



## Entrevista socio

Eva Pastor Sánchez

## Calendario de eventos ADSI

## "Martes con ..."

Cruz Roja  
CCMA 3-CAT

## Junta Directiva

### Presidente

Eduard Zamora

### Vicepresidenta

Elvira Márquez

### Secretario

David Sanmartín

### Tesorero

Emilio Herrero

### Vocales

Francesc Chía

Joan Figuera

Isabel García

Oscar Molins

Míriam Pérez

Macarena Ramisa

Joan Roda

Jordi Silvestre

Oriol Verdura

## En este número ...

### 3

#### PATROCINADORES ADSI

### 4

#### CARTA DEL PRESIDENTE

### 5

#### AGENDA DE EVENTOS

### 6

#### ARTÍCULO DE OPINIÓN

- El impacto de la inteligencia artificial en el mundo de la seguridad

### 8

#### ENTREVISTA A UN SOCIO

### 10

#### ARTÍCULO DE OPINIÓN

- Trump ¿ha llegado el momento para una defensa, inteligencia y seguridad europeas?

### 16

#### NOTICIAS ADSI

- SEDEXPO 2025, seguridad, defensa y emergencias
- Security Forum 2025 compartirá fecha con II edición del Congreso de Seguridad en espacios públicos de Barcelona
- ADSI en la cena anual y entrega de premios de ADSP-Associação dos Directores de Segurança de Portugal

- Convocatoria para concesión de menciones de seguridad privada en Cataluña año 2024

- Informe sobre Tecnologías Biométricas Seguras para el Control de Acceso

- ADSI en la XXXVII Edición de los Trofeos de Seguridad de la revista SEGURITECNIA

- "Martes con" Cruz Roja Española

- "Martes con" Corporació Catalana de Mitjans Audiovisuals -3CAT

- Actualización de datos

### 27

#### NUESTROS PATROCINADORES

- AXIS
- IMAN
- SCATI
- PUERTAS GISMERO
- BY DEMES

### 36

#### FORMACIÓN

### 38

#### REVISTAS Y ENLACES DE INTERÉS

### 39

#### LECTURA RECOMENDADA

La opinión manifestada por los autores de los artículos publicados a título personal que se publican en este medio informativo no necesariamente se corresponde con la de ADSI como Asociación.

Esta comunicación se le envía a partir de los datos de contacto que nos ha facilitado. Si desea cambiar su dirección de correo electrónico dirija su petición por correo postal a "ADSI -Asociación de Directivos de Seguridad Integral", Gran Via de Les Corts Catalanes, 373 – 385, 4ª planta, local B2, Centro Comercial "Arenas de Barcelona", 08015 -Barcelona, o mediante e-mail a [vicepresidente@adsi.pro](mailto:vicepresidente@adsi.pro)

Si o no desea recibir nuestros mensajes informativos utilice los mismos medios, haciendo constar como asunto "DAR DE BAJA". Su petición será efectiva en un máximo de diez días hábiles.



|                                                                                                                                   |                                                                                     |                                                                                      |                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <br>Soluciones en control de accesos y seguridad |    |    |    |
|                                                  |    |    |    |
|                                                  |    |    |    |
|                                                  |   |    |    |
|                                                |  |  |  |
|                                                |  |  |  |
|                                                |  |  |  |
|                                                |  |  |  |
|                                                |                                                                                     |                                                                                      |                                                                                       |



## Lo mejor para todos en estas Fiestas y para el 2025

Cerramos un año que podemos calificar positiva o negativamente en función del aspecto del que tratemos. Si lo hacemos desde la visión de los afectados por el desastre provocado por la DANA en el levante español, así como de todos aquellos que han perdido personas importantes en sus vidas, o bienes muebles e inmuebles vitales para su día a día, en esta catástrofe sin parangón o por cualquier otra circunstancia en cualquier otra parte del país, sin duda el 2024 va a ser notoriamente negativo. Nuestros mejores deseos de pronta recuperación y ánimos para todos ellos.

Desde otros puntos de mira, para muchos habrá sido un año positivo y cabe felicitarlos por ello, como sin duda es el caso de nuestra asociación, que ante el inminente final de año no cabe más que valorar de muy positivo el ejercicio que cerramos, tanto por el incremento de asociados, la captación de jóvenes del sector, el récord en nuestra ya extensa historia del número de patrocinadores, las muy numerosas e interesantes actividades desarrolladas en nuestros "Martes con...", la colaboración con otras asociaciones y entidades importantes del sector, etc., etc.

El ingente trabajo de nuestra Junta Directiva ha contribuido, un año más, a seguir superándonos en el desarrollo de los objetivos de ADSI y, un año más, esperamos vuestra ayuda en la aportación y apertura de contactos sobre ideas de actividades y mejoras a desarrollar e implantar en 2025.

La asamblea de finales de marzo puede ser un buen momento para debatir sobre ello, aunque para todos aquellos que no podréis estar presentes, por realizarse en Barcelona, sede social de ADSI, o por cualquier otra circunstancia, nos ponemos a vuestra disposición para valorar las propuestas que nos hagáis llegar.

Deseamos que estas fiestas navideñas y el inicio del nuevo año sea lo más prometedor posible para las circunstancias personales y entornos familiares de cada uno de vosotros, que con todo lo grave ocurrido en 2024 tendremos una variedad de situaciones muy dispar, con deseos tan diversos como lo serán las situaciones personales de cada uno.



Para todos, sin excepción, lo mejor en estos días tan entrañables y las mejores expectativas para el inmediato 2025.

ADSI trabajará un ejercicio más a plena capacidad, con las limitaciones que nuestra organización y recursos nos permiten, pero que serán superadas, sin duda, por la ilusionante dedicación de los integrantes de Junta en favorecer al colectivo de la seguridad del país. ■

## ¡Felices Fiestas!

### ¡Y un magnífico 2025 para todos vosotros, para vuestras familias y equipos de trabajo!



Aunque recibiréis información de cada evento con antelación a su desarrollo para formalizar las inscripciones, os detallamos los eventos que organiza ADSI en exclusiva, los que coorganiza con otra entidad y los organizados por terceros en los que ADSI tiene una participación activa de algún integrante de Junta o socio. Anotadlos en vuestra agenda.

### Eventos organizados en exclusiva por ADSI

#### 📍 "Martes con..." en BARCELONA

- 21 enero: *Catedral de Barcelona*

#### 📍 "ADSI con..." en MADRID

- Jueves, 6 febrero: *Real Madrid C.F.*

#### 📍 Asamblea de socios ADSI en BARCELONA

- Jueves, 20 marzo: *Lugar por determinar*

#### 📍 "Martes con..." en BARCELONA

- 8 abril: TMB-Transports de Barcelona (red de autobuses de Barcelona)

Seguimos trabajando para completar el calendario de actividades y "Martes con..." del 2025.

Os agradecemos toda propuesta en la que nos podáis ayudar a través de vuestros contactos.

### Organizados por terceros en los que ADSI tiene una participación activa

📍 26 a 28 marzo 2025: **II SEDEXPO**, *Feira Galicia - Silleda*

📍 4 y 5 junio 2025: **11º Security Forum**, *Atarazanas Reales - Barcelona*



## Hazte socio de ADSI

### ¿Quieres ser Socio de ADSI – Asociación de Directivos de Seguridad Integral?

Para iniciar el proceso de alta como Asociado, envíe un email a [vicepresidente@adsi.pro](mailto:vicepresidente@adsi.pro), indicando nombre y apellidos, una dirección de correo y un teléfono de contacto.

En cuanto recibamos su solicitud le enviaremos el formulario de Solicitud de Admisión.

### ¿Quién puede ser socio de ADSI?

- Quien esté en posesión de la titulación profesional de Seguridad Privada reconocida por el Ministerio del Interior (T.I.P. de Director de Seguridad, Jefe de Seguridad, Detective Privado o Acreditación de Profesor de Seguridad Privada).
- Todo Directivo de Seguridad que posea, a criterio de la Junta Directiva de la Asociación, una reconocida y meritoria trayectoria dentro del sector.



# El impacto de la inteligencia artificial en el mundo de la seguridad

Por **Oriol Verdura**, vocal de ADSI

En la última década, la inteligencia artificial (IA) ha transformado numerosos sectores de la sociedad, y el ámbito de la seguridad no ha sido la excepción. La IA ha logrado integrarse profundamente en sistemas de videovigilancia, alarmas, control de accesos y protección de activos, cambiando la forma en que las organizaciones y los individuos se protegen ante amenazas potenciales. Estos avances no solo han mejorado la eficiencia y eficacia de los sistemas de seguridad actuales, sino que también han permitido una capacidad de respuesta más rápida y precisa, elevando los estándares de protección.

Uno de los usos más significativos de la IA en seguridad es en los sistemas de videovigilancia. Tradicionalmente, estos sistemas dependían de la intervención humana para monitorear cámaras en tiempo real y detectar actividades sospechosas. Sin embargo, la IA ha automatizado este proceso. Gracias al aprendizaje automático y a la visión por computadora, los sistemas de videovigilancia pueden analizar de manera autónoma grandes cantidades de datos visuales, identificar comportamientos anómalos o potencialmente peligrosos y emitir alertas en tiempo real. Por ejemplo, en espacios públicos o empresas, la IA puede detectar situaciones como la presencia de objetos abandonados, movimientos inusuales o incluso podría identificar rostros de personas con antecedentes delictivos, mejorando notablemente la capacidad de prevenir incidentes antes de que estos ocurran.

En el ámbito de las alarmas y el control de accesos, la IA también ha dejado una huella considerable. Las alarmas modernas ya no son simplemente dispositivos que reaccionan ante una perturbación, como la

apertura de una puerta o una ventana. Hoy en día, muchos sistemas de alarmas utilizan IA para analizar patrones de comportamiento y reducir la cantidad de falsas alarmas. Por ejemplo, un sistema de alarma inteligente puede aprender los hábitos de las personas en una vivienda o una oficina, permitiendo que distinga entre actividades normales y sospechosas, mejorando la precisión de la respuesta.

