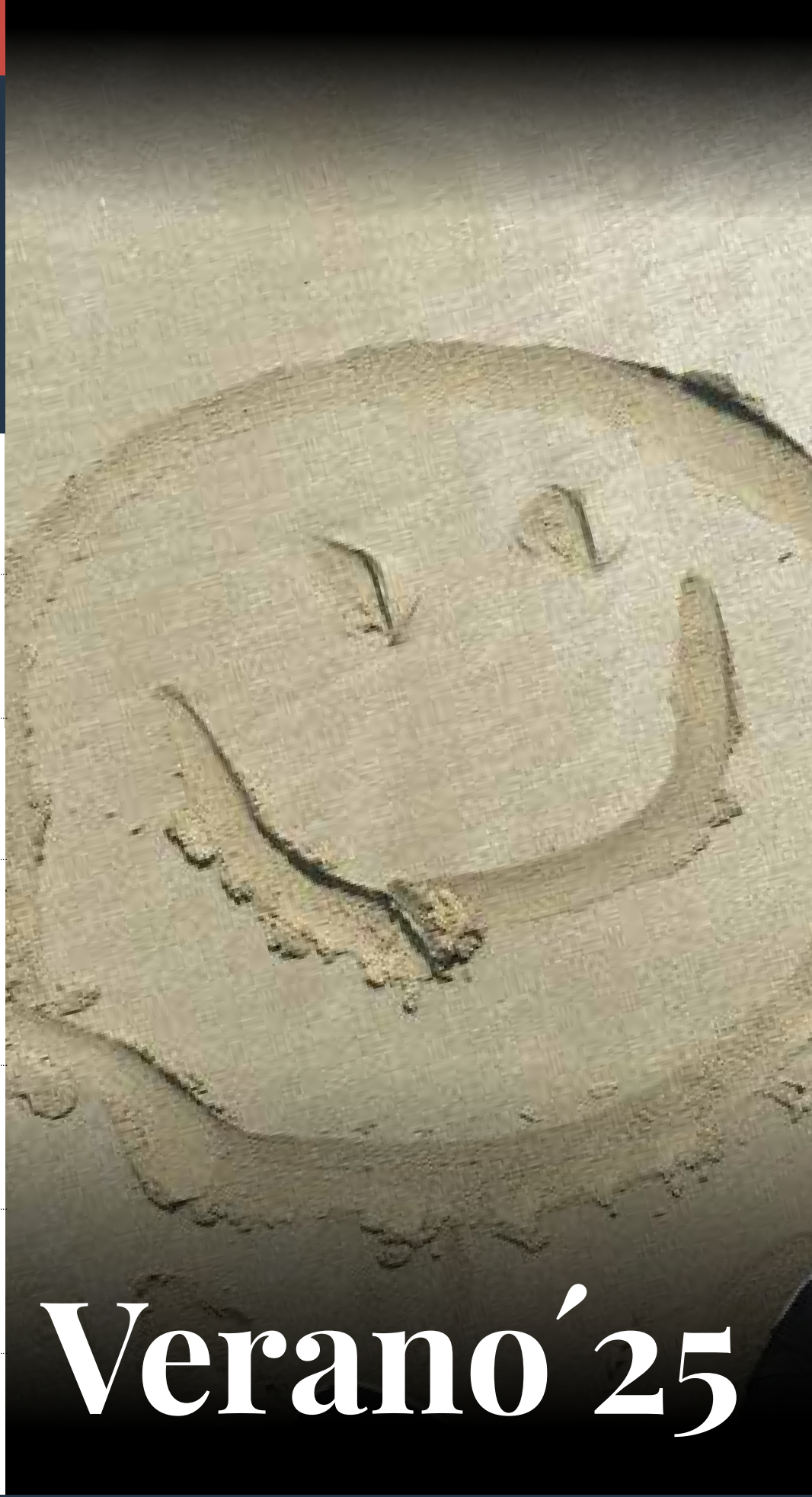
BOLETÍN Nº62 JUL 2025

AEINSE

Asociación Española de Ingenieros de Seguridad



Verano´25

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

Verano´25

¡ya está aquí!

Llegado el mes de junio, desde la Junta Directiva de AEINSE queremos aprovechar este boletín para desear a todos nuestros asociados, colaboradores y amigos un merecido descanso estival. Para quienes tengan la oportunidad de disfrutar de unas vacaciones, les animamos a desconectar, recargar energías y disfrutar de un verano tranquilo y seguro en compañía de los suyos. Y para quienes durante estos meses sigan con sus actividades profesionales, les enviamos también un cordial saludo y nuestro reconocimiento por su dedicación continua.

En este año 2025, y como ya os hemos ido anunciando, una de las citas más esperadas tras el periodo vacacional será la celebración de nuestro Congreso de Ingeniería de Seguridad, que tendrá lugar en otoño y que promete ser un punto de encuentro fundamental para todos los profesionales del sector.

Este congreso no sería posible sin el esfuerzo, compromiso y colaboración de varios de nuestros patronos, a quienes agradecemos de manera especial su implicación para hacer realidad esta importante iniciativa. Estamos convencidos de que será una oportunidad excelente para compartir conocimiento, debatir sobre las últimas tendencias tecnológicas y regulatorias y seguir impulsando la excelencia en el ámbito de la ingeniería de seguridad.

Por otro lado, hemos querido estar presente en los procesos de consulta pública que afectan de manera directa a nuestro sector.

Por ello, hemos presentado nuestras aportaciones al Ministerio en relación con el anteproyecto de la nueva Ley de Ciberseguridad y Resiliencia (CER).

Consideramos fundamental que la voz de los profesionales de la ingeniería de seguridad sea escuchada en el desarrollo normativo, especialmente en aspectos clave como la integración de requisitos técnicos, la protección de infraestructuras críticas y la mejora de los mecanismos de prevención y respuesta ante incidentes de ciberseguridad.

Esperamos que nuestras observaciones sean tenidas en cuenta y contribuyan a una ley más robusta, realista y alineada con las necesidades reales del sector.

Desde AEINSE queremos agradecer la confianza de todos nuestros socios y colaboradores, y reiterar nuestro compromiso con la representación activa del sector ante las administraciones, así como con la promoción de la innovación, la formación continua y la mejora de las buenas prácticas en ingeniería de seguridad.

¡Feliz verano para todos
y nos vemos en el Congrso
tras las vacaciones!

ANTEPROYECTO DE LEY
DE TRASPOSICIÓN DE LA DIRECTIVA CER

Entre el 30 de mayo y el 10 de junio pasados se abrió la audiencia pública sobre el Anteproyecto de la Ley de Protección y Resiliencia de las Entidades Críticas que se redacta en cumplimiento de la obligación de trasponer la Directiva Europea de Resiliencia sobre Entidades Críticas, conocida como Directiva CER.

Desde Aeinse se solicitó a sus miembros la creación de un Grupo de trabajo específico para estudiar dicho Anteproyecto y debatir sobre la conveniencia de presentar las alegaciones correspondientes, en su caso, en lo que afecte el Anteproyecto a nuestro desempeño como ingenieros.

Este Grupo de Trabajo decidió presentar dos alegaciones en concreto, relacionadas con las **Disposiciones Adicionales 7ª y 8ª**.

Son las siguientes:

Disposición adicional 7ª
Quizá debiera ser más explícita en lo que se refiere al uso permitido de control de accesos con identificación biométrica. Se sugiere que en el párrafo "las entidades críticas establecerán sistemas de reconocimiento biométrico de identificación o autenticación en todas o algunas de sus instalaciones con objeto de garantizar el control de accesos" se sustituya el verbo "establecerán" por "podrán establecer" y también se insta al Ministerio del Interior para que, cuanto antes, regule con una norma de rango menor las características técnicas que permitan instalar este tipo de sistemas.

>>

ANTEPROYECTO DE LEY DE TRASPOSICIÓN DE LA DIRECTIVA CER

Disposición adicional 8ª
Como en el caso anterior también sería importante ser más precisa la redacción en cuanto al uso de medidas antidrones. También se sugiere que en el párrafo "las entidades críticas establecerán sistemas antidrones de detección en todas o algunas de sus instalaciones con objeto de garantizar su protección" se sustituya el verbo "establecerán" por "podrán establecer" y también se insta al Ministerio del Interior para que, cuanto antes, regule con una norma de rango menor las características técnicas que permitan instalar este tipo de sistemas.

Por otra parte, el Grupo de Trabajo alcanzó unas conclusiones sobre el significado de este Anteproyecto de Ley y su repercusión en el sector de la Seguridad que a continuación se refiere:

"Este Anteproyecto de Ley, pese a lo que se indica en la Directiva CER que intenta trasponer, se ha escrito con un enfoque muy disjunto a la Ley que traspone la Directiva NIS 2 (Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad). Parece lógico pensar que la Resiliencia de una empresa implica la protección ante todo tipo de riesgos, pero los de amenazas informáticas se recogen en la Ley correspondiente a la Directiva NIS 2 y en la presente Ley (en adelante Ley CER) se excluyen. Obviamente hay amenazas mixtas, física y de ciberseguridad que han de tratarse con arreglo a dos legislaciones diferentes.

