BOLETÍN Nº61 ABR 2025

AEINSE
Asociación Española de Ingenieros de Seguridad

Asamblea´25

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

El Congreso de Ingeniería de Seguridad se pospone al segundo semestre del año

Como ya se manifestó en el boletín anterior, este año AEINSE retoma la organización de los Congresos de Ingeniería de Seguridad que se vieron interrumpidos por la pandemia del COVID y sus limitaciones y miedos posteriores a las reuniones.

El último se celebró en el año 2019. Siguiendo con la pauta de realizarlo en los años impares, en los que no hay SICUR, el de 2025, por razones de ajuste en la planificación del evento, tendrá lugar en Madrid en el segundo semestre del año en lugar de en el primero previsto. Serán notificados fecha y lugar convenientemente.
Acorde con los objetivos de nuestra Asociación, se tratarán temas relacionados con la innovación y desarrollo tecnológico, contribuyendo a la formación y divulgación técnica en la ingeniería de seguridad. Además será punto de encuentro e intercomunicación entre socios, patrocinadores y otros asistentes.

Entre los temas previstos está, como no podía ser de otro modo, la influencia y uso de la Inteligencia Artificial en los análisis inteligentes de los sistemas de CCTV, la automatización de los controles de acceso, la detección de intrusión y otras aplicaciones. También trataremos los desafíos y necesidades de la Ingeniería de Seguridad y la figura del ingeniero, la ciberseguridad de los equipos y aplicaciones y la detección perimetral en sus aspectos tecnológicos actuales, la necesidad de disminuir las falsas alarmas y la gestión de las CRAs.

Esperamos que este congreso tenga el éxito de las ediciones anteriores y se cumplan los objetivos de divulgación y formación que nos hemos propuesto. Será una oportunidad clave para conocer en profundidad los avances tecnológicos y debatir sobre el futuro de la IA en seguridad electrónica. El evento reunirá a expertos del sector para compartir conocimientos y experiencias sobre los temas apuntados.
A pesar de esta modificación, el congreso seguirá abordando temas cruciales como las tecnologías emergentes en Inteligencia Artificial.

CCTV y análisis inteligente
El desarrollo de IA en sistemas de videovigilancia ha permitido transformar el CCTV de una herramienta pasiva a un mecanismo inteligente capaz de analizar imágenes en tiempo real. La detección de anomalías, el reconocimiento facial y el procesamiento de matrículas son algunas de las funcionalidades que han mejorado la seguridad en diversos entornos.

Control de accesos automatizado
Las soluciones de control de accesos han incorporado IA para fortalecer la seguridad mediante autenticación biométrica y análisis predictivo de patrones de entrada. Esto ha permitido que empresas y organismos gubernamentales reduzcan riesgos y optimicen la gestión de accesos sin comprometer la eficiencia.

IA en la detección de intrusiones
Los sistemas modernos de detección de intrusión han evolucionado gracias a la IA, logrando identificar comportamientos sospechosos y anticipar amenazas. La combinación de sensores avanzados con algoritmos predictivos mejorará la capacidad de respuesta y podrá prevenir incidentes antes de que se materialicen.

Otras aplicaciones en seguridad electrónica
La IA también se ha integrado en la ciberseguridad, protección perimetral y respuesta a emergencias. Su capacidad para procesar grandes volúmenes de datos en segundos permite detectar vulnerabilidades y coordinar respuestas eficientes ante eventos críticos.

AEINSE
Asociación Española d
Ingenieros de Seguridad

NOTICIAS AEINSE

ASAMBLEA'25

29
ABR
2025

CONVOCATORIA ASAMBLEA GENERAL ORDINARIA

El Presidente, de acuerdo con lo establecido en el Capítulo III, Artículo 18, de los Estatutos, convoca la ASAMBLEA GENERAL ORDINARIA de AEINSE.

Tal como reflejan nuestros Estatutos, en aras a promover el mayor grado de participación y seguridad de l@s asociad@s, la **Asamblea General Ordinaria 2025** se realizará con carácter mixto, es decir, tanto presencial en Madrid, como por teleconferencia, el próximo **29 de Abril de 2025**, a las **19:00 horas**, en 1ª y única convocatoria.

De forma presencial el acceso a la Sala podrá realizarse desde 30' antes.

L@s soci@s que elijan la fórmula telemática, podrán unirse a la reunión desde su equipo pc o portátil y con tablet o smartphone, vía streaming en el enlace que encontrarán al final del documento. La fase de conexión se iniciará desde 15' antes.

Quien no pueda asistir y desee participar en las votaciones podrá hacerlo con voto delegado, remitiendo a aeinse@aeinse.es el documento ya enviado a los socios o entregándolo en mano antes de la Asamblea por la persona delegada.

ESSIIF. Fire & Security School

a través de su área conocimiento en seguridad , en la que colaboran AEINSE y la Universidad Isabel I, ha desarrollado este programa formativo, que tiene como objetivo fundamental proporcionar al alumnado una formación completa y cualificada en sistemas de control de accesos.

05 MAYO
13 JUNIO
2025

El curso tendrá lugar entre el **5 de mayo y el 13 de junio** próximos, con **20 horas de clases en vivo/directo** vía plataforma de videoclases. La dedicación estimada por parte del alumno es de **60 horas.**

Su objetivo fundamental es proporcionar al alumnado una formación completa y cualificada en sistemas de control de accesos, desde el punto de vista de sus condicionantes legales y normativos, tecnología, diseño, instalación, puesta en marcha y mantenimiento de los mismos.

Todos los alumnos que superan el **Curso de especialización en sistemas de control de accesos** reciben el título propio de la Escuela, con certificación del contenido superado, las horas cursadas y la fecha de inicio y de fin de los estudios realizados. **El curso tiene un descuento especial para los socios de AEINSE.**

+información **matriculación**

S-GRID

Reja sensora de fibra óptica

para protección de túneles, tuberías y desagües

Sicuralia Systems

S-GRID es una solución avanzada de Sicuralia que protege canalizaciones y conductos de diversos tamaños. Este sistema combina una reja física robusta con sensores de alta tecnología, adaptándose a tuberías, desagües, túneles abiertos, canales, conductos de aire o ventanas que requieren protección. La reja, construida con materiales resistentes, soporta fuertes caudales y permanece operativa incluso cuando está completamente sumergida en agua durante años.

Los sensores de fibra óptica integrados permiten la detección temprana de intrusiones o manipulaciones no autorizadas, enviando alertas en tiempo real al sistema de gestión de seguridad. Esta característica es esencial para infraestructuras críticas donde la integridad de las canalizaciones es vital para el funcionamiento seguro de las operaciones.

Sicuralia, reconocida por su experiencia en seguridad perimetral, ofrece con **S-GRID** una solución que combina protección física y tecnológica, garantizando una defensa integral de las infraestructuras hídricas o de cualquier otro tipo. La adaptabilidad del sistema a diferentes entornos y su capacidad para integrarse con plataformas de gestión existentes lo convierten en una opción ideal para empresas que buscan fortalecer la seguridad de sus instalaciones.