En cuanto al control de accesos, la IA ha facilitado la implementación de tecnologías avanzadas como el reconocimiento facial y la autenticación biométrica. Ya no se trata solo de tener una tarjeta o código de acceso, sino que las cámaras y los sensores pueden identificar automáticamente a las personas autorizadas para entrar en áreas restringidas, haciendo el proceso más seguro y sin fricciones. La autenticación multifactor basada en IA, como el reconocimiento del iris, huellas dactilares o incluso la forma de caminar, ofrece un nivel de seguridad que reduce significativamente el riesgo de accesos no autorizados.

Además de la vigilancia y el control de accesos, la IA ha demostrado ser una herramienta eficaz para proteger activos en sectores como la banca, las telecomunicaciones y la industria. Con la capacidad de analizar patrones en grandes volúmenes de datos, la IA puede identificar comportamientos anómalos en transacciones financieras, protegiendo contra fraudes y ciberataques. Empresas tecnológicas y financieras ya



están utilizando sistemas de IA para detectar amenazas en tiempo real, minimizando las pérdidas y aumentando la seguridad de los activos digitales.

Sin embargo, a pesar de los avances que ya hemos presenciado, la implementación de la IA en seguridad no está exenta de desafíos. Uno de los mayores retos es la preocupación por la privacidad. El uso extendido de cámaras y sistemas de reconocimiento facial ha suscitado debates sobre los límites éticos de la vigilancia. ¿Hasta qué punto es legítimo monitorizar a los individuos en aras de la seguridad? Esta es una cuestión clave que las empresas y los gobiernos deberán abordar mientras la IA sigue evolucionando.

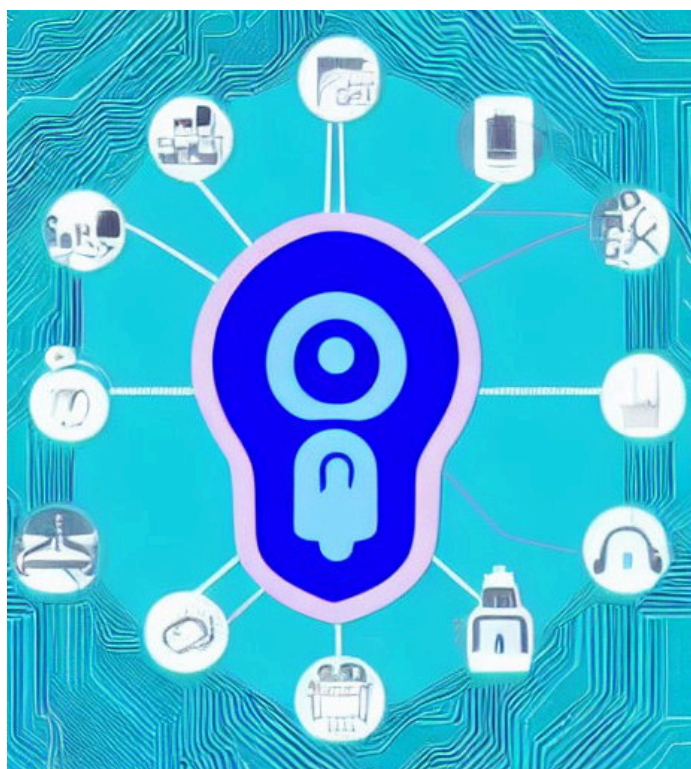
Otro desafío importante es la dependencia excesiva en estos sistemas. Aunque la IA es eficiente, no es infalible. Los sistemas de seguridad basados en IA pueden ser vulnerables a errores o manipulaciones, como el uso de técnicas de falsificación de imágenes (deepfakes) para engañar a los sistemas de reconocimiento facial. La seguridad debe seguir evolucionando, no solo para hacer frente a las

amenazas actuales, sino también para garantizar que la IA no se convierta en una herramienta que pueda ser usada en contra de quienes intenta proteger. La tentación puede ser muy grande y la línea que separa protección de invasión es cada vez más delgada.

## Mirando hacia el futuro

El potencial de la IA en el mundo de la seguridad es inmenso. Como hemos visto, a día de hoy ya tenemos muchas aplicaciones en marcha, pero no podemos olvidar que la IA que tenemos hoy es lo que se conoce como "Narrow AI", es decir, que una IA sólo sirve para un campo en concreto cada vez. La gran diferencia con la Inteligencia Humana es que ésta es capaz de aprender y gestionar múltiples campos a la vez. Cuando esto suceda con la Inteligencia Artificial, habremos alcanzado lo que se conoce como IAG (Inteligencia Artificial General). Será en ese momento en el que podremos equipararla con nuestros cerebros. Con eso y con los avances en el procesamiento de datos en tiempo real, los sistemas de seguridad podrán responder aún más rápido y con mayor precisión a incidentes. En un futuro cercano, podríamos ver una mayor integración de la IA con el Internet de las Cosas (IoT), permitiendo que sistemas de seguridad interconectados actúen de manera autónoma, adaptándose a las amenazas emergentes. Además, es probable que la IA continúe mejorando las capacidades de predicción, anticipando crímenes o incidentes antes de que ocurran, lo que abriría un nuevo paradigma en la protección de personas y activos.

En resumen, la IA ya está revolucionando la seguridad, y aunque enfrenta retos importantes, su futuro promete un mundo más seguro, eficiente y conectado, siempre que lo sepamos gestionar ...¿Será la humanidad capaz de hacerlo?.



# Eva Pastor Sánchez

## Security Specialist en MANGO

### ¿En qué campos de la seguridad se centra tu día a día y que función desempeñas?

Como Especialista de Seguridad en Mango, mi día a día se centra en asegurar los niveles de seguridad adecuados para que puedan llevarse a cabo las actividades propias de la empresa, colaborando en la protección a las personas, bienes y activos frente a amenazas procedentes de hechos delictivos o no deseados, creación de procedimientos de seguridad para minimizar esos riesgos, dotación de medios humanos y tecnológicos y coordinación para su adecuado funcionamiento.

### ¿Principales retos o proyectos relacionados con la seguridad en tu empresa?

Nuestros principales retos relacionados con la seguridad son el proyecto del nuevo Campus ubicado en Palau-solità i Plegamans, donde se encuentran el centro de diseño y las oficinas centrales Mango; y en las tiendas tenemos como objetivo fomentar una mayor concienciación y compromiso con la seguridad organizacional, abarcando la gestión de la seguridad y emergencias a nivel global.

### ¿Cuál es tu formación académica?

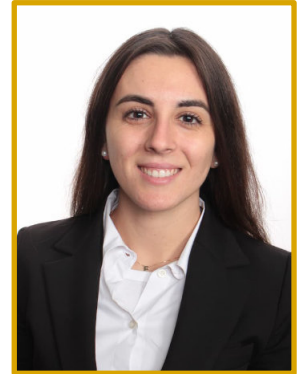
Mi formación académica es principalmente el grado de Prevención y Seguridad Integral (UAB), con el que además obtuve la habilitación de Detective Privado. También realicé el curso Superior en Gestión y Derecho de la Seguridad, donde obtuve la habilitación de Directora de Seguridad y Jefa de Seguridad.

Actualmente estoy cursando el máster en Prevención de Riesgos Laborales con las 3 especialidades: Seguridad en el Trabajo, Higiene Industrial y Ergonomía y Psicosociología Aplicada (UNIR).

### ¿Cómo accediste al mundo de la Seguridad y en que empresas/responsabilidades has ido avanzando desde entonces?

Siempre había mostrado especial interés por el mundo de la seguridad y, para mi sorpresa, existía un grado que impartía la materia correspondiente a este sector con una visión integral, así que no dudé en decantarme por él. Durante la carrera realicé prácticas de Prevención de Riesgos Laborales en RWE, y al finalizar estos estudios

junto con la obtención de las habilitaciones de Detective Privado y Directora y Jefa de Seguridad, me topé con la vacante de MANGO para ocupar el puesto de Especialista en Seguridad, donde coordinamos el correcto funcionamiento de las áreas de intrusión, CCTV, CCAA, gestión de emergencias e incidencias, sistemas contra incendios, formaciones, etc., tanto en las centrales logísticas y de oficinas como en las tiendas.



### ¿Cómo crees que ha evolucionado la Seguridad desde tus inicios hasta ahora?

Imagino que todavía me encuentro en mis inicios de mi carrera profesional y me queda mucho por afrontar del mundo de la Seguridad y su evolución constante, pero si bien es cierto que en estos últimos años estamos viviendo la revolución tecnológica y digital, además con el uso de la Inteligencia Artificial en auge, lo que nos está permitiendo, cada vez más, monitorizar procesos y tareas y trabajar el dato.

### ¿Cómo ves la profesión de director de seguridad en el medio/largo plazo, qué cambiarías de la misma y como crees que evolucionará?

Creo y confío en que la profesión del Director de Seguridad adquiera mayor relevancia en el medio o largo plazo. Tras los acontecimientos que han ido ocurriendo en estos últimos años y con la manifestación de nuevos riesgos tan severos, se está acogiendo de manera gradual y generalizada mayor cultura de Seguridad, que demuestra la necesidad de contar con esta figura dentro de las Organizaciones para poder hacer frente a los retos que se presentan.

Para mejorar la profesión, considero que debemos poner el foco en la formación y actualizar y profundizar los contenidos que se imparten en la misma.

### ¿Exigirías Departamento de Seguridad a las empresas en función del nº de empleados, nº de centros de trabajo, nº de ocupantes, de sus riesgos específicos, etc., o consideras que debe ser de libre creación en todo caso?



Exigiría Departamento de Seguridad a las empresas que, por su actividad, estén sometidas a un riesgo elevado. Por el contrario, todas las organizaciones ya deberían evaluar sus riesgos y establecer las medidas oportunas para minorizar o evitar estos.

**¿Te parece correcto disponer de dos vías formativas tan diferenciadas para obtener la habilitación como Director de Seguridad (curso de habilitación TIP de un año, o grado universitario de 4 años) y que cambiarías?**

Al realizar ambas vías de formación, considero que el curso de un año es limitado para alcanzar la interiorización de las materias que se imparten. Para cambiar esto, creo que sería ideal que, o bien se complementase con prácticas, ya que al final donde terminas de formarte es en la calle y no en el aula, o bien se ampliase el curso de manera que se pudiera dedicar más horas a cada ponente y temario.

