciones modernas, versátiles y orientadas a la demostración práctica, **DESICO** reafirma su compromiso de seguir creciendo, innovando y manteniéndose cerca de sus clientes.

dormakaba

SafeRoute:

innovación y flexibilidad en sistemas de evacuación

SafeRoute de dormakaba redefine la gestión de salidas de emergencia al integrar, de forma inteligente, múltiples requisitos en una misma puerta, incluso cuando son contradictorios. Responde a las necesidades de bomberos, policías, vigilantes, arquitectos y gestores de edificios.

Cumple con **EltVTR** y **EN 13637**, garantizando calidad y seguridad. Incorpora un anillo luminoso que indica el estado del sistema y facilita la detección de fallos. El restablecimiento de alarmas es sencillo gracias a su interruptor con llave, lo que mejora la operatividad y el mantenimiento.

El sistema se basa en licencias escalables (basic, standard y premium), que permiten pagar solo por las funciones necesarias y ampliarlas sin añadir hardware extra. Esta flexibilidad asegura una solución adaptable hoy y en el futuro.

El panel de control central SCMC permite supervisar y gestionar en tiempo real puertas individuales, grupos o zonas completas. Facilita el desbloqueo centralizado desde una sala de control, la vigilancia del estado de cada puerta (cerrada, desbloqueo temporal o permanente, o en alarma) y la gestión de retardos (T2) o denegaciones de salida, todo conforme a las normativas de seguridad. Su diseño modular se adapta a distintas instalaciones y cumple la **EN 13637** para una protección óptima.

Con altos niveles de seguridad, calidad y fiabilidad, **Safe Route** refuerza la protección y simplifica instalación y mantenimiento.

+información

DORLET consolida su liderazgo
en la protección de infraestructuras críticas

DORLET cierra el 2025 con un balance muy positivo, consolidando su posición en el mercado y demostrando que su visión estratégica, centrada en las necesidades reales de los clientes y en la innovación constante, es la clave para afrontar retos actuales y futuros.

Entre los hitos más relevantes de este año, destaca la obtención de la certificación de **Grado 4 en Intrusión (EN-50131)** que se une a la de **Grado 4 en Control de Accesos (EN-60839)** obtenida hace unos años; esto convierte a **DORLET** en el primer fabricante español en alcanzar este doble reconocimiento en el nivel más alto.

Otro de los logros más significativos de este 2025 ha sido ser el **único fabricante nacional** en incluir una solución de control de accesos cibersegura en el prestigioso **Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)** avalado por el **Centro Criptológico Nacional (CCN).** Estos reconocimientos no solo confirman el óptimo rendimiento de las soluciones en situaciones críticas, sino que también ofrecen a los clientes la máxima garantía de que las personas, los activos y las infraestructuras estarán protegidas frente a amenazas cada vez más sofisticadas.

Además, este año ha estado marcado por un intenso trabajo del departamento de **I+D** para desarrollar soluciones nuevas que aportarán un valor añadido al mercado. Estas novedades verán la luz a lo largo de 2026, reforzando la apuesta de **DORLET** por la excelencia tecnológica y la mejora continua.

VIDEOSISTEMAS FFV GEUTEBRÜCK

Sistemas de Grabación GEUTEBRÜCK G-CORE:

Tecnología alemana diseñada para evolucionar al ritmo del sector de la seguridad

En F.F. Videosistemas utilizamos los sistemas de grabación Geutebrück, tecnología alemana con más de 50 años de experiencia en el sector. Su arquitectura flexible y escalable permite adaptarse a las necesidades de cada instalación, desde pequeños entornos industriales hasta grandes corporaciones, garantizando siempre máxima eficiencia y continuidad operativa.

Estos sistemas destacan por su robustez y fiabilidad, incorporando hardware industrial, ciberseguridad avanzada mediante cifrado **AES-256** y estándares **FIPS**, junto con **sistemas RAID** para asegurar tolerancia a fallos y **FAILOVER** para garantizar disponibilidad continua.

A ello se suma un entorno completamente personalizable, donde cada usuario accede solo a las herramientas necesarias según su rol, optimizando la gestión y reforzando el control interno.

La plataforma ofrece una operativa ágil gracias a funciones como reproducción 1000x para revisar horas de vídeo en segundos, sincronización entre cámaras y exportaciones seguras en formato propietario.

Además, integra metadatos de analíticas basadas en IA y sistemas de terceros, como control de accesos o logística, permitiendo búsquedas forenses más rápidas y decisiones mejor fundamentadas.

Además, la nueva función **Canales DIF** unifica en un solo visor las mismas analíticas provenientes de diferentes cámaras, llevando la operatividad y la seguridad a un nuevo nivel. Con **G-SIM**, tanto el vídeo como los datos se gestionan desde una misma plataforma, facilitando la supervisión simultánea de múltiples instalaciones en distintas ubicaciones geográficas. Y permitiendo la gestión de más de 50.000 cámaras.

+información

Hanwha Vision

Cámaras bi-espectro para detección temprana de incendios

Hanwha Vision, presenta sus cámaras bi-espectro para detección temprana de incendios, combinando radiometría térmica e imagen visible.