En resumen, **S-GRID** representa una innovación significativa en la protección de canalizaciones, aportando una solución robusta y confiable para la seguridad de infraestructuras críticas.

+información

Nuevo sistema de control de esclusas

para entornos de alta seguridad

El sistema de control de esclusas de SCATI es una solución avanzada para gestionar accesos en áreas críticas como bancos, infraestructuras estratégicas y sectores altamente exigentes.

Este sistema evita aperturas simultáneas no autorizadas, optimiza el flujo de personas y refuerza la seguridad con reglas de acceso personalizadas. Integrado con **SCATI SENTRY**, permite una supervisión centralizada en tiempo real, activando alertas y garantizando un control preciso. La integración con **SCATI SENTRY** también facilita la generación de reportes detallados sobre el uso de las esclusas, lo que ayuda a optimizar la operativa y mejorar la seguridad. Su compatibilidad con sistemas de videovigilancia y control de accesos permite una gestión integral de la seguridad, asegurando un control eficiente y preciso en cada punto crítico de la instalación

Principales ventajas:

- **Máxima seguridad:** Impide accesos indebidos y optimiza la gestión de personas.
- **Supervisión en tiempo real:** Alertas inmediatas ante intentos de intrusión.
- **Integración total:** Compatible con control de accesos, videovigilancia y sensores.
- **Respuesta ante emergencias:** Pulsadores de desbloqueo inmediato.
- **Eficiencia energética:** Reducción de consumo en climatización.
- **Cumplimiento normativo:** Adaptado a los estándares más exigentes.

Con este lanzamiento, **SCATI** refuerza su compromiso con la seguridad e innovación, proporcionando soluciones inteligentes para la protección de entornos sensibles.

+información

AXIS COMMUNICATIONS

AXIS Communications introduce la búsqueda de texto libre en su

AXIS Camera Station Pro

(VMS de gestión de vídeo y control de accesos)

Una potente herramienta forense de vídeo que permite a los usuarios buscar con su propio texto. Esto mejora la flexibilidad y acelera las investigaciones al buscar objetos en movimiento en grandes cantidades de vídeo grabado.

La búsqueda por texto libre ofrece a los usuarios una mayor flexibilidad y les permite personalizar las consultas para satisfacer las necesidades específicas de cada caso con menos limitaciones. Pueden describir objetos móviles con mayor detalle utilizando lenguaje natural y asociaciones, lo que permite resultados más relevantes.

Se basa en un modelo básico de código abierto, entrenado en miles de millones de pares de imagen-texto y ajustado por Axis para casos prácticos de vigilancia con el fin de mejorar el rendimiento. Gracias a las asociaciones, los usuarios pueden ampliar el alcance de la búsqueda. Por ejemplo, es posible buscar personas que lleven uniformes profesionales, como trabajadores de la construcción. A continuación, el modelo encontrará objetos que coincidan con estas características típicas.

Además, es posible encontrar objetos con una marca o logotipo determinados. Para obtener resultados más rápidos se puede combinar con filtros, como la fecha y la hora, el objeto en el área, la dirección, el tamaño y la duración.

Con la búsqueda de texto libre, los datos de vídeo solo se procesan en el servidor local, lo que permite un cumplimiento normativo más sencillo. Además un registro de búsqueda ayuda a los roles de administrador a detectar cualquier uso indebido.

descarga prueba gratuita

Suite IVA Pro

(Inteligence Video Analitics Pro)

BOSCH

Bosch amplía su galardonada suite IVA Pro (Inteligence Video Analitics Pro) con siete nuevas licencias, que ofrecen detección precoz y fiable, uso sencillo y personalización para distintos entornos:

IVA Pro Privacy
Recopila datos sin alterar la privacidad; utiliza máscaras semitransparentes para anonimizar personas y objetos, al tiempo que conserva los datos procesables.

IVA Pro Appearance
Facilita la búsqueda forense con datos precisos sobre atributos físicos, como ropa y pelo.

IVA Pro Personal Protective Equipment (PPE)
Respalda el cumplimiento de la normativa detectando a las personas y sus EPI, como chalecos de seguridad o cascos, y alerta cuando faltan.

IVA Pro License Plate
Captura con precisión las matrículas de varios vehículos a velocidades de hasta 120 km/h (75 mph) y transmite la información en tiempo real.

IVA Pro Vehicle Make Model
Identifica marcas y modelos de vehículos de más de 140 fabricantes y 2.000 modelos.

IVA Pro License Plate + Make Model
Combina los datos de la matrícula y marca/modelo del vehículo para una gestión eficaz del tráfico y soluciones de aparcamiento.

IVA Pro Dangerous Good Signs
Identifica rápidamente las señales de mercancías peligrosas (ADR) en vehículos a velocidades de hasta 120 km/h (75 mph).

Las soluciones basadas en AI, como **Intelligent Video Analytics Pro**, le ayudan a tomar decisiones inteligentes y a implantar medidas de forma proactiva para minimizar los riesgos y los posibles daños a personas y propiedades.

+información

casmar
Comprometidos con la seguridad

SR7

Innovación en protección contra incendios

En la seguridad contra incendios, contar con sistemas fiables es clave. SR7 se distingue por su tecnología avanzada y su enfoque en la prevención y detección temprana.

Recientemente, ha mejorado su algoritmo de detección, integrando cámaras térmicas y video analítica para identificar sobrecalentamientos y llamas con mayor precisión. Esto soluciona desafíos en entornos como parques fotovoltaicos, donde los reflejos solares dificultaban la detección temprana.

Una innovación clave es el modo sobrecalentamiento, que analiza gradientes térmicos en lugar de depender de la visibilidad de llamas. Esto permite una detección más rápida y precisa.

Ventajas del sistema SR7

- **Detección anticipada:** Identifica anomalías térmicas antes de que se produzca un incendio.
- **Mayor alcance:** Hasta 10 veces más capacidad de cobertura.
- **Optimización de costes:** Reduce la necesidad de múltiples equipos según el diseño de cada instalación.

Además, **SR7** se destaca por su fácil instalación, mantenimiento práctico y modularidad. Su soporte técnico especializado garantiza asesoramiento, formación y asistencia, asegurando soluciones eficientes para cada proyecto.

Con estas innovaciones, **SR7** se consolida como una de las opciones más avanzadas en protección contra incendios.

DESICO®

Servicios gestionados de IoT

Desico IoT Cloud es una solución cloud-native diseñada para recopilar información procedente de dispositivos IoT, independientemente de la tecnología utilizada. Gracias a su compatibilidad con múltiples canales de comunicación disponibles en el mercado, ofrece una integración versátil y eficaz.

Esta plataforma se ha implantado con éxito en diversos sectores, algunos críticos como hospitales y centros penitenciarios, donde facilita la supervisión de movilidad, señales técnicas y monitorización ambiental, especialmente en entornos como CPDs.

Además, la Compañía ha desarrollado una aplicación específica para configurar alertas de sensores y una plataforma que permite gestionar avisos, registrar información asociada a incidencias, generar informes y mucho más. Por otra parte, su experiencia en tecnologías PSIM permite ofrecer trazabilidad completa, automatizar tareas y cerrar incidencias de forma automática.