**¿En la formación para ejercer como director de Seguridad, que materias o aspectos deberían potenciarse, que no se traten en profundidad ahora?**

Debería potenciarse la formación en Ciberseguridad e Inteligencia Artificial puesto que se encuentran en auge y traen consigo nuevos riesgos y oportunidades, y también se debería poner el foco en las técnicas de los sistemas de seguridad, ya que en el mundo laboral es esencial conocer el producto para tratar con los clientes y proveedores y proteger el negocio.

**¿Ventajas de integrarse en una asociación de profesionales de la seguridad?**

La ventaja principal es el networking que ofrece cada espacio que compartimos, lo que te permite conocer cómo funcionan otras empresas, así como sus productos y servicios, y te permite tener a tu alcance el contacto de compañeros del sector con quien poder intercambiar opiniones y experiencias y mantenerte actualizado de las últimas novedades.

**¿Qué te ha llevado a afiliarte a ADSI en concreto?**

Lo que me llevó a afiliarme a ADSI es la cantidad de entornos que ofrece para compartir tiempo y conocimiento con otros profesionales y organizaciones del mundo de la Seguridad y los diferentes sectores que la contratan.

**¿Qué debe mejorar ADSI en relación con la prestación a sus asociados?**

Estoy muy contenta con la gestión actual de ADSI y creo que debe seguir en esta línea, velando por aproximar a los profesionales del sector.

**¿Cómo podría incrementarse la colaboración entre directores de seguridad de ámbitos/sectores/empresas diferentes de nuestro país?**

La colaboración podría incrementarse con la creación de un foro de preguntas y respuestas donde podamos participar exponiendo nuestras inquietudes, soluciones y experiencias que nos topamos en nuestro día a día.

**En un mundo cada vez más globalizado y por tu experiencia, ¿destacarías algún país en la gestión de la seguridad y cómo mejorarías el intercambio de experiencias y conocimiento entre países?**

Destacaría países como Nueva Zelanda por la cultura de seguridad que adoptan los propios ciudadanos, donde ellos mismos se supervisan, ayudan y advierten de los peligros iniciales que detectan. Igualmente creo que todos podemos aprender de todos y debemos tener una mente abierta para crecer conjuntamente.

Actualmente se realizan congresos internacionales de Seguridad, de todas formas, sería interesante que hubiera un foro oficial de Directores de Seguridad Privada o una IA generativa a nivel mundial donde poder retroalimentarnos intercambiando las experiencias y conocimiento que envuelve esta profesión. ■

🚲 Un hobby: Viajar y cantar.

📖 Un libro: “Comunicación No Violenta: Un lenguaje de vida” – Marshall B. Rosenberg.

🎵 Una canción: “Las cosas pequeñas”, de Marta Santos.

🏖️ Un lugar para desconectar: El mar, en cualquier parte del mundo.

🕒 Un momento de la historia: Cada uno de los momentos de la historia es ideal pues todos dan lugar a lo que somos hoy, pero me quedo con el presente.



# Trump ¿ha llegado el momento para una defensa, inteligencia y seguridad europeas?

Por **Alfonso López Clavier**, Coronel GC (r) y Presidente de APTIE

Artículo publicado en "El Radar", diario de seguridad, defensa, drones y ciberseguridad

**En este artículo no hablaremos de Trump, de sus planteamientos, políticas y enfoques en general. Trataremos exclusivamente del nuevo escenario en Seguridad y Defensa que se plantea a Europa tras la elección de Donald Trump como Presidente de los EE.UU. de América. Sus reiteradas peticiones a las naciones europeas de la OTAN, que incrementen sus gastos de Defensa de forma significativa y que se impliquen más en su propia defensa, bajo amenaza de salirse de la Organización del Atlántico Norte, empiezan a ser percibidas como una amenaza real.**

Como consecuencia de ello plantearemos brevemente y sin profundizar dos cambios que planean en las declaraciones hechas últimamente por máximos responsables de la UE y que revierten de plano las políticas de seguridad europeas de los últimos 70 años, como son, por una parte, la necesidad de crear un ejército europeo con sus consiguientes políticas militares, armamentísticas e industriales. Y, por otro, la creación de una estructura de Inteligencia que, asume la contrainteligencia, la ciberseguridad y la seguridad económica. A ello añadimos la novedosa y necesaria la coordinación/cooperación del esquema de Inteligencia con un nuevo modelo policial europeo.

Hago distinción clara entre Defensa y Seguridad, porque, a mi entender, la Seguridad engloba a la Defensa, pero hay muchos otros campos de seguridad fuera de la Defensa. Por ello trataremos en esta primera parte los temas de Defensa, dejando para una segunda parte los de Inteligencia y los diferentes planteamientos de una futura estructura de los Servicios de Inteligencia europeos.

## 1.- Panorama de situación de la defensa europea ante los planteamientos de Trump

En los últimos tiempos, la posibilidad, ya confirmada, de que Trump ganara las elecciones en USA, suponía en la mayoría de los políticos y de determinados medios

comunicación, así como en mundo empresarial occidental una enorme preocupación.

En anteriores y reiteradas declaraciones, Trump incidió en la necesidad imperiosa de que las naciones europeas (pero no solo ellas) deben responsabilizarse de su propia seguridad y de la europea. Para ello deberían dedicar al menos el 2% de su presupuesto a Defensa. Todo ello bajo la amenaza de que EEUU podría retirarse de la OTAN y sus tropas de Europa. Estas declaraciones, en mi opinión, han sido analizadas muy deficientemente por los políticos y los medios europeos, que insisten en que Trump quiere dismantelar la OTAN y dejarnos en manos de Rusia. Sin entender las razones de Trump y que este planteamiento no es exclusivo de Trump, que no es ni una salida de tono ni una amenaza extemporánea, si no una reclamación que, con razón, todos los presidentes norteamericanos, desde Kennedy, llevan haciendo a los dirigentes europeos de forma más o menos clara.

Su planteamiento es que no resulta admisible que EE.UU. llegara a tener más de 300.000 soldados y numerosas bases en Europa, y dedique un gasto considerable a la defensa europea, mientras los países europeos mantenían unos presupuestos para Defensa ridículos, se desentendían, salvo Gran Bretaña, de la defensa y seguridad europea y se vanagloriaban de dedicar una parte enorme de sus presupuestos a gasto social, al tiempo que se permitían criticar el militarismo e imperialismo USA, por las bases afincadas en Europa y el mundo.

Esta preocupación de los presidentes de USA y, en concreto, de Trump, no ha dado lugar por parte europea a analizar y a hacer planteamientos serios sobre lo que significan. La clara apuesta de la mayoría de los partidos políticos sobre los problemas y riesgos que iba a traer su vuelta a la presidencia de EE.UU., junto al





posicionamiento de los medios calificándolo prácticamente como un peligro existencial para Europa, particularmente en los campos de la democracia, la Seguridad y la Defensa, ha supuesto una clara parálisis en el imprescindible análisis que se debería haber hecho desde el momento que Trump lo planteó en serio.

La invasión de Crimea e importantes extensiones de Ucrania en 2014, no fueron suficientes para concienciarse de que existía una amenaza gravísima para Europa. Pero la brutal segunda invasión ya al corazón de Ucrania, despertó claramente las alarmas. Esta situación de una guerra real en territorio europeo que ya va para tres años, el aumento de las amenazas terroristas y de la guerra híbrida, plasmada en millones de ciberataques a todos los niveles, junto a la constatación de que el interés norteamericano y anglosajón se enfocan decididamente hacia el escenario indopacífico, están haciendo cambiar la percepción política, militar y social de los riesgos tangibles a los que nos enfrentamos los europeos. Y que algunas propuestas hechas anteriormente con la boca pequeña por algunos dirigentes europeos, empiecen a concretarse en declaraciones inimaginables hace poco.

Lo primero ha sido la decisión de que la Unión Europea cuente por primera vez con un Comisario de Defensa y Espacio, Andrius Kubilius con lo que ello significa. Recientemente la presidenta de la Comisión europea, Úrsula von der Leyen, pidió al exministro finlandés, Sauli Niinisto, un informe sobre el nivel de preparación

europeo ante los nuevos planteamientos para la seguridad, en su más amplio sentido. Desde el militar, al económico, industrial y protección de infraestructuras críticas, tanto contra ataque militares, como del terrorismo, ciberataques, amenazas híbridas y seguridad ciudadana. Lo fundamental del informe es que plantea varios temas trascendentales: la necesidad de una defensa militar convencional europea, de una estructura de seguridad ante las amenazas cibernéticas e híbridas, de una Defensa económica y, finalmente, y nada menos que el de una Agencia de Inteligencia europea.

Inicialmente no considero necesario tratar el tema de las estructuras de seguridad ante las amenazas cibernéticas e híbridas, tanto a niveles nacionales como europeos, dado que actualmente ya existe conciencia de su necesidad y son muy numerosas y potentes, y se van integrando rápidamente a nivel europeo, occidental y de la OTAN.

### **Implicaciones para la Defensa**

En cuanto a Defensa y sus implicaciones militares, los planteamientos fundamentales son, sin ser exhaustivos: a) La decisión política y social, a nivel UE y de cada nación que la integra, de constituir un ejército europeo a corto y medio plazo, definiendo de forma clara sus misiones, mando, estructura y despliegue, entre otras. b) Dedicar de forma constante al menos el 2% del presupuesto de cada país a Defensa. c) Definir de forma clara la política



industrial de Defensa a corto, medio y largo plazo de manera que integre tanto el presupuesto, los procedimientos como la fabricación, mantenimiento y ciclo de vida.

No profundizaré en cada punto, dado que cada uno de ellos es inmenso y objeto de estudios de las organizaciones y entidades políticas y de Defensa de cada nación y de la UE. Aunque no olvidaré la necesidad imprescindible de consensuarlo de manera abierta y sincera con EEUU, al tiempo que Rusia no lo vea como una amenaza cierta contra ella.

Para tener un punto de vista global, veamos algunas cifras de los principales presupuestos de Defensa en el mundo. USA dedicó en 2022 876.943 M\$, el 3,5%. China sobre 292.000M\$, equivalente al 1,6%. Rusia, el 4,5%, 109.000 M\$. Por su parte, la totalidad del gasto de los países de Europa fue de 239.000 M€, prácticamente igual que el de China, 1,6% el chino y 1,54% el europeo, pero disperso. De todas formas, estos datos rebaten la idea primigenia de que "Europa no puede hacer nada contra los colosos mundiales". Mentira y cobardía. Europa dispersa, no somos más que países en decadencia, unida es la tercera potencia mundial, y eso si no tenemos en cuenta a Iberoamérica.