Esto genera especialmente problemas a la multitud de empresas que han de cumplir con ambas leyes (todas las Entidades Críticas), generando dos organismos con los que relacionarse CNPREC (antiguo CNPIC) y Centro Nacional de Ciberseguridad.

El conjunto de las dos Leyes deja especialmente complicado el cumplimiento de lo legislado sobre los Sistemas de Seguridad de Entidades Críticas (CER), pues son todas a su vez Entidades Esenciales (NIS2). Estos Sistemas, regulados por la "Ley CER" deben ser protegidos ante ataques de Ciberseguridad según la "Ley NIS2", y viceversa, los ataques físicos a las infraestructuras Informáticas están regulados por la Ley NIS 2 pero han de atenerse a lo regulado de medidas Seguridad Física en la Ley CER.

Entre los no muy numerosos rasgos de coherencia entre ambas leyes se encuentran:

- La inclusión, en ambos casos, de las empresas de Seguridad Privada que prestan servicios a Entidades Críticas o a Entidades Esenciales como a su vez pertenecientes a ambas categorías (ver en los Anexos de ambas Leyes).

- La inclusión de los técnicos de ciberseguridad en la categoría de profesionales susceptibles de ser acreditados, retocando al respecto lo previsto en el artículo 2 apartado 9 de la Ley 5/2014 de Seguridad Privada (pendiente de desarrollar mediante el inexistente Reglamento), según se indica en la Disposición Final 2ª de la Ley NIS 2.

Es muy destacable que la previsible aprobación de estos dos Anteproyectos de Ley deja fuera de vigencia la Ley PIC, y su Reglamento queda obsoleto.

Por otra parte, la Ley de Seguridad Privada 5/2014 también agudiza su obsolescencia, además de precisar más que nunca un Reglamento que la desarrolle.

ACCESO SIN FISURAS

Las credenciales LEGIC para móviles ahora en Google Wallet

LEGIC

Estamos encantados de informar que 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

Sicuralia anuncia el lanzamiento de

HxGN dC3 de Hexagon

Hexagon, tras la adquisición de Qognify, ha comenzado a integrar sus soluciones bajo la marca HxGN, incorporando tecnología LiDAR 3D para reforzar su oferta en seguridad física. Esta fusión estratégica permite a la compañía ampliar sus capacidades con herramientas innovadoras para la protección de infraestructuras críticas.

Sicuralia anuncia la disponibilidad de **HxGN dC3 Video**, la nueva plataforma unificada de seguridad física de **Hexagon**. Esta solución evoluciona la reconocida **Qognify QVMS**, mejorando la gestión de incidentes con un enfoque integral y en tiempo real.

Uno de los componentes más destacados es **HxGN dC3 LidarVision**, que utiliza **tecnología LiDAR** para ofrecer supervisión 3D avanzada. Esta herramienta permite la detección volumétrica y visualización tridimensional de amenazas, disminuyendo las falsas alarmas y protegiendo áreas completas, no solo perímetros.

Además, la plataforma incluye **HxGN dC3 Orchestrator**, un sistema de gestión de información de seguridad física (PSIM) que optimiza la conciencia situacional y la respuesta ante incidentes.

Con más de 30 años de experiencia, **HxGN dC3** promete mejorar la eficiencia operativa, la capacidad de respuesta y el cumplimiento normativo en entornos empresariales, consolidándose como una solución robusta y completa en seguridad inteligente.

Contacta hoy mismo con **Sicuralia** para obtener más información y descubrir cómo **HxGN dC3** puede transformar tu estrategia de protección perimetral.

+información VIDEO

+información LIDARVISION

+información ORCHESTRATOR

SCATI

ATENCIÓN REMOTA, INMEDIATA Y PROFESIONAL DESDE CUALQUIER LUGAR

SCATI Remote Assistant: Funcionamiento simple, apoyo inmediato

SCATI REMOTE ASSISTANT

atención remota profesional e inmediata desde cualquier lugar

SCATI REMOTE ASSISTANT es una innovadora solución de atención remota que transforma la experiencia del usuario en ubicaciones desatendidas. A través de un tótem interactivo y robusto, los usuarios pueden contactar directamente con un operador mediante videollamada, con solo pulsar un botón.

La solución está integrada en la plataforma **SCATI SENTRY**, desde la cual el operador visualiza al usuario, consulta planos, accede a cámaras del entorno y activas funciones asociadas a la atención o seguridad, todo desde una única interfaz.

El tótem incorpora cámara, audio bidireccional, pantalla táctil y diseño antivandálico, lo que lo hace ideal para espacios públicos o críticos. Además, cuando no está en uso, puede emplearse como pantalla de digital signage para mostrar contenidos promocionales o informativos.

SCATI REMOTE ASSISTANT ofrece múltiples beneficios:

- Optimiza recursos al reducir la necesidad de personal físico
- Garantiza una atención profesional centralizada.
- Permite una atención inmediata al usuario.
- Mejora la seguridad mediante funcionalidades disuasorias

Esta solución versátil se adapta a distintos sectores y usos, desde puntos de información, hasta soporte técnico o control de accesos.

Con **REMOTE ASSISTANT, SCATI** redefine la atención remota, combinando tecnología, eficiencia y cercanía.

+información

AXIS COMMUNICATIONS

AXIS lanza sus primeros SENSORES AMBIENTALES

sensores de calidad del aire en interiores

"La mala calidad del aire en interiores es un problema importante de salud pública", afirma Robert Woyar, director global de productos de Axis Communications. «La Organización Mundial de la Salud estima que, cada año, casi 4 millones de muertes son causadas por la contaminación del aire interior en todo el mundo.

El vapeo de los estudiantes ha alcanzado niveles epidemiológicos en las escuelas y debe detectarse y restringirse de forma eficaz. Ciertas instalaciones específicas, por ejemplo, centros de datos y entornos de fabricación controlados, requieren un control preciso de los parámetros de calidad del aire, como la humedad relativa, la temperatura y el nivel de partículas.

Axis Comunications anuncia la incorporación a su cartera de productos de dos sensores que supervisan la calidad del aire en interiores, detectando vapeo, humo, así como otros contaminantes como pueden ser partículas, compuestos orgánicos volátiles, óxidos de nitrógeno y dióxido de carbono, además de medir la humedad y temperatura.

El modelo **AXIS D6210**, disponible en el primer semestre de este año, es integrable con otros dispositivos **Axis** (cámaras, altavoces, sirenas,..) compartiendo su dirección IP y no precisando alimentación ni switch, agregando información a la propia del dispositivo asociado.

En el segundo semestre, se incorporará el sensor **AXIS D6310**. Un modelo independiente, con su propia dirección IP y funcionalidades adicionales. Estas incluyen una función estroboscópica multi-LED para el estado del sensor y los avisos, un altavoz y micrófono integrados, alimentación PoE, un sensor de infrarrojos pasivos (PIR) y **AXIS Audio Analytics.**

+información

Bosch DesignHub

Planifique con precisión... asegure con confianza

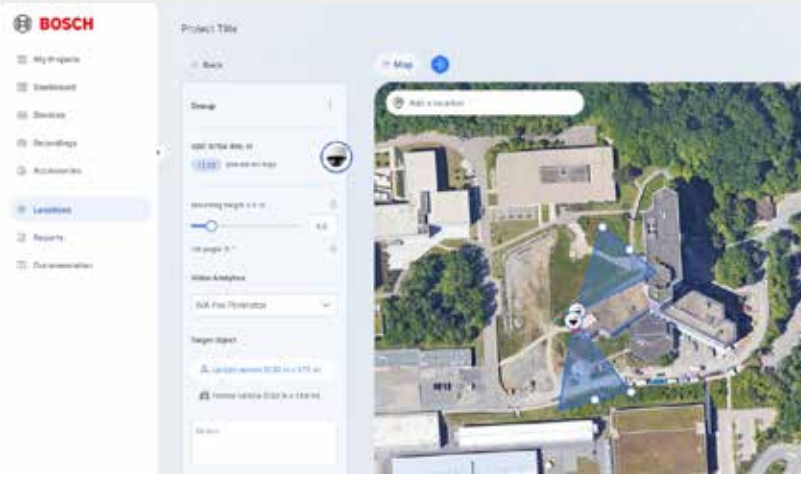
BOSCH

DesignHub es la nueva herramienta de diseño integral de los sistemas de videovigilancia de Bosch. Gracias a esta herramienta totalmente gratuita y online, usted podrá definir y planificar con precisión un sistema de este tipo, de forma simple y eficiente.

La herramienta de diseño y planificación **DesignHub** contiene todo lo necesario para diseñar la solución de videovigilancia de **Bosch**, desde la selección de cámaras y sus accesorios de montaje, hasta los sistemas de gestión y grabación. Puede además añadir licencias adicionales a las cámaras para análisis específicos basados en IA, así como otros elementos típicos del sistema, como teclados de operador o estaciones de trabajo.

También incluye la opción de añadir mapas y planos para ubicar las cámaras sobre ellos, y tener así una visión global del sistema.

Por último, usted puede obtener toda la documentación relativa al diseño del sistema, reportes personalizados, la obtención de un listado de materiales, y solicitar un presupuesto del sistema diseñado.