El módulo de informes facilita la validación y exportación de datos, así como la creación de cuadros de mando personalizados para una mejor toma de decisiones.

Desde el punto de vista de la personalización, **Desico** ofrece la posibilidad de adaptar la plataforma a las necesidades específicas de cada cliente o desarrollar versiones sectoriales orientadas a industrias concretas.

Recientemente, **Desico** ha lanzado un servicio de soporte 24/7 orientado a clientes que requieren una atención continua sobre las señales de sus equipos IoT. Este servicio se basa en un equipo técnico especializado, tiempos de respuesta reducidos y atención personalizada con contacto directo con responsables clave de cada organización.

Desico se ha integrado con **Evalink**, lo que permite su conexión con múltiples CRA's, con su primer caso de éxito ya implantado en España.

dormakaba

La innovación en control de accesos da un paso más allá con la nueva cerradura electrónica Locker Lock 21 20 de dormakaba, diseñada especialmente para taquillas, vestuarios y mobiliario en entornos como empresas, centros educativos o instalaciones deportivas.

CERRADURA ELECTRÓNICA

Locker Lock 21 20

seguridad inteligente también para taquillas

Este sistema inteligente sustituye los tradicionales cilindros mecánicos por tecnología RFID de última generación, permitiendo una gestión eficiente y sin llaves físicas.

Gracias a su diseño modular, el **Locker Lock 21 20** se puede instalar fácilmente en armarios metálicos existentes sin necesidad de cableado, y su diseño compacto se adapta tanto a puertas con bisagra derecha como izquierda.

Entre sus múltiples funcionalidades destacan el acceso personalizado mediante tarjeta o llavero, el sistema

de "elección libre" de taquilla y un sistema motorizado de cierre de alta fiabilidad.

Además, el sistema se integra perfectamente con las soluciones de control de acceso existentes de dormakaba, tanto en modo autónomo como online, ofreciendo una solución global y segura.

+información

DMA

la llave que necesitas en la palma de tu mano

DORLET Mobile Access (DMA) es la solución de DORLET® que revoluciona el acceso a las instalaciones al transformar el smartphone de los usuarios en una credencial virtual segura. Gracias a las tecnologías NFC y BLE, los usuarios pueden acceder y transitar por la instalación de forma rápida y eficiente.

DMA ofrece dos modos de acceso, adaptándose a las diferentes necesidades y preferencias de los usuarios. El **modo OnTouch (NFC)** permite el acceso acercando el smartphone a un lector de la **gama EVOpass** (EVOpass® 10 BLE, EVOpass® 20 BLE, EVOpass® 40 BLE, EVOpass® 80 BLE).

Por otro lado, el **modo Button (BLE)** permite seleccionar explícitamente la puerta desde la aplicación móvil, lo cual es ideal para situaciones que requieran de más precisión, distancia de lectura o un acceso sin contacto. Esta tecnología, disponible tanto para **Android** como para **iOS**, mejora significativamente la experiencia de los trabajadores sin comprometer en ningún caso la seguridad en las instalaciones. Las organizaciones que implementan **DMA** disfrutan de un sistema escalable, fácil de integrar y altamente seguro, diseñado para cumplir con los requisitos más exigentes, incluso en **infraestructuras críticas.**

Esta solución es idónea para organizaciones que buscan adaptarse a las tendencias actuales, apostando por la innovación y la eficiencia sin comprometer la seguridad de las instalaciones.

+información

Hanwha Vision

Visión inteligente, imágenes increíblemente detalladas.

CÁMARA T SERIES AI 26MP

Nueva Solución de 26MP

con Inteligencia Artificial

Hanwha Vision presenta TNO-A26081, una cámara de ultra alta resolución impulsada por Inteligencia Artificial.

Con una resolución de 26MP a 30 fps para captar hasta el más mínimo detalle, esta solución es una opción ideal para vigilar grandes áreas.

Visión nítida y máxima flexibilidad

La resolución de la TNO-A26081 ofrece un nivel de detalle superior. Es especialmente adecuada para estadios y recintos donde la seguridad y el control de multitudes son críticos. Sus análisis basados en Inteligencia Artificial (conteo de personas y vehículos, gestión de colas, mapas de calor) facilitan una gestión eficiente de cualquier evento. Gracias a su alta sensibilidad, también es ideal para aeropuertos, puertos y plantas industriales, donde la captura precisa de detalles es clave. El modelo está equipado con un zoom óptico (55-250 mm), permitiendo un campo de visión flexible.

Análisis avanzados

La aplicación WiseAI permite la detección avanzada de objetos y atributos, identificando detalles como el color de la ropa (superior/inferior) o si una persona usa mascarilla o gafas. En el caso de los vehículos, puede detectar el tipo y su color, mejorando así las investigaciones forenses.

Rendimiento excepcional en condiciones adversas y baja iluminación

Equipada con un sensor APS-C CMOS, TNO-A26081 destaca en entornos de baja luminosidad, proporcionando imágenes nítidas tanto de día como de noche. Su capacidad superior en condiciones de poca luz garantiza una vigilancia ininterrumpida, incluso en escenarios de iluminación desfavorable.

+información

Feria ISC West 2025 de Las Vegas

presentación de innovaciones en Seguridad

Johnson Controls destaca en ISC West 2025 sus avanzados productos y soluciones, diseñados para mejorar la seguridad, la automatización y la conciencia situacional en tiempo real.

Entre las novedades técnicas presentadas destacan:

La nueva versión **C•CURE IQ 3.10** de Software House que incluye nuevas características, como mapas interiores/exteriores integrados con total continuidad, funciones mejoradas de gestión de videoclips y un nuevo conjunto de paneles de control como parte de la suite de Inteligencia de Seguridad. Esto aumentará significativamente el enfoque y la respuesta de seguridad al unificar los flujos de trabajo de control de acceso y videovigilancia.

Las controladoras **iSTAR Edge G2** de Software House han sido renovadas para soportar más puertas por panel, con hasta 8 lectores y 1 millón de titulares de tarjetas, y ahora cuentan con verificación OSDP.

La cartera de productos que soportan OSDP se extiende a una nueva familia de módulos de Entrada/Salida OSDP, los primeros en la industria, que ofrecen una protección inigualable con encriptación de extremo a extremo OSDP.

La Solución de Seguridad de **Kantech, Exacq, DSC** e **Illustra** reúne cuatro sistemas en una plataforma integrada sin fisuras: **Control de Acceso Kantech, Gestión de Video Exacq, Detección de Intrusión DSC y Cámaras Illustra**. Las tecnologías se combinan para proporcionar un ecosistema de seguridad unificado, interoperable y escalable para aplicaciones comerciales y empresariales.

En su 140º aniversario, la compañía reafirma su compromiso con la innovación en soluciones sostenibles y seguras.

Fábricas más eficientes con analítica de vídeo

En las fábricas, la analítica de vídeo se ha convertido en una herramienta esencial para mejorar la seguridad, productividad y eficiencia operativa. Más allá de la vigilancia clásica, los sistemas CCTV inteligentes convierten imágenes en datos útiles, y los alinea con los objetivos de las industrias 4.0.