Aquí surge una pregunta ¿Cómo es posible que los ejércitos ruso y chino sean formidables con presupuestos equivalentes, al menos sobre el papel y sin considerar su armamento nuclear, mientras que Europa, como se ha visto con la guerra de Ucrania, prácticamente carece de municiones para aguantar una semana de combates? Salvo Polonia que, tanto por memoria histórica sobre sus dos vecinos como que tiene la amenaza real "al otro lado del camino", lleva años dedicando hasta el 4% de su presupuesto a Defensa, como Gran Bretaña, que, aunque no está en la UE, es Europa, mantiene un importante gasto permanente en defensa por una cierta idea imperial, unido al convencimiento de que tiene que ser el principal

aliado de los EEUU, con quien tiene que estar siempre sea a las duras como a las maduras.

La respuesta es sencilla, no existe un ejército europeo, ni están integrados los de las diferentes naciones, ni ha existido una voluntad política de constituirlo ni de integrarlo, aunque se hacen continuamente reuniones, ejercicios, unificación de estándares, en lo que los de la OTAN tienen una importancia capital.

Sin embargo, como veremos, esta situación está evolucionando rápidamente. Las declaraciones de Von der Leyen, de Roberta Metsola, Presidenta de la Eurocámara, y otros dirigentes europeos indica un cambio de rumbo radical de tratar este tema de forma clara. Es significativo que la propia Von der Leyen haya comunicado que prevé para el próximo año un presupuesto europeo conjunto de 350.000 M€, aunque no integrado.

El problema de los órganos de decisión de la Unión Europea y de cada nación que la integran, es que tendrán que explicarle a sus ciudadanos este cambio, al tiempo que reducir sus políticas sociales en sus presupuestos, pasando a aumentar de forma significativa los gastos en Defensa y Seguridad, es decir mayores presupuestos, como mínimo el 2%, para Ejércitos más eficaces y para una industria de armamento potente y coordinada.

Pero si esto ya chirría a los oídos de la clase política europea, se tendrán que tomar muy en serio la tarea tan gigantesca que supone construir un ejército europeo, de los problemas políticos, sociales, técnicos, organizativos, etc. que suponen, además de las previstas interferencias extranjeras, fundamentalmente rusas y chinas, de gobiernos populistas, de pacifistas bien intencionados y de los "otros", sin descartar las lógicas procedentes de USA, normalmente por motivos económicos.

Y, si se toma una decisión positiva, todo ello ¿qué va a significar en cuanto a política industrial de Defensa? A mi entender: a) La decisión política de cada país de aumentar sus presupuestos de Defensa; b) Creación de una estructura política y militar de Dirección de la política industrial común europea de Defensa; c) Planteamiento de unificar sistemas de armas, es decir que, en lugar de 27 modelos de vehículos blindados, haya solo uno o dos, lo mismo con los aviones, los buques de guerra, la artillería, etc. En resumen, copiar el modelo norteamericano; d) Decidir en qué naciones y regiones se instalan esas fábricas y las de componentes, junto a la de quién decide, quién tiene preeminencia en cada decisión y procedimientos de colaboración e integración de



sistemas (recordemos las peleas de los senadores USA defendiendo la instalación y/o mantenimiento de fábricas e instalaciones militares en su estado). Podemos continuar, pero creo que todo ello es más bien competencia de cada gobierno y de sus organismos de política y estrategia de defensa e industrial.

Solo quiero hacer una última consideración a tener muy en cuenta en esa nueva política de defensa, tanto militar como industrial. Las naciones europeas compran a las empresas norteamericanas de armamento sobre 65.000 M\$ al año. Si se integra y crea una potente industria militar europea, lo que es lógico teniendo en cuenta el PIB europeo, aquellas verán descender considerablemente sus ingresos. Pienso que es un tema extremadamente delicado a tener siempre presente.

Termino volviendo a la pregunta si Trump cumplirá su amenaza y hasta dónde. Creo que la idea de que Trump está buscando abandonar la OTAN no representa su política real ni el pensamiento de la estructura militar norteamericana. Primero, porque sería un suicidio occidental. Segundo, porque pienso que Trump actúa fundamentalmente como empresario norteamericano, muy práctico, que mira el gasto y acostumbrado a tirarse faroles hasta donde estén sus intereses verdaderos. Y, finalmente, porque creo que, como dice Christopher Miller, el último Secretario de Defensa interino del primer mandato de Trump: "Descartamos la idea de que Trump se esté preparando para abandonar la alianza. Creemos que su objetivo final es una mejor distribución de los costes de la defensa occidental y, en particular, de la europea".

Cierro este tema con dos consideraciones que la UE tiene que tener ya claro: Para USA y el mundo anglosajón la prioridad y el peligro existencial ha pasado a China y la región del indopacífico. La otra, que el problema de Rusia pasará en su mayor parte a ser casi exclusivamente europeo.

Cierro esta parte con unos planteamientos que creo satisfarían a Trump y a los EEUU. Europa aumenta sus presupuestos nacionales sobre el 2%; avanza en la creación del ejército europeo; define una única y clara política con Putin (aquella del gánster y el dentista "¿Verdad que no nos vamos a hacer daño"?), sin apoyar claramente a Israel, lo hace de forma decidida en cooperar a la caída del régimen de los Ayatollahs, ayudando a que Irán se convierta en una democracia y añada todo su potencial económico, humano, cultural, etc, a la paz de Oriente próximo, y, finalmente, sin entrar en las alianzas del Indopacífico, para que China vea

claramente que no le conviene avanzar a planteamientos de hegemonía mundial, al menos en lo militar.

Las diferentes formas de enfocararlo, canalizarlo y resolverlo, para bien o para mal, dependerán de las habilidades políticas y de una realidad militar y social europea creíble. Si Europa no toma decisiones en estos y otros muchos temas, Europa empezará a difuminarse.

**Veamos ahora, sin descender a profundizar, la revolucionaria propuesta del expresidente finlandés Niinisto, cuya valentía alabo, de crear una Agencia de Inteligencia europea. Entramos en otro de los pocos campos de soberanía nacional terriblemente espinoso y complejo, para cuyo planteamiento e implementación se necesitarán auténticos estadistas y no políticos temporales que solo piensen en su próxima reelección.**

## **2.- Implicaciones para la seguridad europea. Hacia una nueva estructura de inteligencia europea**

El tema de los Servicios de Inteligencia siempre se ha tomado en general muy a la ligera, cuando son estructuras imprescindibles muy complejas de soberanía de cada Estado, por lo que mi parte, hago una consideración inicial y básica. En lugar de "una Agencia de Inteligencia europea", deberá plantearse "el Esquema de Inteligencia europeo".

El modelo de Inteligencia clásico mundial comprende, de forma general y sin ser exhaustivo, tres Servicios secretos civiles y uno militar, organizados por ámbitos de competencias: Una Agencia o Servicio de Inteligencia, especializada en luchar contra los peligros y agresiones exteriores (CIA de USA, MI6 británico, FSB ruso, BND alemán, etc.) Segundo, un Servicio de Contrainteligencia, que lucha contra los peligros que se producen en el



interior de la nación, sea por extranjeros o por nacionales (FBI de USA, MI5 británico, BfV o Servicio de Defensa de la Constitución alemán, la DGSE francesa, el FSB ruso (antigua KGB), etc) Característica importante de estos Servicios es que sus Directores, aunque estén adscritos a algún ministerio por razones administrativas y logísticas, pueden informar directamente a sus respectivos Presidentes de la nación y a las Comisiones de Inteligencia de sus Parlamentos. En general, aunque civiles no son servicios policiales, pero si tienen controles judiciales. El tercer brazo son los Servicios de Inteligencia de Señales (NSA norteamericano, CGHQ británico, etc), responsables del seguimiento de todo lo que se transmite por las ondas, internet, etc. Por el coste y las complejidades técnicas que suponen, suelen atender a todos los demás Servicios, y unas veces son independientes y otras se integran en el Servicio de Inteligencia Exterior. El círculo se cierra con el Servicio de Inteligencia y Contrainteligencia de cada uno de los Ejércitos, uno a nivel central y otro en cada Ejército.

Este es el modelo tradicional, que se repite normalmente en todo el mundo. El español tiene como característica que carece de un Servicio de Contrainteligencia, de Inteligencia Interior o de Defensa de la Constitución, como tal. Las competencias de este tipo de Servicio están distribuidas y entremezcladas entre el CNI y los Servicios de Información de Policía Nacional y Guardia Civil, ambos con ciertas características de Servicios de Inteligencia y bastante eficaces y potentes. Por su parte, el CNI, de gran eficacia operativa, a mi entender precisa de una potenciación, principalmente de personal. Para atender prácticamente las misiones de tres Servicios de Inteligencia, dispone del mismo personal que cualquier nación de la entidad de España dedica solamente a cada

uno de sus Servicios. Es encomiable su eficacia operativa y en la ciberseguridad de la Administración española, al tiempo la promoción de la Cultura de Defensa, Económica y de Inteligencia que desarrolla. La creación del Departamento de Seguridad Nacional DSN, dependiente de Presidencia del Gobierno, supone un avance en el esquema de seguridad nacional.

En cuanto a la Inteligencia o Seguridad Económica, citada por Sauli Niinistö como una actividad fundamental a proteger, considero que entra en los campos de Inteligencia y Contrainteligencia, incluyendo además a otros Ministerios y organismos con responsabilidades económicas, industriales, financieras, etc., además del de todo el tejido económico y empresarial privado. Ejemplo paradigmático es Francia, en la que el Comisionado de la República para la Seguridad Económica depende directamente del Presidente de la República, con la potencia, capacidad de concienciación, ventajas y posibilidades que esta dependencia le concede. En España, por lo que sea, no podemos afirmar que exista una verdadera conciencia de defensa de nuestros intereses económicos, incluyendo los culturales, a todos los niveles.