Tanto si es con consultor, integrador de sistemas o distribuidor, **DesignHub** fue diseñado pensando en sus necesidades. Una herramienta todo en uno que le permite planificar con precisión, seguridad y confianza.

+información

Casmar y Honeywell

unen fuerzas para distribuir soluciones avanzadas de detección de incendios

Casmar se complace en anunciar su nuevo acuerdo estratégico con Honeywell. Gracias a esta alianza, comenzaremos a distribuir los sistemas de protección contra incendios de Honeywell en España y Portugal.

Fundada en 1906, **Honeywell** cuenta con más de un siglo de experiencia y ha sido pionera en la creación de sistemas de detección avanzados, integrando tecnologías como sensores inteligentes, conectividad IoT y automatización para ofrecer la máxima protección en entornos industriales, comerciales y residenciales.

La marca ha reforzado su catálogo con tecnologías avanzadas que optimizan la seguridad y el mantenimiento de los sistemas. Sobresale la nueva serie de detectores inteligentes con función de autoevaluación (Self-Test), capaces de realizar pruebas automáticas de humo sin intervención manual, cumpliendo con los estándares EN54.

También cobra relevancia la tecnología OTBlue de Gent, marca que introduce detectores multicriterio con sensores ópticos LED azul y análisis temporal de señales, mejorando la detección de incendios abiertos, latentes y de alta temperatura.

Igualmente, merece mención la gama **S-Quad** de **Honeywell**, que integra detectores con sirena y dispositivos de alarma visual (VAD) certificados según la norma **EN54-23**, ofreciendo alertas acústicas y visuales en un solo equipo, ideales para entornos como hoteles u hospitales. Finalmente, se debe mencionar la nueva serie de centrales LT de **Morley-IAS**, que se caracteriza por su diseño compacto y pantalla táctil de 4,3 pulgadas, con una configuración intuitiva e integración con dispositivos inalámbricos.

Los productos de **Honeywell** ya se encuentran disponibles en nuestro catálogo. Descubra las soluciones de este fabricante en nuestra web o contacte con su comercial para obtener más información.

DESICO refuerza su compromiso con la ciberseguridad

En DESICO, entendemos que la ciberseguridad ya no es solo una cuestión técnica, sino un componente esencial de cualquier estrategia empresarial sólida. Por ello, llevamos tiempo abordando una transformación significativa en el diseño de nuestros productos, en nuestros procesos internos y en nuestra estructura organizativa, con el objetivo de integrar la seguridad de la información como un pilar central de nuestras operaciones.

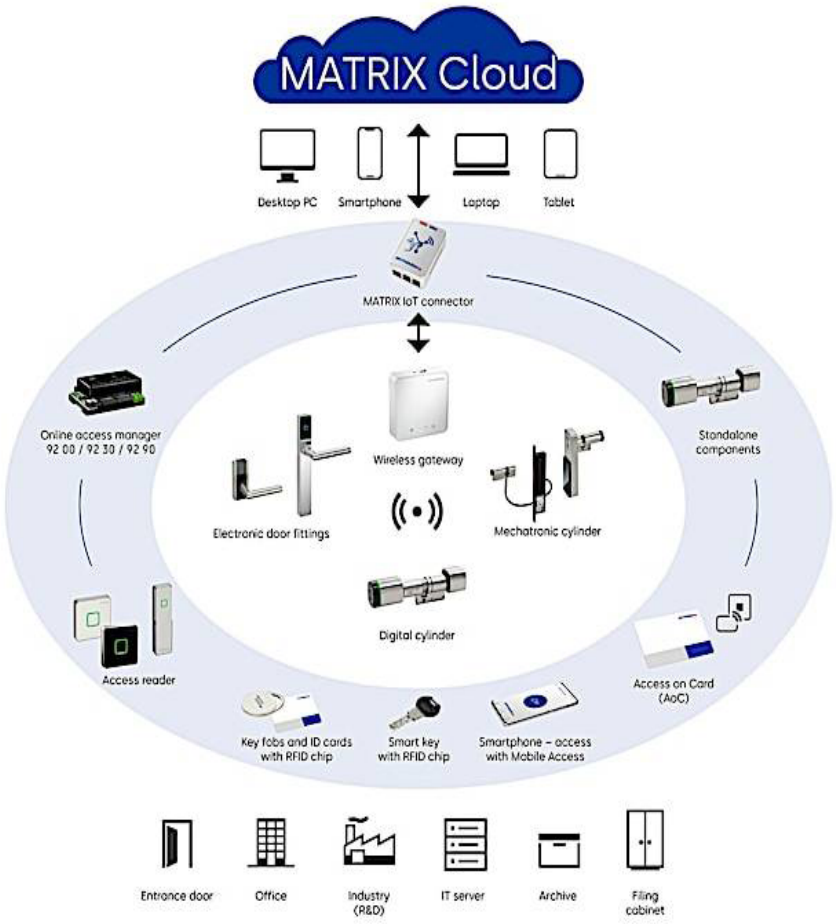
Como parte de esta transformación, **DESICO** ha obtenido la certificación **ISO/IEC 27001**, el estándar internacional que valida las buenas prácticas en gestión de la seguridad de la información. Este hito ha supuesto una revisión a fondo de nuestros sistemas, políticas y controles, alineando nuestras prácticas con los requisitos más exigentes del sector.

Pero esta evolución no se detiene aquí. Seguimos trabajando permanentemente en implementar nuevas certificaciones y líneas de trabajo que nos permitan ir más allá del cumplimiento normativo, integrando la seguridad desde el diseño en cada fase de desarrollo y operación, así como adoptando las mejores prácticas en la implantación de nuestros productos. En este proceso, estamos colaborando con expertos y autoridades para desarrollar los sistemas y productos que nuestros clientes demandan, bajo las regulaciones europeas y nacionales.

Es por ello que, el pasado 10 de junio, **DESICO** coorganizó junto a **CASMAR** la **I Jornada de Seguridad bajo Normativa**, donde se pudieron analizar las novedades normativas que afectan a la ciberseguridad de los productos y cómo **DESICO** se prepara para el cumplimiento de las futuras obligaciones de CER y NIS2. **DESICO** también fue protagonista en el **17 congreso SEG2: CiberSeg España, centrado en la Soberanía Digital**, es decir, en la importancia de disponer de proveedores nacionales y/o europeos para asegurar la independencia y soberanía de las organizaciones europeas sobre sus datos. En este evento, **DESICO** abundó en su compromiso con la seguridad de la información y en el papel estratégico que está llevando a cabo como proveedor de organizaciones nacionales de alto riesgo.

Para **DESICO**, proteger la información de nuestros clientes y de nuestra propia organización no es solo una responsabilidad, sino también una apuesta estratégica de largo recorrido.

dormakaba



MATRIX CLOUD

La nueva era en la gestión de accesos, sin infraestructuras complejas

Gestionar el control de accesos ya no tiene por qué implicar servidores, instalaciones costosas ni mantenimiento constante.

Con MATRIX Cloud, dormakaba presenta una solución 100 % en la nube que simplifica la gestión de accesos y ofrece máxima seguridad y flexibilidad.

La plataforma permite controlar todos los accesos desde cualquier lugar, sin necesidad de infraestructura IT compleja. Además, las actualizaciones son automáticas y la seguridad está certificada, garantizando un sistema siempre al día y protegido frente a amenazas.

La instalación es rápida y no interrumpe la operativa diaria. Los costes son predecibles y adaptables a las necesidades de cada empresa, lo que facilita su planificación.

MATRIX Cloud es ideal para responsables de seguridad que buscan un sistema moderno, escalable y libre de complicaciones técnicas. Y lo mejor: es posible implementarlo sin realizar cambios drásticos en la infraestructura existente.

Descubre cómo puedes transformar tu gestión de accesos.

+información

La importancia de las certificaciones en entornos críticos

DORLET

En infraestructuras críticas, la fiabilidad de los sistemas de seguridad no puede dejarse al azar. Contar con soluciones certificadas —bajo estándares como UNE-EN 50131-1 y UNE-EN 60839-11-1— no solo garantiza la calidad del producto, sino que asegura su comportamiento ante amenazas específicas y bajo condiciones extremas.

En **DORLET** trabajamos con dispositivos certificados en Grado 4, lo que implica resistencia frente a ataques sofisticados, supervisión continua del sistema y respuesta controlada ante intentos de manipulación o sabotaje.

Estas certificaciones aseguran que tanto el hardware como el software cumplen con criterios verificables: cifrado de comunicaciones, detección de pérdida de integridad, gestión segura de eventos, control de accesos lógico con roles definidos y trazabilidad completa. Esto no solo facilita la homologación en proyectos complejos, sino que reduce el riesgo de brechas, errores de configuración o comportamientos no documentados.

En el contexto regulatorio actual —con NIS2 y el Reglamento CER en el horizonte—, disponer de soluciones certificadas facilita el cumplimiento normativo, aporta confianza a los operadores y auditores, y permite una gestión proactiva del riesgo.

En definitiva, las certificaciones no son un distintivo comercial: son la base sobre la que construir sistemas seguros, auditables y resilientes.