En términos de seguridad, se destacan dos soluciones: detección de intrusión y reconocimiento de vehículos. Estas tecnologías permiten identificar movimientos no autorizados y gestionar accesos mediante lectura de matrículas, optimizando la trazabilidad y reduciendo errores humanos.

La protección del personal también se fortalece al detectar automáticamente si los operarios usan el equipamiento adecuado, minimizando riesgos y evitando sanciones. Además, la monitorización de la productividad permite identificar patrones de rendimiento y mejorar procesos de forma continua.

La analítica de vídeo aplicada al control de calidad es igualmente poderosa, al detectar productos defectuosos y automatizar la supervisión de líneas de producción, reduciendo desperdicios y mejorando la eficiencia.

Este enfoque integral transforma datos en ventajas competitivas, permitiendo a las industrias optimizar recursos y mejorar resultados sin necesidad de grandes inversiones en infraestructura.

¿Quieres ver la analítica en acción?

consulta este enlace

LEGIC

Con el soporte añadido de Apple Wallet, LEGIC ofrece una integración nativa en los sistemas de Apple. Esta colaboración crea una experiencia similar a la de una tarjeta en iPhone o Apple Watch, proporcionando a los usuarios una comodidad adicional y convirtiendo el acceso seguro más fácil que nunca.

LEGIC añade Apple Wallet

a su porfolio de gestión de credenciales

Gracias a **LEGIC Connect para Apple Wallet**, los usuarios pueden:

- Almacenar y gestionar de forma segura todas sus claves digitales en un solo lugar.
- Acceder sin problemas a espacios corporativos y privados, en cualquier momento y lugar.
- Experimentar una funcionalidad sencilla, similar a la de una tarjeta, directamente en el iPhone o Apple Watch, sin necesidad de tarjetas de plástico.
- Disfrutar de las ventajas de la tecnología NFC y del modo Express, sin necesidad de desbloquear el dispositivo.
- Tenga siempre acceso incluso con batería baja, Power Reserve mantiene sus llaves funcionales hasta cinco horas.
- Disponer de una solución de gestión de accesos para el futuro.

La gestión segura de credenciales nunca ha sido tan fácil.

La tecnología de **LEGIC** garantiza la entrega segura de credenciales a Apple Wallet, donde se pueden almacenar, actualizar y gestionar con facilidad.

+información

NUEVO RETO

PARA LOS INGENIEROS DE SEGURIDAD

Alfonso
Bilbao Iglesias

MIEMBRO DE **AEINSE**
alfonsobicg@gmail.com

El nuevo entorno

Hace unos 20 años se produjo un cambio gradual, pero sin vuelta atrás, de la sustitución de las cámaras de televisión analógicas por otras digitales y, sobre todo, de la sustitución de los cableados analógicos y coaxiales por el uso generalizado de las redes ethernet. Las infraestructuras de los Sistemas de Seguridad que proyectábamos, instalábamos y poníamos en marcha los ingenieros de Seguridad estaban cambiando rápidamente.

Inicialmente pedimos ayuda a las empresas que instalaban redes digitales para oficinas y entidades financieras, y poco a poco fuimos adquiriendo los conocimientos para saber dimensionar y parametrizar ese tipo de redes que invadían todos los Sistemas de Seguridad. Hoy la digitalización afecta a todos los equipos y Sistemas de Seguridad, y forma parte del ecosistema técnico en el que nos desenvolvemos.

También de forma gradual, sin vuelta atrás y más aceleradamente, las ciberamenazas a los Sistemas de Seguridad están obligando (aunque aún sin reflejo en la legislación aplicable) a la implantación de medidas de Ciberseguridad en estos Sistemas.

También, al igual que cuando comenzó la digitalización, en las empresas usuarias hay departamentos que tiene algo que decir. En el pasado los departamentos de Informática solían influir, e incluso determinar, que electrónica de red había que utilizar en los Sistemas de Seguridad y, en muchos caos, o lo instalaban sus proveedores habituales de redes, o incluían la red en su mantenimiento específico. En casi todos los casos se trató de una colaboración entre los Departamentos de Informática y los de Seguridad de las empresas usuarias.

En el tema de la Ciberseguridad a implantar, lo más deseable (y no siempre ocurre) es que se dé una colaboración estrecha entre el Departamento o Dirección de Ciberseguridad y el Departamento de Seguridad (física). Los procedimientos, soluciones y equipos específicos de Ciberseguridad han de ser coherentes con los existentes entre el resto de las infraestructuras informáticas de la empresa.

En cualquier caso, los Ingenieros de Seguridad que proyecten, instalen o administren los Sistemas de Seguridad, han de incorporar a sus conocimientos los suficientes de Ciberseguridad que les permitan, cada vez con más profundidad, contar con la Ciberseguridad en todo lo referente a su actividad, interactúen o no, con los Departamentos de Ciberseguridad de las empresas propietarias de los Sistemas, o con las empresas de Ciberseguridad que den servicio a esas empresas.

Por otra parte, los fabricantes y distribuidores de equipos y aplicaciones de Seguridad están ya implementando medidas de Ciberseguridad en ellos, pendientes de normativa internacional que se está desarrollando más lentamente de lo deseable.

Herramientas para los Ingenieros de Seguridad

Obviamente uno de los pasos evidentes para la adecuación de los Ingenieros de Seguridad a este nuevo entorno es la adquisición de conocimientos de Ciberseguridad de forma académica. Existen numerosos másteres de diferente profundidad, en universidades públicas y privadas, que pueden ser muy adecuados, además de múltiples cursos especializados en asociaciones, empresas de consultoría, etc. Es totalmente recomendable acudir a esta iniciación inmediata. Se trata de entender las nuevas amenazas, las medidas de Ciberseguridad a considerar, el entorno regulatorio, etc. y cómo tener en cuenta todo esto en nuestro trabajo de ingenieros.

Independientemente de este aterrizaje en la nueva tecnología a incorporar a nuestro bagaje personal existen dos documentos de gran interés a tener en cuenta, que nos pueden ayudar a enfocar la implantación de la Ciberseguridad en los Sistemas de Seguridad, los de nuevo diseño e implantación, y los existentes que requerirán también disponer de Ciberseguridad ante las nuevas amenazas.

Estos dos documentos, en los que tuve la fortuna de participar al igual que otros miembros de **AEINSE** (muy destacadamente **Raúl Aguilera**), tienen distinto origen. El primero cronológicamente es el **"AEINSE 10/21 Guía de buenas prácticas de Ciberseguridad en Proyectos de Seguridad Física",** redactado por varios miembros de nuestra Asociación en 2021 y presentado en una sesión técnica en **SICUR** en 2022. Nos referiremos en adelante a él como **"Guía 10/21 de AEINSE"**.