Pero, en los últimos años este esquema está completándose en todo el mundo con un nuevo actor, los Cuerpos policiales de todos los niveles como generadores de información y, en determinados momentos, de inteligencia. Como bien describe el Coronel de la Guardia Civil (r), José Duque, en su tesis doctoral "De la Cooperación Policial Internacional a la Cooperación Internacional de Seguridad y de Inteligencia. El Modelo Federal Cooperativo de Estados Unidos", inicialmente en EEUU y después en diferentes



países se está viendo que las diferentes Policías, sean locales, estatales y/o especializadas, y otras Agencias regionales/federales no policiales ni de Inteligencia, tienen actualmente una gran capacidad de generar ingentes datos de interés para la Inteligencia y la Seguridad nacional.

Como conclusión parcial podemos decir que si la UE decide crear un sistema de Inteligencia deberá estudiar con profundidad el modelo norteamericano, contemplando sus diferentes niveles de seguridad y teniendo en cuenta las realidades de cada sitio. Hagamos las equivalencias forma aproximada: Las ciudades y condados USA, con las ciudades, regiones, länders y Comunidades de cada nación europea. El nivel estatal USA es bastante difícil de equiparar con los Estados/naciones europeas, ya que éstas entran más bien en comparación con el nivel federal USA. Al ser la Seguridad y la Inteligencia atributos de soberanía nacional ¿Cómo se integrarían los 27 Servicios de Inteligencia, Contrainteligencia y los militares europeos entre sí? Importancia capital es el problema de la jerarquización de competencias, prioridad y de autoridad de cada Servicio, entre ellos y en relación con los diferentes Cuerpos policiales y demás Organismos de las diferentes Administraciones de la Unión y de cada país. Este rompecabezas y ardua tarea se los dejo a los estadistas, a los genios y a los profesionales. Lo primero que se precisará será una Ley de Secretos Oficiales muy bien hecha y eficaz.

Un posible camino inicial podría ser la creación paulatina de Agencias federales europeas especializadas, fundamentalmente en campos civiles y tomando como ejemplo las, por el momento, 53 Agencias federales norteamericanas. Al igual que Bismark comenzó la unificación alemana con un Servicio Postal común, igual podría irse creando Agencias europeas con diferentes competencias en Seguridad, como las de Armas y Explosivos, Postal, Antidrogas, Contra Incendios, Seguridad en el Transporte, de Aviación, Aeronáutica y del Espacio, Alcohol y Tabaco, Medio Ambiental, Investigación Criminal, Económicas, etc. Todo ello de manera que se engrasen los procedimientos de cooperación y se incremente paulatinamente la confianza entre todos los países respecto a la eficacia, seguridad, discreción e independencia de cada nueva Agencia.

En el campo policial estatal existen dos modelos de organización en el mundo: Los Cuerpos de Policía de carácter exclusivamente civil y los Cuerpos policiales de

naturaleza Militar. Para el objeto de este artículo, un modelo a estudiar y posiblemente a constituir como una Agencia Policial de naturaleza Militar europea, podría ser la FIEP, la Asociación Internacional de las Gendarmerías y Cuerpos Policiales con Estatuto Militar. Fue creada en 1992 por la Guardia Civil, la Gendarmería francesa, los Carabinieri italianos y la Guardia Nacional Republicana portuguesa. Actualmente, bajo la presidencia de Francia, agrupa a 20 Cuerpos policiales de carácter militar, más un observador, San Marino. Tienen organizada estructuras de cooperación comunes en personal, logística, servicios y nuevas tecnologías, a través de Estados Mayores y centros de formación conjuntos ubicados en diferentes naciones.

Hace un tiempo se integraron Cuerpos americanos como los Carabineros de Chile y la Guardia Montada de Canadá. La incorporación de la Gendarmería Real de Marruecos, la Gendarmería turca y otros Cuerpos europeos, suponen una estructura con más de un millón de policías con carácter militar. Que, en palabras del profesor Miguel Á. Acosta Sánchez, de la Universidad de Cadiz, en su trabajo "La Asociación Internacional de Gendarmerías y Fuerzas Policiales con Estatuto Militar (FIEP): ¿un instrumento a disposición de la gestión integrada de fronteras europeas?, afirma que "representa un caso muy particular de cooperación". Y que "la FIEP pretende aportar medios y capacidades para la constitución de una fuerza europea de policía en el marco de la Política Común de Seguridad y Defensa (PESD)".

En cuanto a una Policía civil, la conversión de EUROPOL en una verdadera Agencia Policial europea, con capacidades ejecutivas podría ser efectiva. Si se complementa con un verdadero espacio judicial europeo, que evite las barrabasadas de algunos juzgados como los alemanes y belgas en los casos de Puigdemont y los terroristas de ETA, se cerraría el círculo de seguridad policial europeo muy eficaz y eficiente.

Finalmente, un penúltimo paso sería el de abordar la creación de las Agencias Europeas de Inteligencia Económica y la de Señales, para finalizar con las de Inteligencia, Contrainteligencia y militares, junto con los Comités de Inteligencia del Parlamento Europeo.

Si con estas ideas colaboro al menos en un poco en los planteamientos con vistas a la creación e integración de los modelos de Seguridad, Inteligencia y policial europeo, creo que será un paso interesante. ■



## SEDEXPO 2025 prepara una cita muy dinámica en la que seguridad, defensa y emergencias mostrarán sus novedades del 26 al 28 de marzo

ESTA TERCERA EDICIÓN DEL CERTAMEN, QUE TENDRÁ LUGAR EN EL RECINTO FEIRA INTERNACIONAL DE GALICIA ABANCA, CONJUGARÁ UNA ATRACTIVA ÁREA EXPOSITIVA Y UN COMPLETO PROGRAMA DE ACTIVIDADES CON EXHIBICIONES, SIMULACROS, TALLERES Y JORNADAS TÉCNICAS



La Feria Internacional de Seguridad, Defensa y Emergencias, SEDEXPO, trabaja desde hace meses en su tercera edición, la cual tendrá lugar del 26 al 28 de marzo de 2025 en el recinto Feira Internacional de Galicia ABANCA, situado en el municipio de Silleda, en Galicia.

Sedexpo 2025 volverá a conformar un punto de encuentro en el que organismos públicos, instituciones, empresas y profesionales de estos ámbitos vitales para la sociedad podrán explorar oportunidades de colaboración, intercambiar experiencias y poner en valor la innovación.

Una propuesta con la que pretende superar su pasada convocatoria, celebrada en noviembre de 2023, y que contó con 209 firmas expositoras de 24 países, de las cuales 83 fueron expositores directos de Alemania, España, Francia, Israel, Italia, Letonia, México, Países Bajos, Pakistán y Portugal. Unas cifras que supusieron que los expositores directos ocuparan un 5,4% más de espacio y procedieran de un 42% más de países que en la anterior edición, siendo además el número de empresas extranjeras presentes un 29% más. La cita recibió a 3.607 visitantes, lo que supuso un 22,5% más que en su primera convocatoria.

En 2025 el área expositiva de Sedexpo contará con empresas y entidades que mostrarán interesantes

novedades e iniciativas. Se expondrá equipamiento y sistemas de seguridad pública y privada, material para las Fuerzas y Cuerpos de Seguridad del Estado, Protección Civil y Emergencias; equipos de protección individual, tecnología aplicada, herramientas de ciberseguridad, análisis e inteligencia; soluciones de prevención de riesgos laborales, equipos de emergencias, dispositivos de detección y extinción de incendios, robótica, aeronáutica, simulación y servicios de consultoría e ingeniería, entre otros.

En cuanto a su programa de actividades, destacará de nuevo por su gran atractivo. Sus conferencias y talleres tendrán gran interés para la transferencia de conocimientos, mientras sus exhibiciones y simulacros permitirán al visitante tanto comprobar in situ las funcionalidades de productos y servicios como sorprenderse con las capacidades de distintos cuerpos de emergencias y de seguridad del Estado.

Para todo ello, una veintena de entidades, departamentos de la Xunta de Galicia y de la Administración Central y colectivos vinculados con los sectores implicados vuelven a apoyar esta cita desde su comité organizador y como colaboradores.

Además, Sedexpo cuenta nuevamente con el patrocinio de la Civil UAVs Initiative, una iniciativa estratégica liderada por la Xunta de Galicia que tiene como finalidad promover soluciones innovadoras basadas en vehículos aéreos no tripulados (UAVs) para mejorar la prestación de los servicios públicos y crear un polo de innovación tecnológica en este segmento del sector aeroespacial.



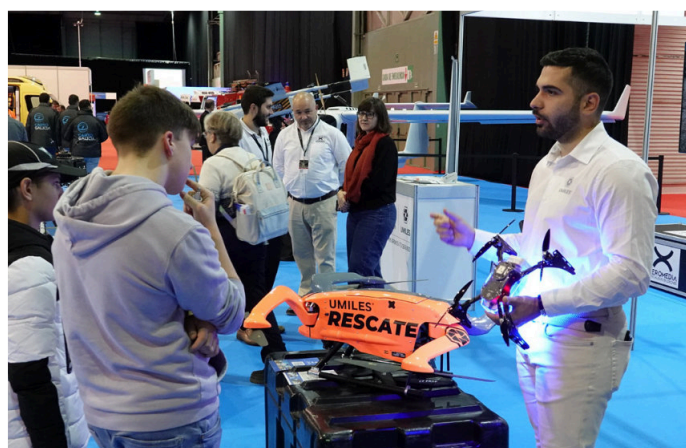


## UNA FERIA ÚNICA POR SU DINAMISMO

La posibilidad de mostrar y ver en funcionamiento y a través de demostraciones aquello que en otras ferias se expone de una forma mucho más estática, es ya una seña de identidad de Sedexpo y uno de sus principales aspectos diferenciadores.

En la pasada convocatoria el certamen sorprendió con exhibiciones de distintos modelos de drones, rescates en el agua con vehículos acuáticos eléctricos, puestos de mando avanzado para coordinar los servicios públicos, privados y sanitarios en eventos, simuladores de conducción de ambulancias en realidad virtual o prácticas extremas en alto estrés en tiro simulado. Asimismo, sus simulacros fueron espectaculares, como el protagonizado por la Guardia Civil, que escenificó la intervención ante un secuestro con arma blanca con participación de medios como un helicóptero, también la recreación de la extinción de un incendio con ataque combinado de medios aéreos y terrestres para la defensa de una vivienda aislada organizado por la Xunta de Galicia o el ejercicio sobre futuras capacidades de la unidad operativa de drones de la Agencia Gallega de Emergencias (AXEGA) en la búsqueda de personas desaparecidas.