PNS-NEXUS

Plataforma Avanzada de Gestión Remota de Eventos

Desde F.F.Videosistemas nos complace presentar PNS-NEXUS, una plataforma web que permite acceder y gestionar de forma centralizada los eventos generados por sistemas de grabación GEUTEBRÜCK.

Posee cuatro potentes herramientas:

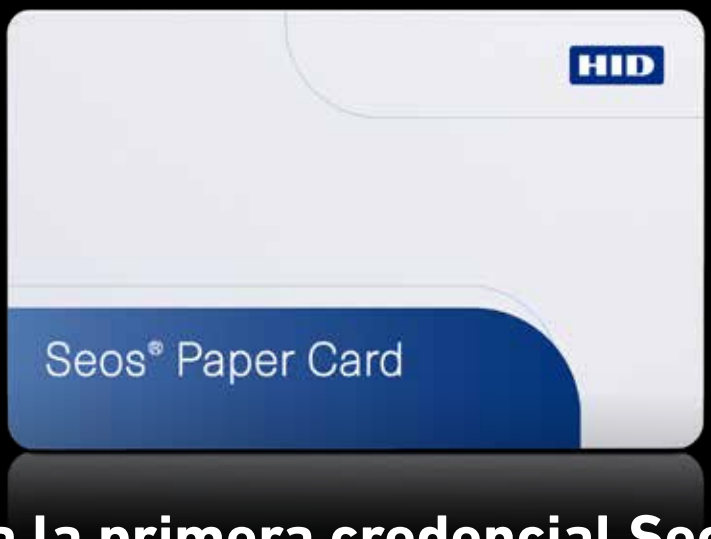
1. LPR (Reconocimiento de Matrículas):
Permite búsquedas precisas mediante filtros como matrícula, fecha, color de vehículo o pertenencia a listas blancas o negras. Esto facilita la identificación y seguimiento de vehículos dentro de la instalación, mejorando significativamente la seguridad.

2- LOGISTICS:
Ofrece trazabilidad completa de paquetes gracias a la gestión de eventos de lectura de códigos. Cada registro se acompaña de imagen, metadatos y opciones de exportación que facilitan la auditoría y resolución de incidencias.

3- FORENSIC SEARCH:
Permite realizar búsquedas precisas de incidencias mediante filtros avanzados como tipo de objeto (persona o vehículo), selección de zonas dentro de la imagen, color de prenda (superior o inferior) entre otros, optimizando así la eficiencia operativa y agilizando la resolución de eventos relevantes.

4- FACE APP
Permite/proporciona supervisión de accesos asociados a tecnología de reconocimiento facial. Permite realizar búsqueda por identificadores (nombre, número de tarjeta), dispositivos e instalaciones, así como también gestionar credenciales de los dispositivos permitiendo altas, bajas y modificaciones de forma centralizada.

PNS-NEXUS transforma los datos en información útil, accesible y exportable, desde cualquier lugar y en cualquier momento.



HID Presenta la primera credencial Seos® Papel

diseñada y fabricada a para reducir la utilización de PVC en usos temporales

La credencial HID Seos en papel es una credencial pensada para el uso de control de accesos asequible, ideal para aplicaciones o usos de manera temporal, pero con un alto nivel de Seguridad.

Fabricada con papel con certificación FSC, la credencial de papel Seos ofrece tecnología de seguridad avanzada, demostrando una vez más, el compromiso de **HID** con la sostenibilidad, al reducir el uso de plásticos derivados del petróleo y el contenido de PVC. Al estar 100 % libre de PVC, reduce significativamente la huella ambiental en los vertederos

Bajo este contexto, **HID** presenta las nuevas tarjetas de acceso altamente seguras fabricadas en papel, demostrando la innovación continua de la marca sin comprometer la seguridad y la experiencia de sus clientes.

HID Seos Papel, se suma a la ya exitosa SEOS Bambú lanzada hace más de 2 años. permitiendo adicionar otra opción sostenible dentro de los ecosistemas de acceso físico, ya que respalda una cadena de valor más respetuosa con el medio ambiente en entornos donde todavía se requieren tarjetas de acceso físicas.

La **Credencial SEOS Papel**, posee los mismos niveles de Seguridad que el resto de los productos de la línea SEOS, como son:

- Autenticación mutua (conforme a la norma ISO/IEC 24727-3)
- Diversificación de claves (basada en NIST SP800-108 con AES 128).
- Mensajería segura (conforme a la norma EN14890-1:2009).
- Derivación de claves de sesión basada en NIST SP 800-56A.
- Plataforma con certificación de hardware Common Criteria (CC) EAL 5+.

La **Credencial SEOS Papel**, también es compatible con **HID FARGO DTC,** permitiendo personalizar la misma, del mismo modo que se realiza con una credencial de PVC.

+información

Impulsando la nueva generación: una mirada al nuevo

SoC Wisenet 9 de Hanwha Vision

El futuro de la seguridad exige soluciones más inteligentes, eficientes y sólidas. Hanwha Vision lidera esta transformación lanzando su System on Chip (SoC) con Inteligencia Artificial integrada más avanzado: Wisenet 9.

Un factor diferenciador fundamental es la incorporación de dos Unidades de Procesamiento Neuronal (NPU), que triplican el rendimiento en comparación con la generación anterior. Este enfoque garantiza que la calidad de video y las analíticas dispongan de recursos independientes, evitando que una función afecte negativamente a la otra.

Revolución de la Inteligencia Artificial integrada

La inteligencia artificial es poderosa, pero también puede ser intensiva en recursos. **Wisenet 9** cambia esa narrativa. No solo es inteligente, también es eficiente, optimizando cada aspecto de su funcionamiento.

Wisenet 9 también aprovecha la Inteligencia Artificial para ofrecer análisis avanzados. Su tecnología mejorada permite analizar numerosos atributos (color, mochila, mascarilla, gafas, edad o género), junto con analíticas clave, facilitando la toma de decisiones.

Otras prestaciones importantes son:

- Re-Identification (RE-ID) para seguimiento avanzado de personas
- Máscara Dinámica de Privacidad - Dynamic Privacy Masking (DPM)
- Wisenet 9 es compatible con AI Packs (Tráfico, Retail, Industria), diseñados
- Plataforma Abierta de Hanwha Vision: permite crear soluciones de seguridad a medida
- Certificación FIPS 140-3 Nivel 3; esta certificación garantiza que el chipset cumple con estrictos protocolos de seguridad

Descubre el rango de cámaras **Wisenet 9** actualmente disponible:

+información

Johnson Controls

asegura la resiliencia con las cámaras

Illustra Flex y Pro

Johnson Controls cuenta en sus cámaras Illustra Flex y Pro, con características diseñadas para garantizar la máxima seguridad y resiliencia en entornos críticos. Con tecnologías avanzadas que aseguran la continuidad operativa ante posibles interrupciones, estas cámaras cumplen con los estándares más exigentes, como la normativa NIS2.

Entre sus innovaciones destaca **Tricklestor,** un mecanismo de alta disponibilidad que permite a la cámara almacenar las grabaciones de manera local en una tarjeta SD en caso de pérdida de comunicación con el servidor de grabación.

Estas grabaciones son encriptadas para garantizar la protección de datos, y una vez recuperada la conexión, se realiza un volcado automático a los servidores sin necesidad de intervención del usuario, manteniendo la transmisión en vivo y la seguridad de las comunicaciones.

Además, para mitigar los riesgos asociados a fallos en el suministro eléctrico, las cámaras **Illustra Flex** y **Pro** cuentan con alimentación redundante. Aunque la alimentación habitual sea PoE, tienen la opción de conectarse a una fuente de 24V AC, permitiendo que sigan funcionando incluso si el switch PoE sufre una caída.

Estas características de manera conjunta convierten a las cámaras Illustra en una solución robusta y confiable para entornos críticos, garantizando seguridad, resiliencia y cumplimiento normativo.

Cámara *pinhole* con desenfoque de fondo para el cumplimiento del RGPD

En el sector bancario, garantizar la seguridad física y respetar el Reglamento General de Protección de Datos (RGPD), que regula la captación de imágenes identificables en espacios públicos, es crucial. Las cámaras pinhole con desenfoque de fondo son una opción ideal para cumplir ambos requisitos, especialmente en cajeros automáticos desplazados.

Lanaccess incluye en su amplio catálogo de cámaras IP una cámara pinhole equipada con inteligencia artificial capaz de desenfocar automáticamente el fondo de la imagen.

De este modo, solo se graba con nitidez a la persona que opera en el cajero automático, evitando la identificación de viandantes que pueda comprometer el cumplimiento con el RGPD.

Instalación fácil con tecnología PoE

El dispositivo tiene una resolución de 5 MP y se alimenta mediante PoE (Power over Ethernet), lo que permite su instalación con un único cable para energía y datos, evitando cableado adicional y facilitando el despliegue en cajeros ubicados en exteriores.

+información

EMERGENCIA

CUANDO VIENE DESDE EL SOL...