Diseñadas para entornos críticos, estas cámaras ayudan a identificar posibles riesgos de incendio antes de que se agraven, garantizando la seguridad.

Los incendios pueden causar daños materiales, además de situaciones potencialmente peligrosas. Las cámaras utilizan análisis de video con Inteligencia Artificial para detectar llamas a través del canal visible, mientras que el sensor térmico controla cambios de temperatura. Esta detección en dos capas proporciona alertas críticas de llama y temperatura, permitiendo que los usuarios tomen medidas antes de que un incendio se propague.

Además de la detección de incendios, el control de temperatura permite un mantenimiento proactivo de los equipos: los usuarios pueden controlar valores mínimos, máximos y promedio de temperatura, configurando reglas de eventos precisas en dos regiones de interés. El rango va desde -10 °C a 450 °C.

Equipadas con un **detector térmico QVGA** (160×120) y lentes gran angular, 95° para el modelo **TNM-C2712TDR** y 57° para el **TNM-C2722TDR**, estas cámaras proporcionan cobertura óptima para monitorización de corto y medio alcance (de 7 a 15 metros).

Diseñadas para integrarse en sistemas de seguridad y de monitorización industrial, estas cámaras soportan el **protocolo MQTT**, permitiendo una comunicación eficiente con redes de automatización y control industrial.

Características clave:

- **Detección temprana de incendios con análisis de video e integración de sensores térmicos**
- **Integración SCADA mediante MQTT**
- **Compatibilidad con Milestone, Genetec, SSM y Wave**
- **Diseño compacto**

+información TNM-C2712TDR

+información TNM-C2722TDR

Lector biométrico de reconocimiento facial

HID® Amico™

HID Amico establece un nuevo estándar para el control de acceso con tecnología avanzada de reconocimiento facial, que combina velocidad, precisión y una experiencia fácil de usar.

Diseñado para proporcionar un acceso rápido y seguro en oficinas y áreas de alto tráfico, **HID Amico** es ideal para todo tipo de organizaciones que buscan un lector moderno y sin contacto que sea fácil de administrar y mejore la comodidad del usuario.

Con su diseño compacto y duradero y sus opciones de integración flexibles, **HID Amico** está diseñado para satisfacer las demandas de los entornos dinámicos de hoy en día.

Características principales:

- **Reconocimiento rápido y preciso:** Reconocimiento facial rápido y fácil.
- **Múltiples métodos de autenticación:** Admite 5 métodos de autenticación. Facial, Tarjetas (125Khz & 13,56Mhz), Mobile Access®, código QR y PIN.
- **Seguridad y privacidad:** Soporta el almacenamiento de los datos biométricos dentro de la tarjeta.
- **Integración perfecta:** Soporta protocolos Wiegand y OSDP.

+información HID® Amico™ ficha técnica

FAKE NETWORK SOCIETY:

REDES SOCIALES, IA GENERATIVA Y LA DISOLUCIÓN DE LA REALIDAD...

Virginia Espinosa

Profesora Titular del Depto. de Tecnología y Coordinadora del Grupo de Investigación FI4.0 del Tecnocampus (adscrito a la Universidad Pompeu y Fabra).

LAS REDES SOCIALES HAN REDEFINIDO NUESTRA FORMA DE COMUNICARNOS, INFORMARNOS Y RELACIONARNOS, DANDO LUGAR A UNA SOCIEDAD HIPERCONECTADA QUE EL SOCIÓLOGO MANUEL CASTELLS DENOMINÓ NETWORK SOCIETY. SIN EMBARGO, ESTA HIPERCONEXIÓN NO HA VENIDO EXENTA DE COSTES: PÉRDIDA DE PENSAMIENTO CRÍTICO, EROSIÓN DE LA INDIVIDUALIDAD, PROBLEMAS DE SALUD MENTAL Y UNA CRECIENTE DIFICULTAD PARA DISTINGUIR ENTRE LO RELEVANTE Y LO SUPERFLUO.

En este contexto ya complejo irrumpe con fuerza la inteligencia artificial generativa, una tecnología capaz de crear textos, música, imágenes y vídeos sintéticos con un grado de realismo sin precedentes. Su adopción masiva y acelerada plantea un nuevo escenario de riesgo: la posibilidad de que la desinformación, los deepfakes y las realidades fabricadas acaben configurando una auténtica **Fake Network Society**, donde la frontera entre verdad y ficción se diluya sin concesiones.

Las grandes transformaciones tecnológicas rara vez se anuncian como tales. Se instalan de forma progresiva en la vida cotidiana hasta que, cuando tomamos conciencia de su alcance, ya han redefinido nuestras formas de relación, percepción y pensamiento. Las redes sociales primero, y la inteligencia artificial generativa (IAG) después, constituyen dos vectores tecnológicos que, al converger, están alterando no solo la comunicación humana, sino también nuestra relación con la verdad, la realidad y la propia identidad.