Unas demostraciones y simulacros que convirtieron a este certamen en único, y que volverán a hacerlo en 2025, gracias a su celebración en la Feira Internacional de Galicia ABANCA, un recinto con 400.000 metros cuadrados de superficie con gran versatilidad gracias a sus múltiples pabellones, a los 55.000 metros cuadrados de espacios exteriores destinados a exposición o actividades, su lago artificial o su ring con gradas cubiertas. ■



**TODA LA INFORMACIÓN DE SEDEXPO 2025 PUEDE ENCONTRARSE EN:**

[www.sedexpo.com](http://www.sedexpo.com)

[#sedexpo25](https://twitter.com/sedexpo25)



security  
forum4 – 5 de junio  
Les Drassanes Reials  
Barcelona

securityforum.es



# Security Forum 2025

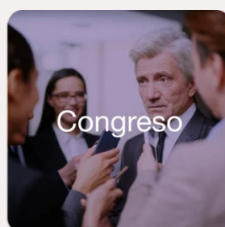
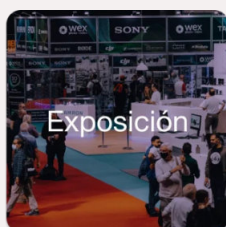
## ¿Sabías que Security Forum 2025 compartirá fecha con II edición del Congreso de Seguridad en espacios públicos de Barcelona?

Las Drassanes Reials de Barcelona se convertirán en el **epicentro de la Seguridad en España** con la **12ª edición de Security Forum**. El encuentro contará con la **colaboración especial** del **Ajuntament de Barcelona**, y abordará "La seguridad 360º" en todas sus áreas (Congreso, Expert Panel y área expositiva).

En coincidencia con Security Forum, el **día 5 de junio** se celebrará en las Drassanes Reials la **II Edición del Congreso de Seguridad en espacios públicos de Barcelona**. Aquí se reunirán los principales **cargos públicos en materia de seguridad de la provincia de Barcelona** para analizar los **retos** a los que se enfrentan los entes públicos en la **contratación de sistemas y servicios de Seguridad**, las **tendencias tecnológicas** y las **iniciativas puestas en marcha** por las diferentes administraciones.

¿Quieres formar parte de los dos eventos de seguridad más importantes de Barcelona en 2025?

**Consulta los formatos de participación y vive la experiencia Security Forum**



Más Información

**CUADERNOS  
DE SEGURIDAD**



Ajuntament de  
Barcelona

**ADSI**  
asociación de directivos  
de seguridad integral



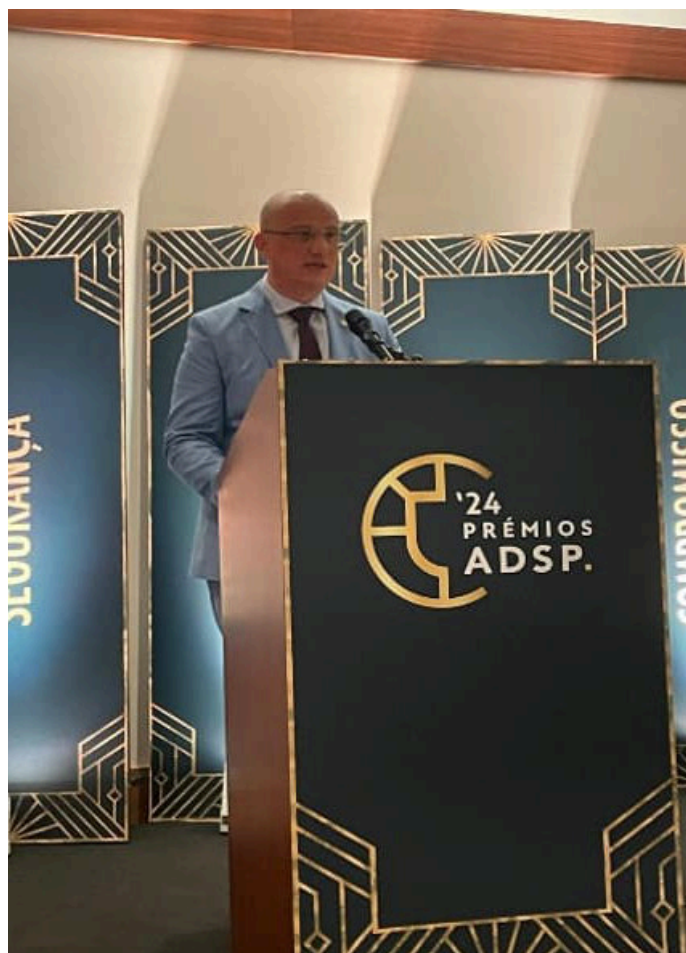
# ADSI en la cena anual y entrega de premios de ADSP-Associação dos Directores de Segurança de Portugal



En representación de ADSI, nuestro presidente, Eduard Zamora, ha asistido a la cena anual y entrega de premios 2024 de ADSP, en la 24ª edición de este evento de nuestra asociación homónima y amiga de Portugal, celebrada en Lisboa el 13 de diciembre.

Agradecemos a su equipo directivo, en especial a su Presidente, José A. Meneses, su amable invitación, que nos brindó la oportunidad de compartir con los profesionales de la seguridad y autoridades policiales de Portugal las vicisitudes de la seguridad privada en su país.

En la imagen de grupo, de izquierda a derecha, Superintendente-Jefe Pedro Neto Gouveia, Director Nacional Adjunto de la Policía de Portugal, José António Meneses, Presidente de ADSP, Superintendente José Fernandes - Director del Departamento de Seguridad Privada de la Policía de Portugal, Eduard Zamora, Presidente de ADSI y Ludovico Jara, Presidente de la Asamblea de ADSP. ■



# Convocatoria para concesión de menciones de seguridad privada en Cataluña año 2024



Generalitat de Catalunya  
**Departament  
d'Interior**

Mediante una Resolución de la Consejera de Interior y Seguridad Pública de 9 de diciembre de 2024, el Departamento de Interior ha convocado el proceso para la concesión de menciones en el ámbito de la seguridad privada en Cataluña correspondiente al año 2024.

Como en anteriores ocasiones, con esta nueva convocatoria, que culminará con la entrega de las menciones en el transcurso del próximo Día Català de la Seguretat Privada, el Departamento de Interior quiere continuar reconociendo de manera institucional el esfuerzo, la dedicación, la excelencia en el cumplimiento de las funciones y, especialmente, la colaboración de los profesionales de la seguridad privada en Cataluña con las administraciones públicas, la policía de la Generalitat y las policías locales de Cataluña.

En definitiva, el Departamento de Interior quiere reconocer, nuevamente, la contribución de los profesionales de la seguridad privada a garantizar un sistema de seguridad de Cataluña más eficaz y eficiente.

De acuerdo con lo que dispone la mencionada Resolución, se inicia el plazo para presentar, ante la Generalitat de Catalunya, las propuestas para todas las modalidades de menciones en el ámbito de la seguridad privada. Este plazo finalizará el día 17 de febrero de 2025, fecha a partir de la cual todas las propuestas presentadas serán valoradas por la Comisión de Evaluación.

Las propuestas de menciones se tienen que presentar telemáticamente, mediante el trámite al cual se puede acceder desde la página web del Departamento de Interior o desde el enlacedeltrámitemencionesseguridadprivada. Asimismo, los requisitos de las personas o entidades que opten a las menciones, la documentación a aportar y los criterios de valoración se rigen por la Orden INT/52/2011, de 30 de marzo, por la cual se aprueba el procedimiento para la concesión de menciones en el ámbito de la seguridad privada en Cataluña. ■

Enlaces:

- [Resolución de convocatoria 2024.](#)
- [Orden INT-52-2011.](#)

## Informe sobre Tecnologías Biométricas Seguras para el Control de Acceso

En el marco del Programa **COOPERA**, el Departamento de Colaboración del Servicio de Protección y Seguridad, remite el Informe sobre "**Tecnologías biométricas seguras para el control de acceso**", elaborado por el Centro Criptológico Nacional.

En dicho informe se pone de manifiesto el uso seguro de la tecnología RBR, pudiendo concluirse que el dato generado fruto de este proceso no es un dato biométrico, y ni tan siquiera sería considerado un dato personal, lo cual, podría provocar un cambio de tendencia en los dictámenes de la Agencia Española de Protección de Datos, considerándolo de sumo interés para gestionar el tratamiento de esta tecnología acorde con la legislación vigente. ■

Enlace del documento:

[Tecnologías Biométricas Seguras para el Control de Acceso](#)



# ADSI en la XXXVII Edición de los Trofeos de Seguridad de la revista SEGURITECNIA

**SEGURITECNIA**  
REVISTA DECANA INDEPENDIENTE DE SEGURIDAD

**ADSI**  
asociación de directivos  
de seguridad integral

El pasado 13 de diciembre, ADSI estuvo presente en el acto de entrega de los premios, como miembro del Consejo Técnico Asesor de Seguritecnia, representada por su Vicepresidenta Elvira Márquez.

Entre otros, fueron reconocidos nuestros asociados: José Márquez, Director de Seguridad de Naturgy, con el Trofeo a la actividad investigadora; Juan Carlos Robledo, Director de Seguridad de Caja Rural de Salamanca, con el Trofeo al mejor usuario de Seguridad Privada. También nuestro patrocinador, SCATI LABS obtuvo el Premio al Mejor Producto de Seguridad. Se reconoció con el Premio Especial del Jurado la labor de la Abadía de Montserrat, con ocasión de su milenario y por su sensibilidad e inquietud respecto de la seguridad, disponiendo del primer Departamento de Seguridad de una comunidad religiosa en el país, que dirige nuestro socio Jesús Alcantarilla.

El acto tuvo un emotivo momento al galardonarse con el Premio al mérito en el servicio en la seguridad pública, a título póstumo, a los integrantes de la Guardia Civil fallecidos en acto de servicio en los incidentes de Barbate, David Pérez y Miguén Ángel González. Junto a ellos se reconoció también el mérito al resto del operativo actuante. ■



## "Martes con..." en Madrid, 19 de Noviembre

### Cruz Roja Española

El pasado día 19 de Noviembre, ADSI celebró con éxito su "Martes con.." en la Cruz Roja, concretamente en el Edificio Corporativo de El Plantío bajo el título los "Sistemas de Seguridad y servicios de prevención". Tras el saludo inicial de bienvenida por parte del Presidente de ADSI, Eduard Zamora, dio comienzo la jornada.