Rafael
Moro Fonseca

Vicepresidente de la Asociación Española
de Lucha Contra el Fuego

PARAFRASEANDO A SU SUPUESTO AUTOR, FRAY LUIS DE LEÓN, COMIENZO ESTE TEXTO CON EL FAMOSO "DECÍAMOS AYER", PARA HACER UNA BREVE REFLEXIÓN, SOBRE LO TRATADO EN EL ARTÍCULO PUBLICADO EN EL NÚMERO 60 DE ESTE BOLETÍN.

Después de escribir ese artículo, esperé, para redactar este texto, a que se celebrase una Jornada, organizada por la asociación que vicepresido: la Asociación Española de Lucha Contra el Fuego, dedicada al asunto de las Tormentas Solares.

Pensado en aquello de que, a veces, "el león (las precitadas tormentas solares), no es tan fiero como el lopintán" y que lo dicho en la Jornada iba a tranquilizar mi ánimo.

Y no sé qué tan fiero es el lopintán, pero que las Tormentas Solares o geomagnéticas, pueden suponer un grave riesgo para la civilización tal como la conocemos, me ha quedado claro, o más claro, después de esa Jornada.

Aunque, bien es cierto, la probabilidad de que se produzca un evento extremo es baja.

CUANDO LA EMERGENCIA VIENE DESDE EL SOL

Para empezar, perdóneseme la digresión: sé que el dicho correcto es *"el león no es tan fiero como lo pintan"*.

Pero es menester reconocer, que el tratar asuntos con cierta gravedad, merece el salpicarlos de unas gotas de ironía, sobre todo cuando, por principio, la gente esboza una sonrisa, si al hablar de los riesgos del sol, no te refieres a la importancia de embadurnarse de aceite protector.

Comenzaba el artículo anterior, con la siguiente "entradilla": ¿Se imaginan que de repente no funcionase la telefonía móvil, ni el resto de sistemas de comunicación; los vehículos fabricados con posterioridad a los años 90 se parasen; los equipos que funcionan con electrónica fallaran; no dispusiéramos de electricidad...?

Pues hemos tenido la inmensa suerte, de que nos ha sido dada la posibilidad de no tener que imaginar todo lo expuesto en el párrafo anterior, gracias a que, con un "origen multifactorial", según la Ministra del ramo, se produjera el apagón del 28 de abril.

Y le llamo suerte, porque nos ha permitido vivir uno de los escenarios que pueden derivarse de una Tormenta Solar especialmente intensa: el de la "caída" de las redes de suministro eléctrico.

Eso sí, el escenario, el del día 28, podría considerarse idílico, sobre todo en cuanto la meteorología se refiere. Y ello facilitó que el comportamiento ciudadano fuera extraordinariamente correcto.

Pero supongamos por un momento, que el apagón se hubiera producido un día de invierno lluvioso y frio y ya atardecido, es decir, oscuro y que se hubiera prolongado hasta el día siguiente..., o más. ¿A que el escenario cambia?

Un apagón producido por fallos en las redes de energía eléctrica, donde no se producen daños en instalaciones, puede estar resuelto en pocas horas, como fue el caso.

Pero una Tormenta Solar, que genere daños en múltiples ubicaciones de tecnología para la producción de energía y su transporte, por la rotura de cables, provocaría un caos mayor que el del 28 de abril.

Revisión de daños...

Hagamos un repaso de lo que sucedió en España (y Portugal) ese día y de qué habría ocurrido, si se hubiera tratado de una Tormenta Solar – en adelante TS- de grado G5:

> Por la caída general del suministro eléctrico, sólo funcionaba la tecnología conectada a generadores que utilizaban diversos combustibles o a sistemas de energía renovable autónomos o a baterías. Esto durante sólo unas horas.

En el caso de que una TS fuese la que dañase las estructuras de suministro eléctrico, el apagón podría durar días.

Y recuperar la normalidad, con la reposición del equipamiento, como los grandes transformadores, meses.

> Hubo una manifiesta dificultad para reponer el combustible para esos generadores, pues sólo funcionaban las gasolineras que disponían a su vez de tales generadores. Y los distribuidores de combustibles, tenían sus propios problemas para la carga de sus cisternas y para su posterior distribución.

En el caso de una TS y siempre que no hubiera habido daños en la electrónica de equipos y vehículos, la vuelta a la normalidad, tendría que ver con la reposición del suministro eléctrico.

> Se produjeron problemas de funcionamiento de las redes de telefonía móvil y de telecomunicaciones en general, debido en su mayor parte a la falta de suministro eléctrico en instalaciones básicas de esas redes y agotamiento de las baterías o del combustible de los generadores, en los equipos remotos ("repetidores").

Si mediara una TS, además podrían verse afectadas algunas bandas de frecuencias.

> No se vieron afectados los sistemas de geoposicionamiento mediante satélites, ni las comunicaciones realizadas a través de ellos (salvo en la componente terrestre de esas redes de comunicación).

Pero las partículas solares pueden dañar componentes electrónicos de esos satélites y en el resto de los de la zona afectada por la TS y alterar sus órbitas, ocasionando fallos en sistemas de posicionamiento global (GPS y otros), fundamentales para navegación, telecomunicaciones y agricultura de precisión.

Y puede llegar a producirse el Síndrome de Kessler (colisiones encadenadas de satélites o sus restos y caída descontrolada a la Tierra).

De hecho, la red de satélites Starlink de Elon Must, está teniendo problemas, debido a las tormentas solares.

Éstas, están influyendo en la velocidad de caída de los satélites que, por haber terminado su periodo de vida útil, son enviados hacia la Tierra.

El descenso lo tienen que hacer a una velocidad que consigue que se desintegren, antes de llegar a nuestra atmosfera.

Lo que no está ocurriendo por esas TS´ s..., y ya están apareciendo restos en algunos lugares de la superficie terrestre.

> Durante el pasado 28 de abril, sólo se produjeron problemas en la aeronavegación, en las instalaciones en tierra (sobre todo aeropuertos).

Una TS afectaría a las rutas de vuelo cercanas a los polos, que pueden sufrir interrupciones en comunicaciones por radio y en sus sistemas de geoposicionamiento.

Como les ocurriría, en lo que se refiere al segundo problema a los vuelos en el resto del mundo, si se producen fallos en los sistemas de geolocalización.

Y pueden también aumentar los niveles de radiación para tripulación y pasajeros.

> Dependemos de la infraestructura digital y redes eléctricas. Lo del día 28 fue sólo un aviso.

Un apagón prolongado podría afectar gravemente a: la Banca y pagos electrónicos; Internet y telecomunicaciones; almacenamiento y respaldo de datos.

> Infraestructuras críticas. Difícil será conocer lo que ocurrió el 28 de abril (curiosamente, fue un 28 de abril, el del 2011, cuando se aprueba Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas) en todo ese sector, pero seguro que se está reconsiderando esa Ley.

¿Qué tan probable es un evento catastrófico?

El evento Carrington de 1859 fue la tormenta solar más intensa registrada. Si ocurriera hoy, podría causar daños valorados en billones de euros y dejar sin electricidad a regiones enteras por semanas o meses.

Se estima que eventos de esa magnitud podrían ocurrir cada 100 a 200 años. Algunos estudios le dan una probabilidad del 12% en la próxima década.

¿Qué se está haciendo?

Por un lado, un monitoreo constante del Sol por varias Agencias USA especializadas: National Aeronautics and Space Administration (NASA); National Oceanic and Atmospheric Administration (NOAA); ... y, en España, desde el Instituto de Astrofísica de Canarias y el Servicio Nacional de Meteorología Espacial, (seNMes) de la Universidad de Alcalá de Henares.

Por otro, se trabaja en la preparación de Planes de contingencia en infraestructuras eléctricas críticas.

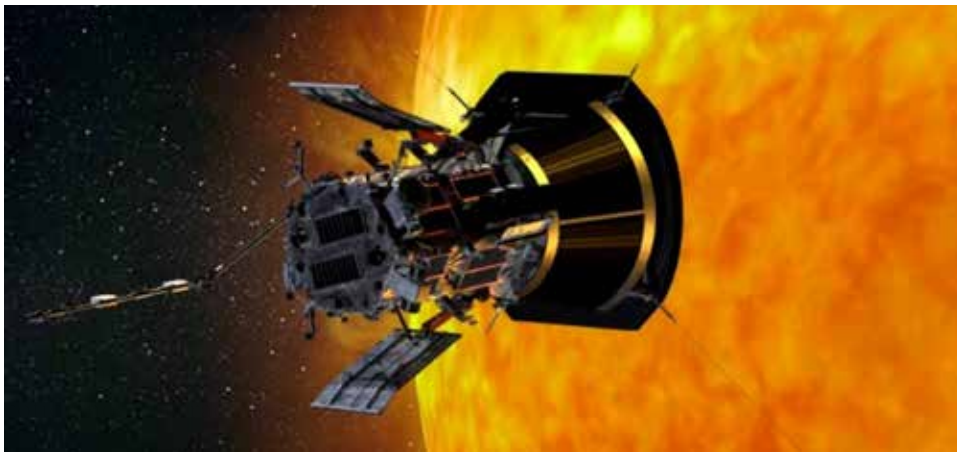
Además, en las nuevas líneas eléctricas, se están implementando diseños específicos para los transformadores y la red que ayudan a reducir el impacto de las corrientes geomagnéticas inducidas. Esto incluye ajustar ciertas características técnicas, como la capacidad de los transformadores para resistir estas corrientes y la configuración de las conexiones eléctricas, para desviar dichas corrientes y minimizar los daños.