Este artículo plantea una hipótesis inquietante y, a la vez, propone una reflexión crítica sobre la convergencia entre redes sociales e IA generativa. La combinación de ambas tecnologías puede estar empujándonos hacia una nueva forma de organización social que podríamos denominar —con cautela— **Fake Network Society: una sociedad hiperconectada** pero crecientemente desconectada de lo real, donde los contenidos sintéticos, las narrativas fabricadas y las identidades artificiales erosionan la frontera entre verdad y ficción. A partir de este diagnóstico, se analizan sus principales implicaciones sociales, éticas y de seguridad, y se esbozan algunas líneas de actuación orientadas a evitar una deriva distópica en la que la realidad y la verdad acaben siendo sustituidas, de forma gradual pero sistemática, por meros artefactos digitales.

Anatomía de una sociedad hiperconectada

Las redes sociales nacieron bajo la promesa de democratizar la información y la comunicación, amplificar la voz individual y conectar a las personas. Sin embargo, tras más de una década de uso masivo, el balance social revela efectos secundarios cada vez más difíciles de ignorar. El entretenimiento constante, personalizado y adictivo se ha convertido en el eje central de estas plataformas. Pero no se trata de un entretenimiento neutral. Está escrupulosamente diseñado para captar y retener la atención mediante mecanismos asistidos por la neurociencia que interpelan directamente a nuestras emociones más primarias: validación, miedo, indignación o deseo.

El precio de esta gratificación constante es elevado. Se observa una pérdida progresiva de capacidad analítica y de pensamiento crítico, junto con una mayor facilidad para la manipulación, la polarización y la radicalización. Los algoritmos no fomentan el contraste de ideas, sino la permanencia dentro de sistemas cerrados de pensamiento, auténticas burbujas cognitivas que refuerzan creencias preexistentes y penalizan la disidencia. En este contexto, la individualidad se diluye y la autenticidad se convierte en un riesgo.

Aldous Huxley anticipó un escenario similar en Un mundo feliz, donde el soma —un narcótico social— mantenía a la población anestesiada, dócil y acrítica. Salvando las distancias, las redes sociales funcionan hoy como un soma digital, no impuesto por un poder totalitario, sino consumido voluntariamente. La homogeneización de gustos, opiniones y estéticas conduce a una pérdida de singularidad; aquí resuena con fuerza la célebre frase con la que **León Tolstói** abre **Ana Karenina**: *"Todas las familias felices se parecen; cada familia infeliz lo es a su manera"*. En la sociedad red, parecerse se convierte en virtud; diferenciarse, en anomalía.

Impacto en la salud mental: una crisis silenciosa

Uno de los impactos más preocupantes de este ecosistema se manifiesta en la salud mental, especialmente durante la adolescencia, etapa crítica en la construcción de la identidad. El aumento de ansiedad y depresión es ampliamente documentado, al igual que la aparición de nuevas patologías asociadas a la autoimagen. El fenómeno conocido como **Snapchat Dysmorphia** ilustra con crudeza esta deriva: jóvenes que desean parecerse a versiones filtradas y digitalmente perfeccionadas de sí mismos, hasta el punto de recurrir a cirugías estéticas para alcanzar un ideal artificial e inalcanzable. A ello se suma un incremento alarmante de conductas autolesivas y suicidios en adolescentes, lo que ha llevado a considerar este fenómeno como un problema emergente de salud pública a escala global.

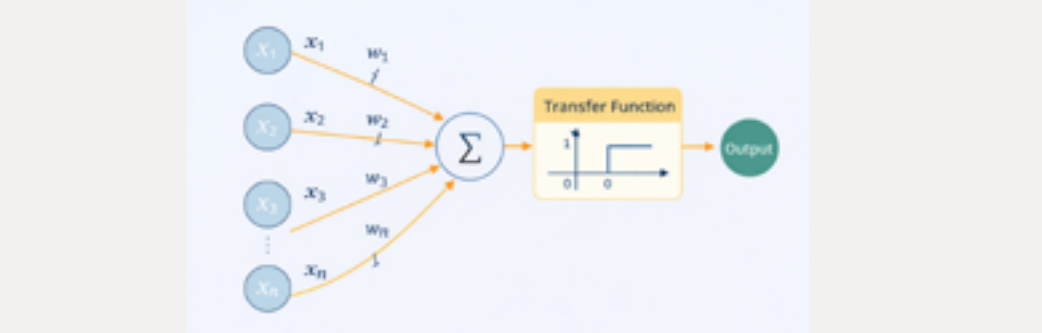
Paradójicamente, la hiperconectividad no ha traído consigo una mayor sociabilidad real. Emergemos como individuos superconectados pero aislados, con dificultades crecientes para relacionarnos cara a cara o incluso para mantener una conversación telefónica bidireccional. Diversos estudios sitúan en torno al 70% el porcentaje de adolescentes que manifiestan ansiedad o rechazo a realizar llamadas telefónicas. Nunca habíamos dispuesto de tantas herramientas de comunicación y, sin embargo, nunca había sido tan difícil comunicarse.