Las ponencias se llevaron a cabo por:

**Doña. Marta Albuerne Llorente.** Coordinadora Autonómica de Programas de Igualdad de Oportunidades en el acceso al empleo.

**Doña. Susana Pérez Riveiro.** Directora Autonómica de Socorros y Emergencias de la Comunidad de Madrid.

- Desde el Área de Empleo, **Marta Albuerne**, presentó las principales iniciativas del Plan de Empleo, diseñado para fomentar la inclusión laboral de personas en situación de vulnerabilidad. Marta explicó cómo este plan combina orientación, formación y acompañamiento para facilitar el acceso al mercado laboral.

En el marco de esta presentación, se destacó la Campaña

#ContrataSin, una actividad de sensibilización orientada a promover la contratación de personas que enfrentan mayores barreras para encontrar empleo. Varias integrantes del equipo de colaboración empresarial subrayaron la importancia de que las empresas asuman un compromiso activo para integrar a colectivos tradicionalmente alejados del mercado laboral.

- Desde el Área de Socorros y Emergencias, **Susana Pérez**, hizo un recorrido detallado de los recursos destinados a la atención de las personas en situación de emergencia sanitaria. Durante su intervención, Pérez detalló los diferentes servicios desplegados en estos contextos, destacando el Transporte Sanitario Urgente, los Servicios Preventivos, los Equipos de Respuesta Básica en Emergencias y los cinco equipos de Respuesta Inmediata en Emergencias. Uno de los aspectos más relevantes abordados fue la gestión de los albergues provisionales. Se recalcó que estas instalaciones son fundamentales en emergencias de gran magnitud, pues requieren un elevado despliegue de recursos humanos y materiales.

El evento también puso en valor la importante labor de Cruz Roja en la DANA que afectó a diversas localidades.





Susana, destacó que la organización ha sido esencial en tareas de limpieza, desescombro y recuperación del entorno, a la vez que se lleva a cabo una atención sanitaria integral y se gestionan sistemas de comunicación y de intervención psicosocial para las personas afectadas. Tema que fue de interés común para las personas asistentes, sobre todo lo relativo a la organización tanto de personal voluntario como los recursos para apoyar las poblaciones que han sido afectadas por la DANA. La humanidad y el compromiso del voluntariado en esta área han sido fundamentales. Más de 3.000 personas voluntarias están apoyando la intervención de Cruz Roja, brindando un valor añadido, en las que el enfoque se centra en la persona y su bienestar integral.

La jornada finalizó con una exposición práctica en el exterior de las instalaciones, donde los asistentes pudieron observar de cerca vehículos y equipos utilizados en operaciones de emergencia.

Como colofón final, pudimos degustar de un cocktail-networking en compañía de todos los asistentes que nos pudieron acompañar. Gracias a todos ellos!!

Agradecer a cada uno de los ponentes la profesionalidad y la entrega prestada con ADSI para poder llevar a cabo esta interesante jornada y en especial a **Mariló Garrido Fernández, Técnica de Colaboración Empresarial** y a **Eva Grueso, Mediadora Social CAED Madrid (Carabanchel) Atención Humanitaria**, por su inestimable ayuda y colaboración para poder organizar esta jornada. ■

*Elvira Márquez*  
*Vicepresidenta de ADSI*



*"Martes con..." en Barcelona, 26 de Noviembre*

## Corporació Catalana de Mitjans Audiovisuals -3CAT

El pasado 26 de noviembre desde ADSI convocamos un nuevo "Martes con", que versó sobre "La seguridad en los medios de comunicación audiovisual de la Generalitat de Catalunya". El evento tuvo lugar en las instalaciones de la Corporación Catalana de Medios Audiovisuales-3 CAT (CCMA) en Sant Joan Despí (Barcelona). En este emplazamiento se localizan varios platós de televisión, redacciones, almacenes y Unidades Móviles, entre otros.

Tras la bienvenida a los asistentes, ponentes y al Departamento de Seguridad de la CCMA por acoger este evento a cargo del Presidente de ADSI, Eduard Zamora, se dio paso a tres interesantes ponencias sobre la:

**"Estructura y operativa del Departamento de Seguridad de la CCMA"**, a cargo de Albert Llarch (Director de Seguridad de la CCMA).

**"Material sanitario específico de los corresponsales que dan cobertura informativa en zonas hostiles"**, expuesto por Antoni Nicolau (Doctor Director del SMPRL de la CCMA).

**"Medios de protección de un corresponsal de guerra"**, con las experiencias de Carles de la Encarnación (filmmaker, reportero de guerra y catástrofes naturales).

La primera ponencia nos llevó a la constitución de la

Corporación Catalana de Medios audiovisuales -3CAT, en 1983, el ente público que gestiona los medios de comunicación audiovisual de la Generalitat de Catalunya, incluyendo canales de televisión, emisoras de radio y los contenidos digitales generados por estos medios. Todo esto con la misión de servicio público. Lluís Llarch siguió describiendo la estructura del Departamento de Seguridad, con Áreas como la Oficina Técnica, Protección y Vigilancia o Coordinación de los Servicios Generales.

Uno de los principales objetivos de este Departamento es garantizar la seguridad y protección de los profesionales de la comunicación mientras llevan a cabo su trabajo. Especialmente la seguridad de los periodistas desplazados en algunos lugares del mundo, destacando las regiones afectadas por conflictos armados o situaciones de violencia política que pueden poner en peligro integridad, hasta la vida, de los periodistas y limitan la libertad de prensa.

Las zonas hostiles o de riesgo se asocian a situaciones relacionadas con la sociedad, como los conflictos armados, violencia política o étnica, criminalidad muy elevada o la presencia de grupos extremistas. También constituyen eventos peligrosos los relacionados con las catástrofes naturales, la falta de infraestructuras y servicios o los riesgos sanitarios. Todos ellos son noticia y lleva a los profesionales a visitarlos en busca de la mejor información para los usuarios de la CCMA.



El doctor Nicolau nos explicó la importancia de un procedimiento claro en la preparación de las salidas a zonas hostiles, con los puntos concretos a revisar para tratar de manera específica e individual cada intervención de los desplazados en las zonas peligrosas.

Cuestiones como la documentación, medidas sanitarias, acompañantes desde origen o en local se preparan antes del desplazamiento, siendo habitual el poco tiempo entre la decisión de salida el inicio del viaje.

En coordinación con el Servicio Mancomunado de PRL del ente, se procura de los Equipos de Protección Individual (EPI) adecuados para cada situación, de acuerdo con la evaluación de riesgos específica para la zona y el tipo de hostilidad. El botiquín se constituye en indispensable, tanto uno individual como uno para el colectivo desplazado. El personal que acude a estas áreas de riesgo tiene una formación específica tanto de uso del botiquín, como de medias de autoprotección, a cargo de técnicos especialistas en estos entornos y dificultades que encontraran en el origen de la noticia. En la distancia, el contacto con estas personas desplazadas, y el seguimiento, es permanente.

La tarde siguió con la intervención de Carles de la Encarnación, enviado especial a muchos de los siniestros e incidentes de gran gravedad que ocurren en nuestro planeta. En su charla nos comentó la importancia de la preparación y recursos cuando está sobre el terreno, ya que trabaja y se mueve en entornos donde el peligro se manifiesta de manera imprevisible y constante, con gran probabilidad de sufrir daños. El ponente destacó la relevancia del compromiso y preocupación de los profesionales de la comunicación para informar y



conseguirlo de una manera segura.

Tras el turno de preguntas, contestadas por los tres oradores, se dio oportunidad a los asistentes de manipular los equipos de protección y se visitaron las instalaciones del canal de televisión. Al finalizar, disfrutamos de un ligero refrigerio mientras aprovechamos para saludar y compartir experiencias entre todos los asistentes, socios y amigos de ADSI.

Gracias a Albert Llarch y a Xavier Baixas del Departamento de Seguridad de la CCMA por su ayuda y colaboración para poder organizar este "Martes con.." a Antoni Nicolau y a Carles de la Encarnación por sus excelentes ponencias y a todos los socios y patrocinadores que nos pudisteis acompañar. ■

**Jordi Silvestre**  
**Vocal de ADSI**



# Actualización de datos de socios y amigos de ADSI

Estimado/a Socio/a, Amigo/a,

En su momento, nos aportasteis vuestros datos profesionales y personales, pero en muchas ocasiones estos han cambiado y nos dificulta el contacto con vosotros cuando nos es preciso.

Por ello, te agradeceríamos que:



Nos escribas un correo a:

- Elvira Márquez [vicepresidente@adsi.pro](mailto:vicepresidente@adsi.pro)
- Eduard Zamora [presidente@adsi.pro](mailto:presidente@adsi.pro)

Si eres socio de ADSI

**Indicando:**

*Nombre y apellidos  
Empresa y cargo  
Domicilio profesional  
E-mail profesional  
Teléfono de contacto*

*Domicilio particular  
E-mail particular  
Teléfono de contacto*

Si eres amigo de ADSI

**¿Deseas recibir nuestras comunicaciones? Facilitáanos tus datos, remarcando que no eres socio.**

Gracias por vuestra colaboración!





# La seguridad en los centros de datos: la importancia de proteger las infraestructuras críticas

Por Peter Dempsey de AXIS Communications

*Ha pasado más de 25 años en el sector de la seguridad ocupando varios puestos que le han permitido asumir la responsabilidad de elementos clave de proyectos de misión crítica y alto perfil en diferentes mercados verticales. Durante los últimos tres años, Peter ha centrado su enfoque en cómo las tecnologías de seguridad respaldan mejor la estrategia de seguridad de una empresa, a la vez que impulsa la adopción y eleva la importancia de la ciberseguridad y las tecnologías emergentes para los profesionales de la seguridad física en los centros de datos. La pasión de Peter por la industria se puede volver a atribuir al enorme éxito en Irlanda con las implementaciones de Hyper Scale y Multi-Tenant Data Centre (MTDC) en los últimos años.*

Los ciberataques pueden provenir de cualquier lugar y pasar desapercibidos durante años, por lo que es imperativo que los centros de datos dispongan de un hardware de seguridad resiliente para evitar la vulneración de unas normativas cada vez más estrictas.