Y en las líneas ya construidas se están instalando sistemas que limitan la presencia de esas corrientes geomagnéticas inducidas. Estos sistemas, compuestos por sensores y elementos electrónicos, detectan anormalidades y bloquean la entrada de estas corrientes a través del conductor de neutro, que es la vía de retorno de la corriente eléctrica en un circuito, protegiendo así la red eléctrica de posibles daños.

También se está invirtiendo en el diseño de satélites resistentes a radiación solar, lo que implica el uso de materiales y técnicas de protección para mitigar los efec-

tos dañinos de la radiación solar, como la radiación ultravioleta, los rayos X, los rayos gamma y las partículas cargadas. Estos efectos pueden incluir daños en los componentes electrónicos, cambios en las propiedades de los materiales y degradación general del rendimiento del satélite.

Estos diseños son especialmente útiles en: satélites GPS, Galileo, etc., que deben operar de forma fiable durante muchos años en un entorno espacial hostil; satélites de telecomunicaciones que requieren una alta fiabilidad y disponibilidad para transmitir datos y señales; satélites que operan en órbitas bajas, donde la radiación es más intensa; sondas como la **Parker Solar Probe**, que están diseñadas para operar cerca del Sol y requieren una protección térmica extrema.



Si como algunos expertos aseguran, tales radiaciones pueden inhibir el funcionamiento de tecnologías basadas en la electrónica, habría de procurarse el proteger esa electrónica de ellas.

Imaginemos que durante una Tormenta Solar G5, los vehículos y equipos de los Servicios de Atención a la Emergencia, no funcionasen. O los de los hospitales.

Por último...

Consciente que se quedan cosas en el tintero, si no se hace a través de la consideración como infraestructuras críticas, debe hacerse como instalaciones de protección prioritaria.

Me refiero, a las sedes de los 1-1-2, o las de telecomunicaciones de Servicios de Atención a la Emergencia, desde su construcción, faradayzando las estructuras de sus edificios, sobre todo las zonas de ubicación de las tecnologías de gestión de los recursos e implementando sistemas de suministro de energía redundantes y que permitan la continuidad en sus funciones durante muchos días.

Sí, las tormentas solares suponen un riesgo real, aunque no inminente, para la civilización moderna altamente dependiente de la tecnología.

Invertir en prevención, resiliencia y vigilancia solar es clave para reducir el impacto de un posible evento extremo.

CONOCE A UN

SOCIO

Javier Morán

SOCIO Nº 130

javier.moran@securitas.es

Buenos días Javier, para arrancar, dinos algunas palabras que nos permitan empezar a conocerte

Soy madrileño, de 57 años y residente en Madrid.

Profesionalmente desde que acabe mis estudios universitarios entré en el mundo de la seguridad y allí he desarrollado toda mi carrera profesional. Y encantado de poder colaborar con Aeinse unos minutos y contaros mis experiencias y mi punto de vista en algunos aspectos.

¿Cuál es tu formación académica?

Mi titulación es de Ingeniero Técnico Industrial en electricidad por la Universidad Politécnica de Madrid

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

Hasta el día de hoy mi actividad profesional se ha desarrollado siempre por varias empresas instaladoras/integradoras de sistemas de seguridad. Y en este transcurrir han existido diferentes cambios de denominación social de la empresa y adquisiciones de estas.

Inicie mi andadura profesional en Comercial Internacional de Seguridad (antes SIT) en 1994, empezando como instalador y posteriormente como coordinador de instalaciones.

Pase a Securitas Seguridad España allá por 1997 como ingeniero de proyectos. Luego Securitas Systems, donde seguía realizando las mismas funciones.

Llegó el cambio de nombre a Niscayah donde realice funciones de delegado de Madrid y posteriormente Gerente de zona Centro. Estos puestos supusieron un cambio en mi desarrollo profesional, pues ya suponían empezar a entender cómo funciona una empresa a nivel de estrategias y resultados y cómo de importante es estar alineado con los objetivos y tratar de que el equipo de quien eres responsable también siga la misma línea. Teniendo la oportunidad de aportar ideas y propuestas.

Tras varios años, Stanley Security realizó una oferta para conseguir la adquisición de Niscayah y en esta empresa pase a desempeñar el puesto de responsable de Oficina Técnica.

Posteriormente Stanley dejo el marcado español y la empresa fue adquirida por un fondo americano pasando a ser parte de Techco Security, en la cual realice funciones de responsable de área de presales durante unos años y acabando como responsable de compras de la empresa, tratando de aportar mi conocimiento técnico a este departamento de la empresa.

Finalmente, Techco fue adquirida por Securitas Seguridad España en la cual he estado desarrollado funciones de Jefe de proyecto para un proyecto emblemático durante unos años y llegando a la actualidad, en la que desarrollo funciones como Jefe de Ingeniería, Presales y Oficina Técnica dando soporte fundamentalmente a cuentas globales.

No recuerdo quien me hizo el comentario, que este mundo de la seguridad electrónica te envuelve y casi te atrapa, y una vez en él y tras varios años , resulta que ya estás en un sector en el cual desarrollas tu vida profesional en diferentes puestos, bien por propia evolución profesional, como por acometer nuevos retos.

Conociendo la historia, coincidimos muchos años en Securitas, me atrevería a decir "muchos cambios para terminar en la misma empresa". ¿cómo viviste los cambios? ¿Qué supusieron para ti?

Como bien comentas coincidimos y si, muchos cambios en los puestos ocupados y con diferentes responsabilidades.

Los cambios me han ido llegando curiosamente para acabar en la empresa donde realmente empezó todo mi desarrollo como ingeniero de proyectos, el cual me ha ido dando la experiencia para acometer otros retos.

Todos los cambios me han aportado diferentes puntos de ver este mundo y poder aportar mi experiencia y conocimiento.

Y los he vivido inicialmente y en algún caso con alguna incertidumbre al producirse, pero que me han posibilitado ampliar mi experiencia profesional y el "agitarme" para poder acometer los retos que me han supuesto estos cambios.

¿Cómo llegaste al sector?

Cierto es que conocí este mundo un poco por casualidad, porque todo empezó con el proyecto final de carrera relacionado con el desarrollo de un sistema de seguridad para un entorno de pública concurrencia, y surgió la posibilidad de incorporarme a este mundo de la seguridad y ahí empezó todo el camino profesional por diferentes puestos y empresas.

Tienes una experiencia muy completa; comenzaste como instalador, para pasar a la ingeniería de proyectos y gestión de departamentos. En la actualidad, como me has dicho, Ingeniería de presales y oficina técnica. ¿Qué destacarías de cada uno de estos puestos?

Todos los puestos han aportado algo importante, pues bajo mi punto de vista y trayectoria profesional, en este Mundo de la Seguridad Electrónica la mejor Universidad y el desarrollo profesional es el trabajo día a día. Cada puesto con su aportación.

Pero creo que los primeros pasos son los que más me atrajeron. Los trabajos como instalador o coordinador de instalaciones son los que me han proporcionado el conocimiento para entender todo mejor y desde la base; complejidades que posteriormente, como ingeniero de proyectos, he podido aplicar en los proyectos, tanto a nivel de diseño como de coordinación. Bajo mi punto de vista, estos dos puestos son los que me han proporcionado el conocimiento que he ido complementando con experiencia y formación para poder acometer otros puestos de gestión.

Puestos en los que la gestión de cuentas y personas es el día a día y eres el responsable de una "pequeña

empresa" con tus responsabilidades y compromisos dentro de una gran empresa.

El paso por Oficina Técnica me ha permitido trabajar en el mundo de detalle de un proyecto de alta exigencia documental; es el puente entre el proyecto y la ejecución técnica.

Además de poder aportar el conocimiento a la creación de algunos estándares de compañía respecto de esta parte relativa a procedimientos técnicos, o documentales.

Trabajar en el departamento de compras te aporta otro punto de vista, que es importante entender dentro de la empresa, y es la capacidad de negociación con proveedores para aplicar las estrategias de la empresa, tanto a nivel global como a nivel de proyecto específico. Además de aprender otras habilidades de negociación de alquileres, rentings, contratos de suministro... todo aporta.

En los últimos años tras la vuelta a Securitas, bastante de lo anterior lo he aplicado en mi rol de Jefe de Proyecto, pues aunque los puestos anteriores a éste, bien como ingeniero, delegado o gerente, tenían bastante contacto con el trabajo de campo, este puesto de Jefe de Proyecto, y en concreto para un proyecto de gran relevancia y complejidad, ha sido un gran reto, en el cual he tratado de aportar todo el conocimiento y experiencia.

Y a su vez me ha aportado competencias y nuevas experiencias en este ámbito profesional: toma de decisiones estratégicas bajo presión, coordinación de equipos multidisciplinares, planificar, interlocución con el cliente a diferentes ámbitos y niveles, gestiones administrativas y económicas, etc.