A este escenario se añade la pérdida de capacidad de atención y concentración provocada por la multitarea constante y la fragmentación cognitiva derivada de notificaciones y estímulos simultáneos. El pensamiento profundo, reflexivo y crítico se ve desplazado por una atención dispersa, reactiva y superficial.

En este contexto, las redes sociales actúan como plataformas sofisticadas que explotan la vulnerabilidad humana, con el propósito último de captar nuestra atención y nuestro tiempo para fomentar el consumo acrítico y compulsivo o, en no pocos casos, alterar y manipular nuestra voluntad y capacidad de decisión.

Todo ello ha cristalizado en lo que el sociólogo **Manuel Castells** denominó **Network Society**: *una sociedad organizada en redes digitales donde la información, el poder y la identidad fluyen a través de nodos interconectados*. En este modelo, estar conectado equivale a existir; quedar fuera de la red implica una nueva forma de exclusión social.

En este contexto ya complejo irrumpe la inteligencia artificial generativa entendida como un modelo avanzado de Inteligencia Artificial; una tecnología que presenta un largo recorrido a sus espaldas, pasando del **perceptrón de Rosenblatt** hasta las redes neuronales convolucionales, el **machine learning** y el **deep learning**. Su evolución hacia el estadio de la actual IAG, con aparición de las arquitecturas transformer y de los modelos **Large Language Models (LLM)**, ha estado impulsada por tres factores clave: mayor capacidad de computacion, eficienciación de algoritmos de aprendizaje y acceso a volúmenes masivos de datos.



A diferencia de **IA subyacente**, la **IA Generativa** no se limita a analizar y procesar información y/o automatizar procesos. Su rasgo distintivo es la capacidad de generar contenido nuevo: textos, imágenes, música y vídeos originales. Esta capacidad creativa constituye, al mismo tiempo, su mayor promesa y su mayor riesgo. Por primera vez, una tecnología permite sintetizar realidad a gran escala y a una velocidad sin precedentes, experimentando un punto de inflexión con el desarrollo del modelo **ChatGPT** y su irrupción pública en noviembre de 2022, catapultándola como la tecnología de más rápida adopción de la historia de la humanidad.

Esta disrupción supondrá —si no ha supuesto ya— una nueva revolución en el sentido amplio del término: la aparición de un vector tecnológico capaz de alterar el orden social establecido, como en su momento lo fueron la escritura, la agricultura, o la máquina de vapor que impulsó la revolución industrial. En marzo de 2023, **Bill Gates** lo sintetizaba con claridad: ***"The Age of AI has begun"***.

Una de las cuestiones más inquietantes que suscita la **IA generativa** es precisamente su extraordinaria capacidad para crear textos que nadie ha escrito, imágenes que no existen, personas sintetizadas y vídeos que no son reales. Los llamados *deepfakes* representan una amenaza directa a la confianza social y al ecosistema informativo. Como señalan **Vaccari** y **Chadwick**, estos contenidos sintéticos no solo engañan, sino que generan incertidumbre y erosionan la confianza incluso cuando el contenido es auténtico.

Ejemplos recientes ilustran esta deriva: la "reencarnación" digital de la princesa Leia en la saga *Star Wars*, o el anuncio de Cruzcampo en el que Lola Flores "resucita" mediante técnicas de IA generativa. A ellos se suman, caras de personas que no existen, discursos políticos falsificados o la posibilidad, ya real, de "resucitar" digitalmente a personas fallecidas.

Esta revolución tecnológica, liderada por la **IAG** y asistida por internet y las redes sociales, puede fácilmente degenerar en escenarios distópicos que cristalicen en una Fake Network Society, donde ya no sepamos si lo que estamos viendo —que no viviendo— es realidad o ficción. Una auténtica Matrix 2.0.

José Saramago lo expresó con inquietante lucidez: *«El mundo se está convirtiendo en una caverna igual a la de Platón: todos mirando imágenes y creyendo que son la realidad»*. **George Orwell** fue aún más contundente: *«El propio concepto de verdad objetiva está desapareciendo. Las mentiras pasarán a la historia»*. En este contexto, resulta inevitable afirmar que la IA generativa no ha venido solo para quedarse; ha venido para cambiarlo todo.

Llegados a este punto, la reflexión final se impone. **Markus Gabriel** advierte que nuestra sociedad científica y ultramoderna ha producido sistemas que bloquean el progreso moral, al erosionar la confianza en la verdad, el conocimiento, la realidad y nuestra propia conciencia. *Fake news*, vigilancia digital, propaganda y desinformación conforman un ecosistema que exige situar de nuevo al ser humano —como ser libre y reflexivo— en el centro de la reflexión ética.

Corregir la deriva distópica descrita no admite soluciones simples, pero sí algunas líneas de actuación ineludibles: reconsiderar el principio de precaución frente al despliegue acrítico de tecnologías disruptivas; reflexionar sobre la soberanía tecnológica, especialmente en el contexto europeo; avanzar en una regulación de la IA que no sea meramente reactiva; y promover buenas prácticas en el uso de los smartphones, especialmente en la infancia y la adolescencia.