El otro documento es el emitido por el **Foro Nacional de Ciberseguridad (FNC)** en 2024 **"La gestión de la Ciberseguridad en los Sistemas de Seguridad Física. Recomendaciones y casos de uso"**. En él han participado además de ingenieros del entorno de la Seguridad Física (vario de ellos miembros de **AEINSE**), ingenieros y especialistas de Ciberseguridad, funcionarios de la Administración, profesores de Universidad, etc. Ha sido una experiencia importante de colaboración muy transversal. A diferencia de la **Guía de AEINSE**, va dirigido tanto a los técnicos y responsables de Seguridad Física como a los de Ciberseguridad, en un esfuerzo de hacer de "puente" entre ambas especialidades. Nos referiremos a este documento como **"Recomendaciones del FNC".**

El uso de los documentos de referencia

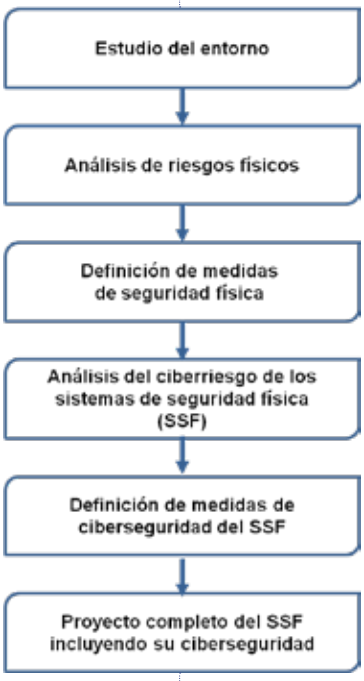
Ambos documentos, de descarga gratuita, incluyen unas descripciones excelentes del alcance del reto tecnológico a afrontar y de dotar al lector poco avezado en la **Ciberseguridad** de una introducción muy adecuada al contexto general de la nueva situación.

Entre ambos sectores de la **Seguridad Física** y la **Ciberseguridad** hay muchas similitudes, pero hay algunas diferencias importantes, además de las terminológicas, fundamentalmente relacionadas con el tipo de soluciones (denominada "medidas" de Seguridad en nuestro entorno y "salvaguardas" en el de la **Ciberseguridad**), dependientes a su vez de la diferente naturaleza de las amenazas que atienden.

En la **Seguridad Física** las amenazas se producen físicamente donde están las personas o los bienes a proteger, y son específicas para ese riesgo que se pretende contrarrestar. El momento del día en que se producen, el lugar, el ambiente sociológico, el tipo de agresor que se espera, etc. determinan un análisis de riesgos concreto que determina a su vez las medidas físicas (el diseño del Sistema de Seguridad), unas medidas operativas (disposición y funciones de los vigilantes, CRA...) y los procedimientos a aplicar.

En el entorno de la **Ciberseguridad** las amenazas tienen origen en cualquier lugar del mundo, no en las proximidades de los activos a proteger. El momento en el que se produzca la agresión no se tiene en cuenta en el análisis de riesgos y, en general, la disposición de las salvaguardas a implementar están relacionadas con el inventario de recursos a proteger (hardware, aplicaciones, bases de datos, continuidad de los procesos) y su importancia en la funcionalidad que se espera de ellos.

Teniendo en cuenta estas diferencias, una buena forma de aplicar los contenidos de ambos documentos puede ser la siguiente:



GUÍA 10/21
de AEINSE

Introducción y Artículo 1

La ciberseguridad en los Sistemas de Seguridad Física.

Buena introducción al tema. Recomendable su lectura.

Artículo 2

Afrontar proyectos de Sistemas de Seguridad Física.

Se expone la necesidad de seguir un ciclo concreto para determinar las medidas de Seguridad y Ciberseguridad. Se parte del Análisis de Riesgos de amenazas físicas para determinar el Sistema de Seguridad Física y sobre el Sistema definido realizar el Análisis de Ciberriesgos para determinar las salvaguardas.

Artículo 3

El riesgo IT de los Sistemas de Seguridad Física.

En este artículo, donde se expone la forma de realizar el Análisis de Riesgos de la Ciberseguridad a aplicar, es donde es recomendable que se siga con más detalle lo expuesto en el documento Recomendaciones del FNC. La razón es que, como se verá a continuación, el documento del FCN realiza un Análisis de Ciberseguridad genérico de los Sistemas de Seguridad Física, de forma que termina dando una lista de salvaguardas de Ciberseguridad a implantar en los diferentes tipos de elementos de un Sistema de Seguridad Física, matizados por el tipo de activos a los que protege (grados de Seguridad).

Artículo 4

Implementar una arquitectura segura: especificaciones de medidas de Ciberseguridad.

También sugerimos que, aunque se lea con atención para comprender la naturaleza de las medidas de Ciberseguridad a tratar, se utilice de forma más práctica las disposiciones del documento de Recomendaciones del FNC.

Artículo 5

Ingeniería y consultoría de Seguridad.

Muy recomendable como guía de estrategias comerciales a seguir en el nuevo entorno en el que nos movemos los ingenieros.

Artículo 6

Bibliografía. – Para saber más.

RECOMENDACIONES FCN

1 Resumen ejecutivo y 2 Necesidad y oportunidad

Muy útiles para enfocar el problema, tanto para los ingenieros de Seguridad como para los usuarios y técnicos de Ciberseguridad que van a tener en cuenta unos activos nuevos, los Sistemas de Seguridad Física, a proteger frente a los Ciberriesgos.

Artículo 3: Sistemas de Seguridad Física. Análisis del ámbito

Determinación de en qué consisten los Sistemas de Seguridad a considerar, tanto las CRA como los que disponen de un Centro de Control de una cierta entidad. Centra el objetivo de lo que se va a tratar y es fundamental para la comprensión por parte de los gestores y técnicos de Ciberseguridad del alcance y ámbito de los Sistemas de Seguridad Física a proteger.

Artículo 4: Análisis de Ciberriesgos

En él se expone el Análisis de Riesgos de Ciberseguridad a realizar. No se plantea que se haga en cada caso de forma sistemática para cada Sistema de Ciberseguridad a aplicar, sino que se propone como justificación de la lista de salvaguardas que se van a plantear (una especie de "check list") para los Sistemas de Ciberseguridad en función de la arquitectura informática y los componentes que incorporen. Igual que en la Universidad nos hacían aprender la demostración de las ecuaciones de Maxwell en lugar de hacernos memorizarlas sin más, en este apartado nos exponen de dónde vienen las medidas que nos proponen aplicar.

Artículo 5: Medidas de Ciberseguridad

Este es el **artículo fundamental**. Es de especial interés la tabla que relaciona las medidas de Ciberseguridad a aplicar para cada subsistema de Seguridad Física en función del grado de Seguridad (que a su vez lo relaciona con el nivel de exigencia a aplicar por la legislación de Seguridad Privada). Se debe acudir a los anexos para entender bien lo que se expone en la tabla.

Artículo 6: Casos de uso

Relación de ejemplos comentados de ataques de Ciberseguridad a Sistemas de Seguridad Física y cómo reaccionarían las medidas de Ciberseguridad a disponer. De gran interés.

Artículo 7: Documentos de referencia

Para saber más.