Finalmente con el retorno al puesto de Responsable de presales y Oficina técnica , lo que me esta aportando es la posibilidad de trabajar en proyectos con clientes globales con sus requerimientos, complejidades y exigencias.

Me gustaría resaltar que en todos los puestos, siempre me he visto apoyado y respaldado por profesionales que han hecho que mi esfuerzo sea más eficaz y poder disfrutar mis satisfacciones con estas mismas personas. Siempre rodeado de grandes equipos de personas.

¿Cuál te supuso mayor esfuerzo y cuál más satisfacciones?

Pues por complejidad, diversidad de cometidos y dimensión del reto, el mayor esfuerzo ha sido trabajar como Jefe de Proyecto.

Pues realmente ha sido un puesto en el que ha sido necesario aplicar bastante de los conocimientos adquiridos hasta el momento de empezar a desarrollar este rol: ingeniería de diseño y aplicación/adaptación del proyecto, oficina técnica, relación con proveedores tanto a nivel de comprar como en el soporte técnico, interrelación con el departamento de seguridad del cliente y del promotor.

Satisfacciones, en general todos los puestos me han aportado satisfacciones de mayor o menor intensidad, porque después de un trabajo bien hecho siempre vienen las satisfacciones.

Centrándonos en los proyectos, ¿el cliente actual es más exigente que el de finales de los noventa? ¿qué es lo más valora en la actualidad?

Pues diría que sí.

Bajo mi punto de vista, han cambiado tanto las expectativas del cliente como la tecnología, que permite requerimientos de seguridad más complejos, tanto a la hora del diseño como a la hora de la implantación. Hoy en día, los clientes tienen mayor formación y acceso a información técnica y comparativas de productos, lo que les permite ajustar y definir mejor sus requerimientos. Con lo que exigen soluciones más personalizadas y justificadas.

Creo que un factor muy importante y que valoran los clientes, es la adaptación de las soluciones a sus necesidades y requerimientos, cada vez mas complejos y que se relacionan con la integración de sistemas (y no solo específicos de seguridad en algunos casos pero relacionados con ella) bajo una misma plataforma de gestión y que les proporcione y permita tener información para analizar situaciones y tomar decisiones de una manera rápida.

Sin dejar de lado temas de alta disponibilidad, conectividad, almacenamiento y gestión desde cloud, acceso desde dispositivos móviles, y obviamente ciberegurdad.

¿Cómo está repercutiendo en la elaboración de los proyectos toda la nueva legislación (NIS, CER, Resiliencia, Ciber,…) ¿Crees que estamos los ingenieros suficiente formados e informados al respecto?
Pues, sin duda, repercute de manera relevante.

Las directivas NIS2 y CER indican los sectores regulados y exigen medidas más estrictas de gestión de riesgos, resiliencia operativa y notificación de incidente, así que la seguridad electrónica debe integrarse con la seguridad lógica y digital.

Durante mi desarrollo profesional, y es obvio y necesario, se han producido cambios de tecnologías aplicables a la seguridad, y mejoras constantes y continuadas de productos y soluciones de acuerdo a la evolución de la citada tecnología.

Pero ya las soluciones basadas en redes de comunicaciones internas y externas, con servidores bien físicos, virtuales, cloud, suponen un riesgo de acceso externo tanto a los propios sistemas de seguridad como el acceso a otro tipo de información del cliente, requieren de esta legislación y estas normativas y por lo tanto de una formación adecuada.

Respecto de la formación, vamos avanzando en este mundo, que es bastante amplio y como indico especializado de conocimientos más propios de IT, y la formación como tal es de la misma manera.

¿Cómo y cuándo llegaste a AEINSE?
Pues me asocié casi en los inicios de la creación de la asociación, la cual conocí por mediación de nuestro presidente emérito Alfonso Bilbao.

Me consta qué tus responsabilidades no te dejan mucho tiempo libre, pero en el que consigues sacar ¿Qué te gusta hacer?
Si, como bien dices el tiempo que me queda libre trato de desconectar de la parte laboral y tratar de hacer un descanso mental para volver al trabajo con ideas más frescas en lo posible.

Lo que mas me gusta en mi tiempo libre es disfrutar con mi pareja, la familia y con los amigos.

Sobre todo, me gusta bastante viajar y hacer algún deporte o actividad deportiva que me vaya permitiendo la condición física.

En todo caso siempre disfrutar de una buena compañía con una cerveza bien fría es todo un placer.

Como punto final ¿Tienes alguna sugerencia para mejorar la Asociación y dar más valor a los socios?
Creo que el trabajo que se ha ido realizando durante estos años por la junta directiva y con la colaboración de los asociados, tiene unos resultados más que visibles, consiguiendo que ya cuando mencionas AEINSE dentro del ámbito de la seguridad, ya son mas que unas siglas desconocidas, es una asociación reconocida.

Sugerencias para mejorar la asociación, creo que las acciones que se realizan la dan visibilidad, pero igual mas presencia en redes sociales. Entiendo que mejor con el apoyo de expertos en estos temas.

Aunque la colaboración a través de los grupos de Whatsapp es muy colaborativa y cuenta con el grupo de profesionales que forman parte de la asociación, propondría poder tener el apoyo de consultoría legal y técnica para poder solventar dudas de un modo más estructurado o procedimental.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Security Forum'25

JUN
4 y 5

La duodécima edición de Security Forum tuvo lugar en las Drassanes Reials de Barcelona los pasados 4 y 5 de junio. Organizado por Cuadernos de Seguridad, impulsado por Peldaño Media Group y con el apoyo del Ayuntamiento de Barcelona, el evento revalidó el éxito de años anteriores con una asistencia de más de 3.000 profesionales.

Seguridad 360º, tecnología, innovación y networking han sido los motores del evento en el que se dieron a conocer novedades y soluciones de seguridad por parte de las empresas expositoras y se desarrollaron las mesas y ponencias del Congreso y Panel de Expertos.

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Aproser y CoESS

publican la versión en castellano de la Carta Europea sobre el Uso Ético y Responsable de la Inteligencia Artificial en los Servicios de Seguridad

La **Confederación Europea de Servicios de Seguridad (CoESS)**, de la que **APROSER** forma parte, publicó el pasado mes de octubre la versión en castellano de la Carta sectorial europea sobre la Inteligencia Artificial, centrada en el uso ético y responsable de esta tecnología en los servicios de seguridad privada.

El documento proporciona a las empresas del sector una guía práctica para anticiparse y adaptarse al nuevo **Reglamento Europeo de IA, 2024/1689** que entrará en vigor a partir del 2 de agosto de 2026.

Aunque existen algunas excepciones:

- Las prohibiciones, definiciones y obligaciones relativas a la alfabetización en IA se aplican desde el 2 de febrero de 2025;
- Algunas normas entrarán en vigor el 2 de agosto de 2025, incluidas las relativas a la estructura de gobernanza, las sanciones y las obligaciones de los proveedores de modelos de IA de uso general.

La Carta ofrece, entre otros contenidos, ejemplos concretos de casos de uso, oportunidades y riesgos, y una lista de verificación destinada a facilitar el cumplimiento normativo, alineado con los valores éticos promovidos por el sector.

+información

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

El BOE publica el acuerdo de Consejo de Seguridad Nacional para elaborar las nuevas Estrategia Nacional de Seguridad y Ciberseguridad

El Boletín Oficial del Estado publicó, el 26 de mayo dos importantes acuerdos del Consejo de Seguridad Nacional, adoptados el pasado 24 de abril, que aprueban los procedimientos para la elaboración de una nueva Estrategia Nacional de Seguridad y una nueva Estrategia Nacional de Ciberseguridad.

La Estrategia de Seguridad Nacional 2021 priorizó el avance en el modelo de gestión de crisis con un enfoque anticipatorio, puso el foco en los aspectos tecnológicos relacionados con la seguridad, y articuló un planeamiento de respuesta a las acciones híbridas.

El cambio significativo del panorama internacional experimentado desde 2021 tiene implicaciones relevantes para la seguridad nacional, que la nueva estrategia deberá reflejar. Por este motivo, en el proceso de revisión estratégica se enfatizarán medidas tales como el refuerzo de la disuasión y defensa, la apuesta por el desarrollo de las capacidades industriales, y el compromiso con la paz y la seguridad internacional.

La Estrategia de Seguridad Nacional de 2021 (ESN21) ratifica la vulnerabilidad del ciberespacio como uno de los principales riesgos para la seguridad del país. Hasta la fecha se han elaborado de forma concatenada dos Estrategias de segundo nivel en materia de ciberseguridad nacional, la primera en el año 2013 y la segunda, actualmente vigente, en 2019 (ENCS19).

El acuerdo subraya la necesidad de adecuar la actual estrategia al nuevo contexto de amenazas y, por otra parte debe alinearse con las pautas establecidas por la UE, tanto en la Estrategia europea de ciberseguridad 2020, como con las distintas políticas y recomendaciones emitidas en ámbitos específicos como, por ejemplo: la Política de Ciberdefensa de la UE de 2022, el 5G, la certificación, la protección de cables submarinos o el «Pacto cuántico».