En este sentido, resulta revelador observar cómo en algunos países nórdicos los padres están optando por sustituir los smartphones por teléfonos sin acceso a internet. No se trata de una moda, sino de un acto de cuidado emocional: reducir la sobreestimulación digital para devolver espacio al aburrimiento, la creatividad, la presencia y la experiencia humana directa. A veces, avanzar significa volver a lo esencial.

La **Fake Network Society** no es un destino inevitable, pero sí una posibilidad real. Desde la perspectiva de la ingeniería de la seguridad, entendida en su sentido más amplio, el desafío ya no consiste únicamente en proteger sistemas, infraestructuras o datos, sino en salvaguardar algo más frágil y fundamental: la confianza, la verdad y la capacidad humana de discernir la realidad.

La pregunta clave ya no es qué puede hacer la tecnología, sino qué debemos permitirle hacer...

FAKE NEWS

Un último apunte...

DISMORPHIA SNAPCHAT

https://www.independent.co.uk/life-style/plastic-surgery-cosmetic-snapchat-teenagers-millennials-dysmorphia-bdd-a8474881.html

IMÁGENES DE CARAS SINTETIZADAS

https://www.noticias3d.com/noticia/72669/nvidia-aplica-inteligencia-artificial-generacion-imagenes-fotorrealistas.html

¿Puedes distinguir entre un rostro real y uno hecho por IA?

Prueba este test - The New York Times

CONOCE A UN

SOCIO

José María Prades Arilla

SOCIO Nº 207

Buenos días José María. Eres un histórico del sector, pero habrá socios que no te conozcan. ¿puedes decirnos algunas palabras sobre ti como presentación?

Toda mi actividad laboral se ha llevado a cabo en lo que ahora se denomina, "emprendedor". En todo momento, traté y lo sigo haciendo, introducir innovaciones y mejoras en los procedimientos y tecnología que se venían utilizando en mí campo de actuación.

¿Cuál es tu formación académica?

Ingeniero Industrial. Ingeniero Técnico Industrial.

Veo que sigues interesado en aumentar tu formación. Me llama la atención el doctorado que está siguiendo ahora. ¿Cómo se combinan las tecnologías de la computación y la ingeniería ambiental?

Si no se cultiva el conocimiento, éste te abandona. Además, hay que alimentarlo con nuevos conocimientos a la vez que se fundamentan los ya recibidos, en este sentido, un "paseo" por las matemáticas y la física suele ser muy interesante. Por otra parte, la seguridad forma parte del "ambiente social".

¿En qué año y en qué sector comenzó tu andadura laboral?

En el año 1973 en el sector de electromedicina.

¿En qué empresas has trabajado desde entonces, en qué puestos y cuál era tu actividad en ellas?

Empecé trabajando como subcontratista para empresas de electromedicina en el ámbito de los equipamientos técnicos para laboratorio de análisis y cardiología (marcapasos). Proseguí en el campo del sonido con la sociedad ELYSON. A mediados del año 1975 tuve conocimiento de la legislación que se había promulgado en materia de seguridad bancaria y otros establecimientos obligados a contar con medidas de seguridad. Tal contacto se inició con la petición de fabricación de centralitas de alarmas lo que hicimos con notable éxito. A partir de ese momento, no me separé del sector de la seguridad desde la sociedad NUTRÓNICA y FILIALES.

Empezaste pisando fuerte, siendo fundador de una empresa ¿qué destacarías de los proyectos desarrollados en Nutrónica?.

Destacaría el desarrollo de la detección de metales en espacios públicos, por ejemplo, para las entidades bancarias, donde desarrollamos nuevos equipos de detección dentro de una labor de investigación en el campo de electromagnetismo.

De tu etapa como profesional independiente ¿Qué actividad era la que más te satisfacía y de cual aprendiste más?

Aquí, hay dos preguntas en una. Donde aprendí más fue en los conceptos necesarios e imprescindibles para la dirección de empresas. La actividad, más positiva consistió en los desarrollos antes indicados, por su elevado contenido técnico y, por qué no decirlo científico.

Actualmente, en tu misión de investigación y análisis de las instalaciones de seguridad ¿Qué aspectos positivos y qué carencias detectas en ellas?

Estimo que no se está viviendo un buen momento profesional respecto a los servicios que prestan las empresas de seguridad, en particular, las de sistemas. En efecto, el feroz escenario comercial y la falta de cultura de seguridad, ha conducido a las empresas de este sector, a "vender a cualquier precio", sin reparar ni analizar los riesgos a cubrir y, por tanto, hacer propuestas razonables de los sistemas de alarma en cuestión.

Por otra parte, el entramado burocrático/administrativo, no dudo en calificarlo de insoportable y totalmente fuera de contexto frente a los riesgos que realmente existen y propician los delitos.

Desde tu actividad formativa por una parte y el contacto con las instalaciones por otra ¿cómo ves la ingeniería de diseño y la calidad de los proyectos de las instalaciones?