Artículo 8: Glosario

Muy útil para los técnicos y gestores de ambos ámbitos, el de la Seguridad Física y el de la Ciberseguridad.

Anexo I Catálogo de amenazas

Fundamental lectura, para entender con la terminología oficial de qué hay que defender a los Sistemas de Seguridad Física.

Anexo II Marco de referencia general de medidas de Ciberseguridad

La parte nuclear de la información sobre qué medidas hay que implementar en los Sistemas de Seguridad Física. Ya sea para el diálogo con el departamento de Ciberseguridad de las empresas usuarias o para tenerlas en cuenta en los materiales y equipos a seleccionar y en los procedimientos a disponer.

Entre las medidas que se describen en este Anexo hay que tener en cuenta que las correspondientes al Marco Organizativo y al Marco operacional han de ser implantadas por la empresa usuaria, con sus buenas prácticas muy probablemente derivadas de su propio Departamento de Ciberseguridad, pero que han de ser complementadas por los procedimientos a entregar al final de la instalación por parte de la Ingeniería o la empresa instaladora. Las medidas derivadas de las descritas en los apartados Medidas de protección y Medidas de productos están muy relacionadas con medidas inherentes a la propia arquitectura del Sistema y a la infraestructura de este, así como a la certificación adecuada en términos de Ciberseguridad de los elementos del Sistema de Seguridad.

Este último aspecto es una parte fundamental de los pasos pendientes a dar en la madurez de la Ciberseguridad. Se necesita un conjunto de normas y certificaciones sobre los elementos de todo tipo a conectar a redes digitales. Estas normas son parte de la misión de ENISA (Agencia de la Unión Europea para la Ciberseguridad) que se están desarrollando en la actualidad y, por parte española, en la labor del CCN (Centro Criptológico Nacional) a través de su labor de certificación. Actualmente están empezando a certificarse elementos de diferentes fabricantes de Seguridad Física. Es para ello de gran utilidad consultar el catálogo CPSTIC del CCN (Catálogo de Productos y Servicios de Seguridad de la Tecnología de la Información).

Sin duda, nos toca hincar los codos y volver a reciclarnos como ingenieros.
Nadie dijo que iba a ser fácil.

REFERENCIAS:

- **AEINSE 10/21 Guía de buenas prácticas de Ciberseguridad en Proyectos de Seguridad Física.**- https://www.aeinse.es/system/files/documentos/AEINSE%2010-%2021%20Gu%C3%A-Da%20de%20buenas%20pr%C3%A1cticas%20de%20ciberseguridad%20en%20SF_0.pdf
- **La gestión de la Ciberseguridad en los Sistemas de Seguridad Física. Recomendaciones y casos de uso.**- https://foronacionalciberseguridad.es/index.php/documentacion/publico/129-gestion-de-la-ciberseguridad-de-los-sistemas-de-seguridad-fisica-2024/file
- **Foro de Ciberseguridad Nacional.**- https://foronacionalciberseguridad.es/
- **ENISA.**- https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_es
- **CCN / CPSTIC** - Actualizado el Catálogo de Productos y Servicios de Seguridad TIC del Centro Criptológico Nacional - Centro Criptológico Nacional - CNI

CONOCE A UNA

SOCIA

Mª Dolores Álvarez

SOCIO Nº 147

mdalvarez@tis-trablisa.es

Buenos días Lola, por favor dinos algo de ti para empezar a conocerte.
Tengo 50 años, andaluza, de Jaén, pero vivo en Sevilla desde que tenía 22 años que comencé a trabajar y tuve que trasladarme. Casada, y madre de 3 hijos de 21, 18 y 16 años que son el mayor logro conseguido en mi vida.

Eres socia de AEINSE desde hace algún tiempo ¿Qué te movió a asociarte?
Me pareció muy interesante el concepto de Ingeniero de Seguridad. En este sector encontramos a veces, que cualquier persona es apta para asesorar sobre seguridad, y creo que se debe reforzar el valor de ingeniero especializado que profesionalice el sector aún más y **AEINSE** contribuye a esta idea.

¿Cuál es tu formación académica?
Ingeniero Técnico Industrial en la especialidad Electrónica Industrial. Estudié en la Escuela Politécnica Superior de Jaén y finalicé mis estudios en el año 1996. También soy Directora de Seguridad desde hace casi 10 años y tengo cursos de especialización en Seguridad para Infraestructuras Críticas.

¿En qué empresas has desarrollado tu carrera profesional y con qué responsabilidades?
Con 22 años comencé a trabajar en **Gas Natural** como gestor comercial. Esta etapa duró 4 años muy gratificantes, pero por motivos personales decidí abandonar la empresa.

Empecé como Ingeniero Comercial en **Fichet Sistemas y Servicios** en el año 2001 empresa de instalaciones y mantenimiento de seguridad electrónica y vinculada al producto de seguridad física (cajas fuertes, producto acorazado, etc.).

Posteriormente la empresa fue comprada por el **Grupo Multinacional Gunnebo** y hace 5 años Gunnebo España, fue adquirida por el **grupo Trablisa** empresa de seguridad global que integra la vigilancia con las soluciones avanzadas de seguridad electrónica. **Trablisa Integrated Security** que es la empresa a la que pertenezco, desarrolla las soluciones de tecnología en instalaciones, mantenimiento y SOC.

En las diferentes etapas profesionales, siempre he estado vinculada al departamento comercial, pero mi cualificación técnica y conocimientos me han permitido desarrollar más facetas en la empresa, prescripción técnica, elaboración de proyectos, formación específica sobre producto físico.

Actualmente y desde hace años, desempeño el puesto de **Key Account Manager clientes Nacionales** en **Trablisa Tecnología**, realizando también apoyo a Andalucía. Gestiono cuentas claves para mi empresa y desarrollo nuevos clientes.

Una parte muy importante en mi trabajo son los proyectos sobre soluciones de compartimentación de alta seguridad, blindajes para recintos críticos y esclusas. Además, estoy inmersa en un proyecto de desarrollo de negocio de Trablisa en Andalucía.

En tu etapa en Gas Natural (hoy Naturgy) entre las empresas instaladoras que gestionabas ¿Había empresas de seguridad?

En esta etapa trabajé con empresas instaladoras de gas. Ello me sirvió para iniciarme en el mundo de las multinacionales y en la parte comercial ya que gestionaba grandes contratas. Fue muy enriquecedor este comienzo en el mundo laboral.

¿Qué te llevó a moverte al sector de la seguridad y qué te mantiene en él?

Llegué por casualidad con 26 años a **Fichet**, desconocía totalmente el sector pero me pareció muy interesante. Por aquel entonces, un grupo de ingenieros de la empresa, empezamos a desarrollar otra forma de hacer las ofertas que presentábamos a los clientes, dando el valor añadido de proyecto técnico a las ofertas que por entonces no se hacía. Considero que fuimos pioneros en esto.

Lo que me mantiene en seguridad, creo que es la continua evolución de este sector que permite no aburrirte y seguir aprendiendo.