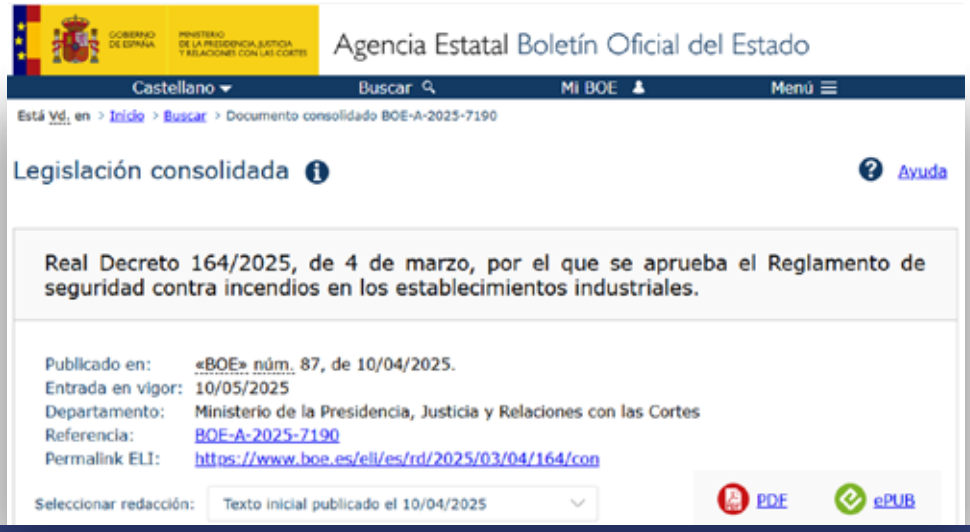
+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

RD 164/2025



Publicado el Real Decreto 164/2025, de 4 de marzo

por el que se aprueba el Reglamento de seguridad contra incendios en los establecimientos industriales.

BOE Núm. 87, jueves 10 de abril de 2025, Sec. I.

"El presente real decreto tiene por objeto revisar el marco normativo relativo a la protección contra incendios, para lo cual se aprueba un nuevo Reglamento de seguridad contra incendios en los establecimientos industriales (en adelante, RSCIEI) que deroga y sustituye al anterior, aprobado por el Real Decreto 2267/2004, de 3 de diciembre."

"Dada la evolución habida tanto en la técnica como en el marco normativo nacional y europeo, se hace conveniente revisar y actualizar los requisitos establecidos en el citado reglamento para adaptarlo a las necesidades y a las soluciones constructivas actuales y, al mismo tiempo, alinearlo con el resto de normativa de productos, instalaciones y edificación."

+información

LEÍDO, VISTO Y OÍDO EN...

En la página número 4 del Boletín de abril 2025 de la Fundación AES encontramos una interesante propuesta de Fernando Sánchez, miembro del grupo de trabajo de ciberseguridad de AES, con el título ¿Qué Formación de Ciberseguridad necesitamos en Seguridad Privada?.

Entre los aspectos tratados en el artículo, presenta un cuadro con las competencias de ciberseguridad que, desde su punto de vista, deben tener los distintos perfiles profesionales de la seguridad privada, desde el instalador hasta los gestores comerciales.

https://aesfundacion.es/boletines/pdf/3.html#book/

SEGURITECNIA

Defensa y Seguridad

Evolución de la seguridad en la defensa: **herramientas PSIM**

Herramientas PSIM

evolución de la seguridad en la defensa

En la página 52 del número 512, marzo-abril 2025, de la revista encontramos un artículo de nuestro socio y vocal de la Junta Directiva **Enrique Bilbao** sobre la utilización de los PSIM en el sector de la Defensa.

"un sector como el de la defensa debería ser capaz de contar con "partners" estratégicos capaces de desarrollar herramientas adaptadas a su casuística, contexto, vulnerabilidades y riesgo" afirma **Enrique.**

artículo completo

LEÍDO, VISTO Y OÍDO EN...

Monográfico
Seguridad en España

La revista, en su número 108, trata de forma monográfica la reconfiguración del sistema de ciberseguridad en España, destacando la importancia del establecimiento de un Centro Nacional de Ciberseguridad.

Recoge información útil que nos ayudará a comprender el complejo panorama actual de Organismos y Normativa, explicando someramente las funciones de la **Secretaría de Estado de Seguridad**, **Secretaria de Estado de Telecomunicaciones e Infraestructuras Digitales, Secretaría de Estado de la Función Pública, Agencia Estatal de Administración Digital, Consejo Nacional de Ciberseguridad** y treinta organismos más.

artículo completo

LEÍDO, VISTO Y OÍDO EN...

Historia de la física cuántica

José Manuel Sánchez Ron

José Manuel Sánchez Ron, divulgador científico y profesor universitario, ha publicado recientemente el volumen II de la **Historia de la física cuántica; la creación de la mecánica cuántica: de Heisenberg al gato de Schrödinger (1925-1935)**. 456 páginas en donde aborda un periodo vibrante y decisivo de la historia de uno de los grandes logros de la humanidad: la física cuántica.

Científicos pioneros como Werner Heisenberg, Erwin Schrödinger, Albert Einstein, Niels Bohr o Paul Dirac, entre otros, son los protagonistas de este periodo fecundo de la historia del proyecto cuántico. José Manuel Sánchez Ron narra en este segundo volumen la culminación de los esfuerzos que permitieron la creación e interpretación de la mecánica cuántica, y profundiza en sus desarrollos teóricos, mostrando cómo algunos de ellos tuvieron resultados científicos imprevistos y asombrosos. Un interesante volumen para los amantes de la física.

El autor es vicedirector de la Real Academia Española y miembro de la Real Academias de Ciencias Exactas, Físicas y Naturales y de la Academia Europea de Ciencias y Artes.

Editorial Crítica – ISBN 9788491997795

JORNADA

Tormentas solares y apagones

El pasado 10 de junio tuvo lugar en el auditorio del Museo de Bomberos de Madrid esta jornada, que estuvo organizada por **ASELEF** en colaboración con el Ayuntamiento de Madrid y su Servicio de Bomberos.

Las tormentas solares son más frecuentes de lo que piensas! Aunque muchas veces ni nos enteramos de su impacto, este fenómeno espacial afecta a las comunicaciones, los sistemas eléctricos, la aviación...

Hasta el punto de que te podrían dejar un tiempo sin móvil o incluso provocar incendios si se producen con mucha potencia.

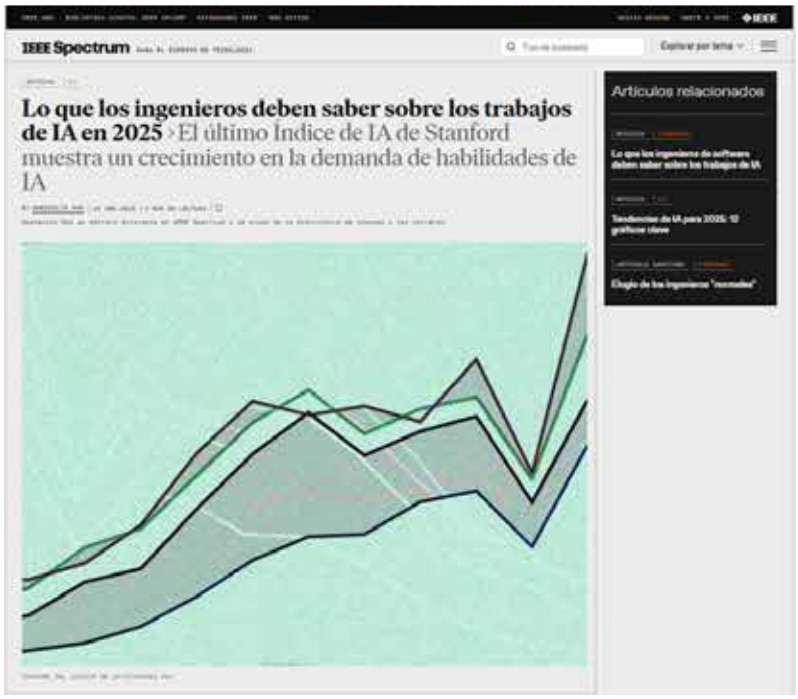
La jornada fue abierta por **Rafael Moro**, vicepresidente de ASELF, y **José Luis Legido**, secretario general. En el siguiente enlace puede verse un vídeo resumen de la jornada.

vídeo de la jornada

LEÍDO, VISTO Y OÍDO EN...

IEEE Spectrum

Lo que los ingenieros deben saber sobre los trabajos de IA en 2025



IEEE presenta un informe sobre la evolución y oportunidades laborales en el segmento de la IA

Parece que los empleos de IA han llegado para quedarse, según los últimos datos del Informe del Índice de IA 2025.

Para comprender mejor el estado actual de la IA, el informe anual del Instituto de Inteligencia Artificial Centrada en el Ser Humano (HAI) de la Universidad de Stanford recopila una amplia gama de información sobre el rendimiento de los modelos, la inversión, la opinión pública y más. Cada año, **IEEE Spectrum** resume nuestras principales conclusiones de todo el informe mediante una serie de gráficos, pero aquí nos centramos en el efecto de la tecnología en la fuerza laboral

Leer el artículo completo: **aquí**