No existe Ingeniería de diseño, dominando el escenario los aspectos comerciales. A ello, contribuye la habitual nula formación en los clientes, incluidos aquellos que poseen departamento de seguridad propio.

¿Tienes alguna sugerencia para potenciar la figura del ingeniero en las empresas de proyectos e instalaciones?

No tengo ninguna nueva sugerencia salvo incidir en que la seguridad debe ser un objetivo de la más alta dirección de las empresas... y lamentablemente, no es así. No es menos cierto que, salvo alguna selecta minoría, las asociaciones de empresas de seguridad contribuyen muy poco a dignificar la profesión de Ingeniero de Seguridad, lo cual, por cierto, no ocurre en otros países de la UE, donde son las asociaciones (de tipo gremial) quienes validan y supervisan el bien hacer de sus asociados, eliminando aquellos que no mantiene el debido rigor profesional y ético.

¿Cómo conociste AEINSE y qué te llevó a asociarte?

A través de algunos miembros que me animaron a asociarme, entre ellos, mí estimado Alfonso Bilbao.

Espero que tu trabajo diario de deje tiempo para cultivar tus aficiones personales ¿Qué te gusta hacer en tu tiempo libre?

Algo de tenis (juego bastante mal) y en verano, montaña. (Pirineos de Huesca).

Y, como siempre, terminamos pidiéndo alguna sugerencia para la mejora de la Asociación.

Parecerá un tópico, pero sería muy interesante publicitar al máximo la existencia de AEINSE y su manual de buenas prácticas de sus asociados en materia de seguridad. A su vez, sería interesante instar a la Administración (Ministerio del Interior) a que termine de una vez aquello que tenga que legislar, pero siempre, dejando actuar a los especialistas sin invadir terrenos técnicos que sólo a ellos compete. Combatir la gran burocracia existente sería un buen propósito. Potenciar la comunicación sería muy útil... pero es caro.

Una consideración final a modo de recomendación, a los técnicos y empresas de seguridad:

Dudad siempre de vuestras conclusiones y decisiones técnicas en materia de seguridad, replanteando continuamente los diseños y propuestas que vengáis realizando.

No cedáis a la improvisación y a soluciones técnicas poco estudiadas, a veces, por razones económicas... ¡el tiempo os lo cobrará!

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Evento Huella 2025: 45 aniversario de Seguritecnia

El evento Huella de este año, organizado por **Seguritecnia** y celebrado el pasado 19 de Noviembre, fue un acontecimiento compartido por más de 300 asistentes, entre ellos varios representantes de seguridad de la Administración, en el que se celebraron los **45 años de la Revista Seguritecnia.** Desde que **Ramón Borredá** fundara la revista en 1980 se han publicado 500 números y más de 50.000 páginas que han recogido la evolución de nuestro sector.

Durante estos años desde **Seguritecnia** se ha creado la **fundación Borradá** y se han incorporado otras publicaciones como **Red Seguridad**, siendo un referente en el sector de la seguridad, tanto por las publicaciones como por los actos, jornadas, eventos, premios instituidos, etc,. Es importante destacar que se trata de una empresa siempre controlada y dirigida por la **familia Borredá**, manteniendo su independencia editorial y objetividad.

Dentro del evento se celebró también la **38ª edición de los Trofeos Internacionales de la Seguridad, donde Seguritecnia y la Fundación Borredá distinguieron a los profesionales y entidades que han contribuido de forma destacada a la protección de personas, bienes y espacios en España.**

Es de destacar también el momento en el que Ana Borredá cedió el testigo de la dirección de la **revista Seguritecnia** a **Javier Borredá**, que reconoció la importancia del relevo generacional: "«Mi abuelo dejó un legado que hoy seguimos transmitiendo. Aquí están mi padre y mi tía, y todos tenemos mucho que agradecerles. Y detrás venís otros: hijos de **Ana** y **Antonio**, algunos ya como becarios, que dentro de unos años tomarán el testigo».

+información Huella 25

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

II CONGRESO MUJER Y SEGURIDAD

El Observatorio Mujer y Seguridad (OMyS) organizó, con la colaboración de Seguritecnia y el Banco de Santander, el pasado 6 de noviembre, el II Congreso Mujer y Seguridad.

Bajo el lema **"Presente y futuro de la mujer en seguridad; con otra mirada"** y con la participación de más de 300 asistentes, se trataron diversos temas, entre otros, como el incremento de la participación de la mujer en el sector, facilitando cifras, tanto del sector público como del privado; la necesidad de protocolos y políticas que integren la perspectiva del género en la seguridad y la importancia de la formación para incrementar su presencia en el sector.

Representantes de **AEINSE** estuvimos en entre el auditorio y pudimos constatar la falta de datos sobre la presencia de la mujer entre el colectivo de Ingenieros y técnicos en las empresas de consultoría, proyectos e instalaciones. Al no estar considerado este colectivo como personal de seguridad en la actual legislación, no hay datos oficiales y, la colaboración de las empresas en facilitar estos datos no ha sido suficiente para generar datos estadísticos.