Has vivido la evolución, desde Fichet a Trablisa, de una de las empresas históricas del sector de la seguridad. Aunque siempre vinculada al departamento comercial, seguramente se han producido muchos cambios y adaptarse y compatibilizarlo con la crianza de los niños siempre es duro ¿Cómo los viviste?

Tengo que decir, que los primeros años profesionales en **Fichet** y **Gunnebo**, fueron algo duros, ya que tenía que compatibilizar, que no es fácil, la maternidad con 3 hijos pequeños y sin ayuda familiar, con un trabajo exigente en la empresa privada. Por entonces no estaba tan extendido el concepto de conciliación y las mujeres teníamos que hacer auténticos malabares para poder llegar a todo, sentirnos excelentes en nuestro trabajo y buenas madres...

Por poner un toque de humor, recuerdo anécdotas, por ejemplo, estar controlando la olla haciendo potitos y al mismo tiempo ultimando detalles de un proyecto de seguridad para entregar urgente... o haciendo un disfraz de madrugada después de un viaje de trabajo.... con organización y mucho trabajo fui superando todas las etapas.

Ahora en **Trablisa** con mis hijos mayores puedo ejercer el trabajo de una forma más sosegada aunque los momentos de estrés no faltan nunca.

Como gestora de grandes clientes ¿Qué aspecto crees que éstos valoran más de sus empresas proveedoras?

En la fase de oferta, considero que lo más valorado es la calidad de la oferta técnica. Esta debe estar bien argumentada, la solución aportada debe cubrir las necesidades planteadas y correctamente definidos los apartados de descripción de la instalación, plazo de ejecución y planificación de la misma. Sin lugar a dudas, la oferta técnica debe venir acompañada de un precio adecuado porque es muy frecuente la comparativa con otras empresas.

En la fase de ejecución una vez la oferta es aceptada, lo que más valora el cliente es el correcto desarrollo de la ejecución de dicha instalación o servicio de mantenimiento. Esto es fundamental para los clientes, que la ejecución se realice conforme a lo pactado (en tiempo y forma) y que el servicio sea eficiente y adecuado (tratamiento de averías rápido, mantenimientos en plazos, etc.).

En resumen, como gestora de clientes, puedo afirmar que la calidad del servicio es lo más valorado por el cliente y lo que permite que una empresa proveedora se consolide en un cliente.

Tienes experiencia en los medios de protección físicos y electrónicos. ¿crees que van de la mano en las instalaciones o, por el contrario, se planifican de forma separada?
Por supuesto que deberían ir de la mano. La primera barrera de entrada a un recinto crítico es la puerta por lo que debe cumplir con requerimientos de seguridad apropiados. Además estos elementos llevan también componentes electrónicos, ya que se vinculan al control de accesos.

Tener correctamente protegida la entrada natural a un recinto crítico (puerta o esclusa), o blindar unas paredes, debe reunir unos requisitos de protección y seguridad similares a los de seguridad electrónica. Resumiendo, deben planificarse de forma conjunta.

Una curiosidad. Me ha llamado la atención al ver tu currículum que para ADIF eres prescriptora de soluciones de puertas especiales para túneles. ¿túneles por los que pasan los trenes? ¿Y también desarrolláis soluciones de otro tipo de puertas y esclusas para Infraestructuras Críticas?
Efectivamente, fabricamos e instalamos puertas para túneles por donde circulan trenes.

En **Trablisa Integrated Security** desarrollamos hace años (cuando erámos **Gunnebo**) una solución propia y ensayada de puertas certificadas para protección contra incendios y además resistentes a la sobrepresión (la sobrepresión que generan los trenes a su paso por los túneles). Estas puertas se instalan en los túneles de alta velocidad como salidas de emergencia para evacuación de personas.

En otras infraestructuras críticas, instalamos puertas y esclusas antibala, antiefracción, antiexplosión o combinadas. Estas soluciones son totalmente a medida con un alto componente de diseño, ingeniería y conocimiento de la normativa propia.

En tu opinión ¿crees que en las ofertas se da el protagonismo que merece a los aspectos relacionados con el proyecto e ingeniería? ¿El cliente se interesa por ello? ¿lo valora?
Como expliqué antes, comencé en el sector como Ingeniero Comercial y para mí es fundamental, y creo que los clientes valoran cada vez más el componente proyecto y como se presenta al cliente la oferta de seguridad. En este sector hay una continua evolución y las empresas instaladoras debemos tener ingenieros que sepan proyectar y dar la solución idónea al cliente basada en un análisis adecuado de necesidades y mejor propuesta tecnológica del mercado. En **Trablisa** se ha apostado por esto creando un departamento de ingeniería importante.

¿Cómo te ves profesionalmente en el futuro?
Veo mi futuro profesional, vinculada a la seguridad. La experiencia y conocimientos en esta especialidad hacen que me sienta cómoda y quiera seguir enfocándome y desarrollándome en este sector. Por otra parte mi empresa **Trablisa** quiere desarrollar el negocio en Andalucía de una forma integral y me veo con la ilusión para formar parte de este proyecto en los próximos años.

Bueno, ya hemos hablado bastante de trabajo ¿Qué otras actividades te satisface realizar?
Sobre mis aficiones, tengo muchas, mi carácter sumamente inquieto ayuda a que en mis ratos libres haga muchas cosas. El deporte es imprescindible para recargar pilas a diario (natación, Hit...) y también pasear a mi chihuahua cuando puedo, es un momento relax...

Un viaje en familia al extranjero al año es obligatorio y muy deseado... Y tengo que decir, que me gusta aprender y probar a hacer cosas nuevas y variopintas, lo último bailar flamenco, la costura y la restauración de muebles.

Finalmente, ¿Tienes alguna sugerencia que nos ayude a mejorar la visibilidad de la asociación y a aportar mayor valor a los socios?
La visibilidad de **AEINSE** es cada vez mayor, es importante estar en los foros de seguridad y en todos los eventos importantes del sector y esto se está haciendo gracias al esfuerzo de la Junta Directiva y de algunos socios muy involucrados.

Se me ocurre como iniciativa para aportar valor a los socios, el promover jornadas pequeñas formativas Teams para abordar novedades técnicas, de normativa, de producto.

Estas jornadas podrían ser impartidas por los propios integrantes de la asociación o patrocinadores para enriquecernos todos de los conocimientos que puede aportar cada asociado / patrocinador, ya que cada uno podemos ser experto en una materia, crear vínculos profesionales y enriquecernos todos.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

JUN
4 y 5

Security Forum'25

Los días 4 y 5 de junio próximos, tendrá lugar en Las Drassanes Reials de Barcelona la 12ª edición de Security Forum, evento en el que las empresas participantes mostrarán las soluciones, dispositivos e innovaciones tecnológicas pioneras y destacadas del sector de la seguridad.

El día 4 se celebrará simultáneamente el Congreso Security Forum con ponencias y mesas de debate relacionadas con las nuevas normativas y la inteligencia artificial entre otros temas.