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

7ª Conferencia sectorial de Seguridad en Puertos

NOV
04

El pasado 4 de noviembre tuvo lugar en el auditorio de la CECA en Madrid la 7ª Conferencia Sectorial de Seguridad en Puertos. Con la asistencia de más de 200 profesionales, se analizaron los desafíos que enfrenta este sector en materia de seguridad que, como dijo el presidente de Puertos del Estado, Gustavo Santana Hernández, en el acto de inauguración, "ha adquirido mucha relevancia porque estamos hablando de infraestructuras estratégicas"

En la conferencia, concebida como espacio de convivencia y conocimiento, los ponentes trataron aspectos de la seguridad relacionados con:

- La evolución normativa en protección portuaria
- La Seguridad híbrida en Puertos
- La Vigilancia y seguridad portuaria
- Casos reales: foco en la planificación
- Nuevas tecnologías al servicio de la seguridad
- Los retos de la seguridad en puertos

.

+información

Más información y acceso al video del evento

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Publicada la Estrategia Nacional contra el crimen Organizado y la Delincuencia Grave

Con la coordinación de Ministerio del interior a través del Centro de Inteligencia contra el terrorismo y el Crimen Organizado (CITCO), y la participación de diversos ministerios y organismos nacionales y autonómicos, así como de expertos independientes, se ha redactado y publicado la Estrategia Nacional Contra el Crimen Organizado y la Delincuencia Grave.

Un documento que, como manifiesta en su capítulo 4, tiene como objetivo *"Neutralizar la amenaza que representa la criminalidad organizada y la delincuencia grave sobre la seguridad y bienestar de la ciudadanía, sus intereses y los del conjunto de España, así como minimizar las consecuencias negativas asociadas a ambas figuras en sus diferentes manifestaciones, proteger a las víctimas y a los colectivos vulnerables, y contrarrestar la interacción creciente con otras amenazas para la seguridad nacional e internacional".*

Por otra parte, en su resumen ejecutivo, describe brevemente la situación en España que se desgrana a lo largo del documento: *"El escenario geopolítico, social y económico global, y las características propias y diferenciales de España en dicho contexto afectan de forma relevante a la evolución de la delincuencia organizada y grave en nuestro país.*

Las amenazas y vulnerabilidades en este ámbito son múltiples, siendo el tráfico de drogas, la corrupción, el incremento de la violencia y de la sensación de inseguridad ciudadana, junto con la influencia del terrorismo, la actividad de las redes criminales de inmigración irregular o el impacto sobre colectivos vulnerables, algunas de sus principales manifestaciones".

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Iván Rubio, en un momento del acto de apertura del Congreso.

VII Congreso de Seguridad Privada en Euskadi

El pasado 29 de octubre tuvo lugar en el Bizkaia Aretoa de Bilbao el VII Congreso de Seguridad Privada en Euskadi. Organizado por Cuadernos de Seguridad con la colaboración del Gobierno Vasco, la Ertzaintza y SAE (Asociación Vasca de Profesionales de Seguridad) contó con la asistencia de más de 200 profesionales.

Durante la jornada se realizar ponencias y debates sobre diversos aspectos de la seguridad. Entre otros, se trató sobre Infraestructuras críticas en Euskadi, análisis del plan de Protección de las infraestructuras sensibles de Euskadi (PISE); Captación del Talento en Seguridad, destacando las necesidades de Dignificar el sector, reforzar y potenciar la formación, adaptar los contenidos curriculares a la necesidad de los competencias actuales en el campo de la tecnología.; La Directiva Europea RED que afecta a los dispositivos inalámbricos y se debatión sobre las figuras del CISO y el director de seguridad con la visión de la aplicación de la NIS 2.

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

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

II Jornada Dora

ENE
21

El próximo 21 de enero, tendrá lugar en el **auditorio Cecabank** de Madrid la **II Jornada DORA** con el lema **"Evolución, balance y perspectivas de un marco en transformación. Un año después: del ámbito legal al impacto real".**

Organizada por **Red Seguridad** y la **Fundación Borredá**, la cita será un foro de balance, evolución y perspectivas sobre la implantación del Reglamento. Todo ello a través de mesas redondas con reguladores, CISOs y representantes de la Administración.

Información e inscripción

SEGURITECNIA


Centrales receptoras de alarmas en España:
evolución, normativa y perspectivas

Centrales receptoras de alarmas en España

evolución, normativa y perspectivas

Articulo de nuestro socio **Pedro Pablo Cavero Roza**
en la **Revista Seguritecnia** número **515. Página 76**

"En la primera década de los años 2000, se llegaron a contabilizar más de 250 CRA, un récord histórico que refleja la expansión inicial del sector. Sin embargo, esa tendencia no se ha mantenido en el tiempo; desde mediados de la década de 2010, el número de CRA ha experimentado un retroceso constante.

A finales de 2024, se sitúa en torno a 120 CRA habilitadas, perdiendo cerca de un 25% en un lustro".

+información

LEÍDO, VISTO Y OÍDO EN...

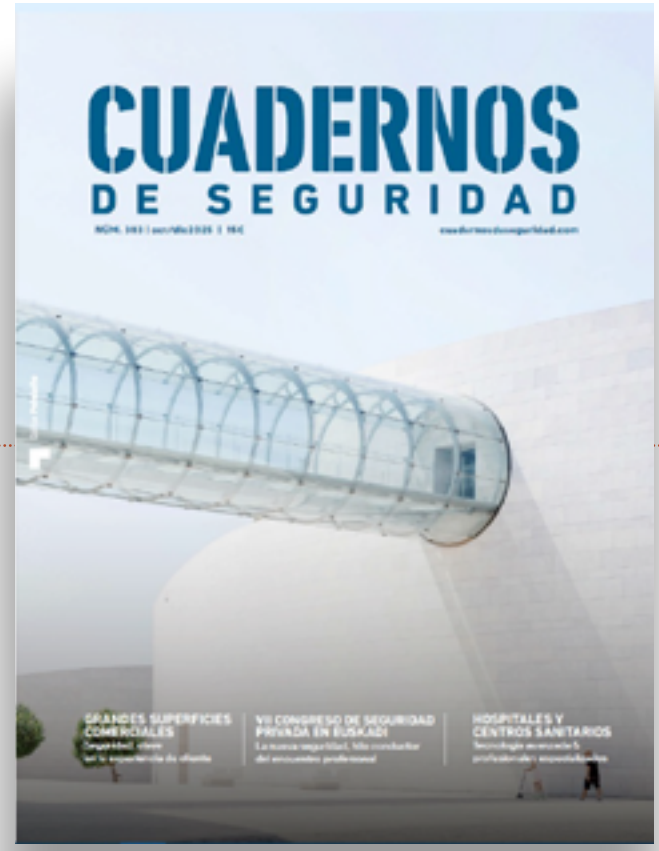
Boletín informativo de la Fundación AES

En el número 5 – octubre 2025- leemos en la página 10 un interesante artículo sobre la **Banalización de la seguridad de las comunicaciones.**

"La ubicuidad de internet y la omnipresencia de las redes sociales han generado un entorno en el que compartir información se percibe como algo natural e inmediato. Publicar datos personales, imágenes o ubicaciones en tiempo real se ha convertido en una práctica común, pero pocas veces se reflexiona sobre el impacto que puede tener..."

artículo completo

LEÍDO, VISTO Y OÍDO EN...



La EDGE AI y la implementación de la AI ACT en Europa

Breve pero interesante artículo sobre la **EDGE AI** y la **implementación de la AI ACT** en Europa:

"La Inteligencia Artificial al Borde (Edge AI) representa una de las transformaciones más importantes en la evolución tecnológica actual. Frente al modelo tradicional basado en grandes centros de datos, Edge, traslada el procesamiento a... "

Cuadernos de Seguridad 383 - pág 50

Informe Victimas de incendios en España 2024 publicado por la fundación Mapfre

"...entre el 1 de enero y el 31 de diciembre, se registraron 234 muertos en total, 172 de ellos en vivienda, cifras que lo convierten en el tercer peor periodo anual desde la primera edición de este informe (2010)".

Interesante informe estadístico considerando el dónde, cuándo y por qué se producen los incendios y explosiones. Su misión es concienciar con los datos, que nuestra sociedad tiene el conocimiento y la formación suficiente para reducir progresivamente el número de muertes por incendio y explosión.

+información

¿Qué trabajos sobrevivirán a la inteligencia artificial y cuáles morirán?

Interesante podcast de **Red seguridad** que razona porqué algunos trabajos están más expuestos que otros a ser realizados a través de la Inteligencia Artificial. También aconseja en cómo prepararse para trabajar con ella y no contra ella. El futuro laboral no será de las máquinas ni exclusivamente humano. Será compartido.

Tras una introducción y un pequeño juego, el comentario comienza en el minuto 7 y 52 segundos.

acesso al podcast

LEÍDO, VISTO Y OÍDO EN...

Qué es el 'interés legítimo' de las cookies y por qué se queda la opción activada cuando las configuramos

Probablemente, ante la pregunta al acceder a una página web sobre la aceptación de cookies y la presentación de una larga lista de opciones, nos hemos preguntado dónde empieza el "interés legítimo" de las empresas y dónde el nuestro. Esta página de Maldita pone luz sobre el tema

artículo completo

Naciones Unidas | Noticias ONU
Mirada global Historias humanas

Noticias ONU

En la edición del **25 de septiembre 2025** leemos:

"O gobernamos la inteligencia artificial o ella nos gobernará a nosotros". Esta advertencia del Secretario General de la ONU, **António Guterres**, resonó este miércoles en la Asamblea General durante el lanzamiento del Diálogo Global sobre Gobernanza de la IA, donde España alertó que esta tecnología podría crear *"un futuro de ganadores y perdedores" si no se establecen mecanismos de control global".*

Una llamada de atención para que la IA no se convierta en una pesadilla.

Este artículo está acompañado de otros de gran interés relacionados con él y que se pueden leer en:

Leer el artículo completo: aquí