Un día después, se celebrará el **II Congreso de Seguridad en Espacios Públicos de Barcelona**, donde se abor darán entre otros aspectos, la ciberseguridad en la Administración local, así como intervenciones sobre tecnologías aplicadas a los espacios públicos.

registro visitantes

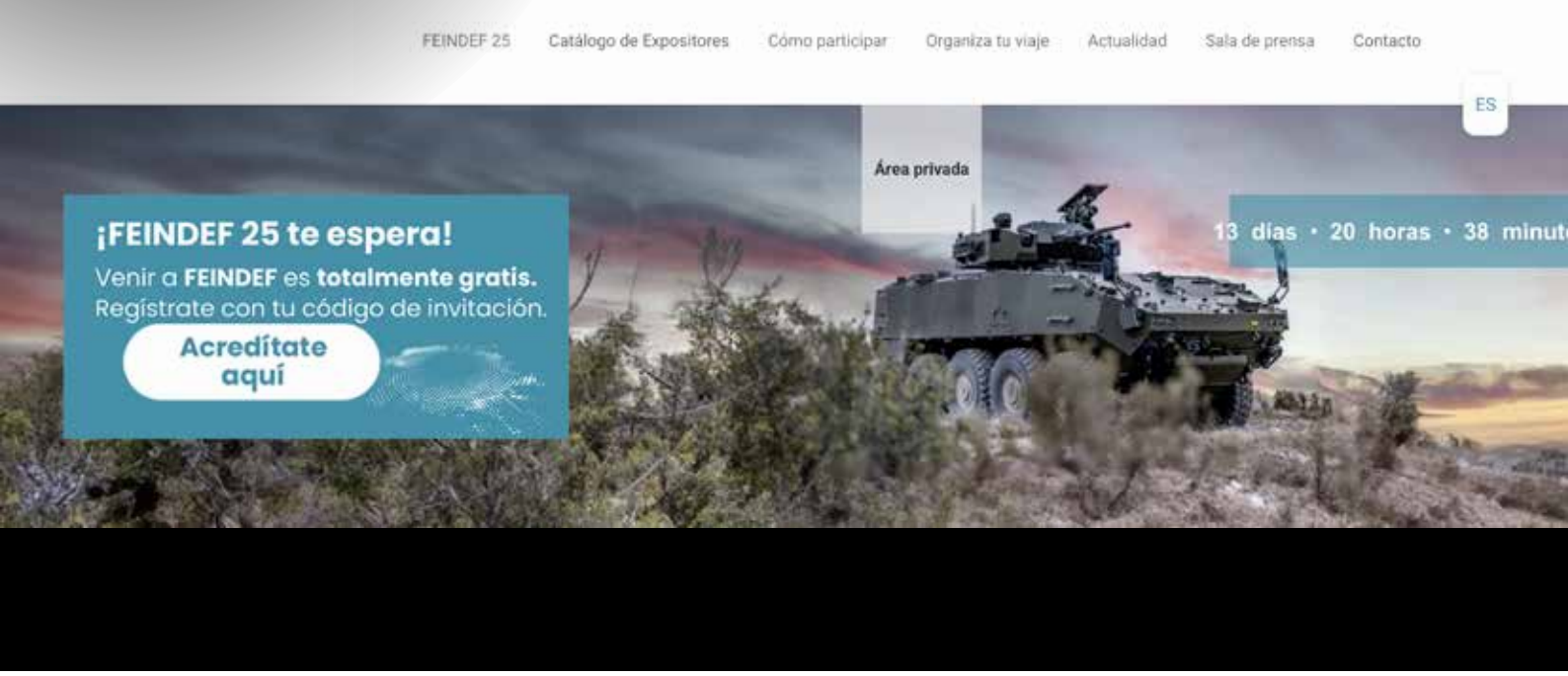
AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

FEINDEF 25

FERIA INTERNACIONAL DE DEFENSA Y SEGURIDAD DE ESPAÑA



Organizada por la Fundación FEINDEF y apoyada institucionalmente por el Ministerio de Defensa, se celebrará los días 12, 13 y 14 de mayo próximos en el recinto de IFEMA (Madrid) la IV Feria Internacional de Defensa y Seguridad de España (Feindef).

Con **más de 500 expositores**, de los que el **35% son internacionales**, la feria se consolida como el escaparate de referencia del sector para la proyección de nuestras empresas y organizaciones en el mercado internacional.

Además del espacio expositivo, tendrán lugar ciclos de de conferencias, talleres y mesas redondas dirigidas por expertos y autoridades destacadas, que abordarán las últimas tendencias en áreas cruciales como ciberdefensa y ciberseguridad, economía circular, eficiencia energética y sostenibilidad, bases logísticas inteligentes, tecnologías disruptivas o el papel imprescindible de las mujeres en la industria de defensa y seguridad.

registro visitantes

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

12º Congreso Protección, Resiliencia y Ciberseguridad

Organizado por la Fundación Borredá, con la colaboración de Seguritecnia y Red Seguridad, esta nueva edición del tradicional Congreso de Protección de Infraestructuras Críticas (PIC) estará dedicado al impacto que tendrá la normativa NIS2 y CER en materia de Prevención, Resiliencia y Ciberseguridad de las entidades importantes y críticas.

Se pondrá el foco el día **6 de mayo** en la **NIS2** y el día **7 de mayo** en la **CER** y tendrá lugar en el **auditorio CECABANK** en Madrid C/ Caballero de Gracia, 2.

La asistencia es gratuita para Administración Pública, RSE, RSI, CISO, CSO, FCS y amigos de la Fundación Borredá, para el resto de profesionales el **importe de la inscripción general es de 160 euros** e **incluye el acceso a los dos días.**

inscripción

LEÍDO, VISTO Y OÍDO EN...

Estudio @aslan 2025 IA

TODO CAMBIA...

"La historia de la Inteligencia Artificial no comenzó en 2018 con ChatGPT. La IA lleva casi 80 años siendo una eterna promesa que, ahora sí, se está haciendo realidad y está provocando una disrupción enorme en el mundo de la tecnología y las empresas.

Esta revolución actual de la IA posiblemente haga que muchas tareas e incluso perfiles profesionales, profesiones enteras y empresas tengan que reinventarse por completo".

¿Quiere saber lo fundamental sobre IA, qué expectativas tienen los principales responsables de empresas de tecnología en España y cómo le puede afectar?

https://aslan.es/estudio-aslan-ia-todo-cambia/

LEÍDO, VISTO Y OÍDO EN...

IEEE Spectrum

9 intrigantes hazañas de ingeniería para 2025

Informe Especial Top Tech 2025 de IEEE Spectrum

Mediciones de metano para las masas

"Desde lo alto de nosotros, los satélites rastrean las emisiones devastadoras de los gases de efecto invernadero que alterarán nuestro clima. Hasta ahora, sus datos han sido privados, compartidos solo con empresas o gobiernos. ***MethaneSAT*** *está cambiando eso. Lanzado el 4 de marzo de 2024, identificará áreas problemáticas específicas y hará un seguimiento más amplio de las emisiones de metano. Cualquiera podrá acceder a estos datos cuando el satélite esté en pleno funcionamiento, a principios de 2025..."*

Leer el artículo completo: **aquí**