Para los ciberdelincuentes, los centros de datos representan un premio lucrativo y atractivo, independientemente de si el objetivo del ataque es robar datos, interrumpir sistemas críticos o desplegar ransomware. Un centro de datos representa un gran número de sistemas, procesos y dispositivos de hardware, y solo se requiere una pequeña rendija en cualquiera de estos elementos para acceder al centro de datos. Si se puede explotar, ocurrirá, y hay muchas vías potenciales de entrada.

Se han encontrado más de 20000 sistemas de gestión de infraestructuras de centros de datos (DCIM) expuestos públicamente, y estos podrían permitir a un atacante interrumpir el funcionamiento de un centro de datos al alterar los umbrales de temperatura y humedad. Algunos sistemas de alimentación ininterrumpida (SAI) también han demostrado ser vulnerables, dando a los hackers acceso a la alimentación de los centros de datos. Y los centros de datos están llenos de dispositivos de Internet

of things (IoT) que podrían actuar como vectores de ataque. Los centros de datos deben ser conscientes de su vulnerabilidad y esforzarse por proteger cada uno de los elementos que componen su infraestructura.

## APT31 - Preparación para ataques ocultos

Es posible que muchos centros de datos ya hayan sido atacados silenciosamente. Los atacantes despliegan ataques «living off the land» (LOTL) cada vez más sofisticados que utilizan las herramientas habituales de los sistemas informáticos en lugar de instalar sus propios archivos maliciosos. Este tipo de infiltración es difícil de detectar y, de hecho, puede pasar desapercibida durante años hasta que el delincuente esté listo para atacar<sup>1</sup>.

Estos actores pueden ser entidades importantes. En muchos casos, se ha descubierto cargas LOTL procedentes de agentes financiados por estados que se esconden en redes críticas. El Centro Nacional de Ciberseguridad del Reino Unido ha implicado ahora a un grupo de piratería informática con financiación estatal, APT31, en un intento de atacar a un grupo de MP. En una lista de otros objetivos, la ciberamenaza APT31 se extiende a la economía del Reino Unido, a las infraestructuras nacionales críticas y a las cadenas de suministro<sup>2</sup>.

Esto pone de relieve la necesidad de que los responsables de los centros de datos adopten un enfoque proactivo en materia de seguridad, que no solo se base en principios conocidos de ciberseguridad, sino que emplee una supervisión activa y una diligencia debida estricta. Y esto es especialmente importante en el entorno normativo actual.



## NIS2 - Detección de anomalías de datos en infraestructuras críticas

La Directiva NIS2 (NIS2) y la Ley de Ciberresiliencia reclasifican los centros de datos como infraestructuras críticas. Ahora entran en la misma categoría que la sanidad, la energía y el transporte, y tendrán que cumplir con el mismo nivel de escrutinio sobre su gobernanza. Los operadores de centros de datos, sometidos a dicha legislación o no, no tienen otra opción que reforzar sus defensas.

El comportamiento de cada componente de hardware, software y firmware dentro de una red debe analizarse de forma periódica para detectar incluso la actividad inusual más inofensiva. Este trabajo de detección también debe extenderse más allá de los límites del centro de datos, ya que la NIS2 se aplica a las actividades de los colaboradores, así como a las entidades críticas. Esto incluye a los proveedores de equipos y, lo que es crucial, a cada paso de su cadena de suministro.

## Búsqueda de vulnerabilidades en la cadena de suministro

Si un atacante no puede infiltrarse en un centro de datos de forma directa, puede que intente inyectar una carga maliciosa en equipos que aún no se han implementado. Los dispositivos IoT son un terreno fértil para los delincuentes: están conectados a la red de forma predeterminada y a menudo no se inspeccionan con el mismo nivel de detalle que los vectores de ataque más obvios. Al igual que ocurre con las cargas LOTL, los dispositivos de IoT maliciosos pueden simplemente ocultarse a simple vista porque permiten a los atacantes infiltrarse basándose en una confianza implícita.

Los ataques a las cadenas de suministro son increíblemente peligrosos y están creciendo, superando los ataques directos de malware en un 40%3 en 2022. Ya

no hay forma de justificar una confianza implícita: los proveedores deben demostrar la seguridad y pureza de su cadena de suministro de forma detallada y adoptar medidas para garantizar que no se produzcan modificaciones no autorizadas. Los centros de datos, a su vez, deben reevaluar todas las relaciones con los proveedores para asegurarse de que no caer en ninguna trampa.

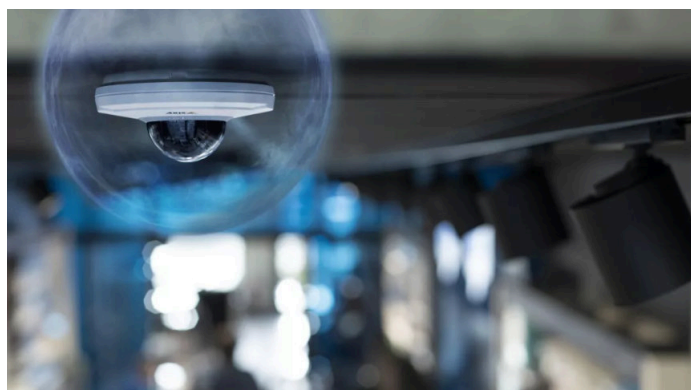
Afortunadamente, la tecnología moderna permite a los proveedores demostrar la legitimidad de su hardware de una forma bastante limpia. El hardware de un módulo de plataforma de confianza protege el firmware firmado, ofreciendo confianza en la integridad de un dispositivo a lo largo de toda la cadena. El arranque seguro evita que se ejecute firmware no autorizado. Y algunos dispositivos pueden almacenar claves y certificados criptográficos de forma segura en su interior, lo que refuerza sus credenciales de seguridad y simplifica el proceso de gestión de las defensas.

## Cómo hacer frente a la presión normativa

Las regulaciones como la NIS2 básicamente obligan a los centros de datos a actuar ahora o enfrentarse a grandes sanciones. Sus términos hacen que los directores de los centros de datos sean responsables no solo de las filtraciones internas, sino también de las causadas por determinados fallos de seguridad de terceros. La seguridad debe reevaluarse de arriba a abajo.

Una sólida seguridad física a través de cámaras, detección térmica, radar y un sistema de control de acceso es claramente fundamental, ya que un atacante en las instalaciones podría causar interrupciones inesperadas. Pero la seguridad lógica es igual de vital para garantizar que los atacantes no accedan a las instalaciones de forma virtual. Cada pieza de hardware y software, ya sea dentro del alcance de las regulaciones o no, debe catalogarse, analizarse, priorizarse y documentarse de forma periódica.

La conformidad debe demostrarse con un registro claro, y los proveedores también deben proporcionarla. Ningún proveedor que se valore desearía suministrar algo que no esté al nivel requerido; trabajar con proveedores que se preocupan por sus productos es el camino para que los centros de datos creen un mundo más seguro e inteligente. ■



## La gestión del servicio de Atención al Visitante y Seguridad en el Museo Nacional del Prado

Desde hace un año llevamos a cabo la gestión del servicio de Atención al Visitante y Seguridad en el Museo Nacional del Prado, un reto que ha supuesto una oportunidad para desplegar nuestra capacidad operativa, técnica y humana en uno de los entornos culturales más prestigiosos del mundo. Este proyecto nos ha permitido demostrar nuestra habilidad para adaptarnos a las necesidades de un espacio que combina un alto nivel de exigencia operativa con la necesidad de ofrecer una experiencia inolvidable a millones de visitantes cada año.

Desde el inicio, implementamos un plan de implantación que garantizara una transición fluida y eficiente. La prioridad fue establecer una coordinación efectiva entre los diferentes departamentos del Museo y nuestro equipo, para asegurar que cada aspecto del servicio se integre de manera ordenada y funcional. Esto incluye la capacitación intensiva del personal en los valores y procedimientos del Museo, así como en el uso del sistema tecnológico Puerta Digital, pieza clave en la gestión de accesos y entradas. La rapidez y eficacia de esta implantación permitieron que los servicios comenzaran a operar con total normalidad desde el primer día.

Uno de los elementos que ha marcado la diferencia en nuestra gestión es el uso de materiales y herramientas de última generación. **Hemos dotado al proyecto con recursos tecnológicos avanzados, como dispositivos electrónicos para la gestión de accesos, cámaras de seguridad CCTV, controles electrónicos y otros sistemas que garantizan un entorno seguro y organizado para los visitantes.** Además, para fomentar la accesibilidad, hemos puesto a disposición del Museo equipos auxiliares como sillas de ruedas, bastones y sillitas de bebé, asegurando una experiencia inclusiva para todos los públicos. Estos materiales, junto con la capacitación continua de nuestro equipo, nos permiten ofrecer un

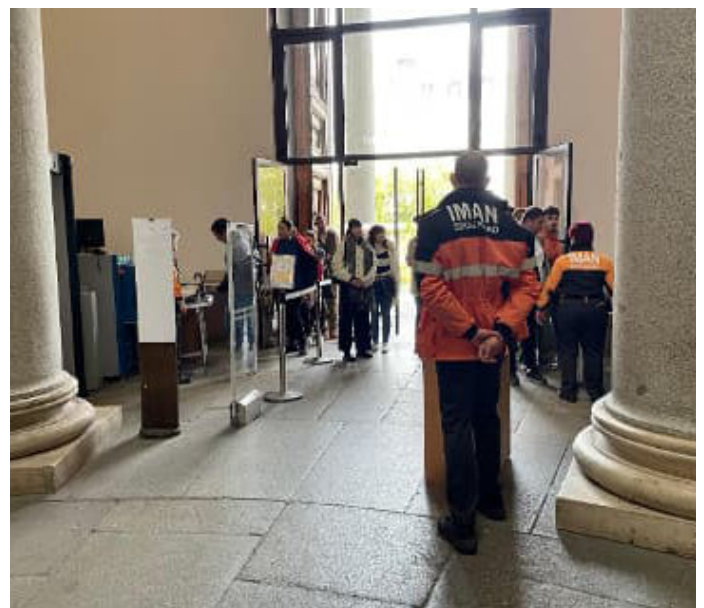
servicio impecable, adaptado a las necesidades específicas del Museo y sus visitantes.

La comunicación ágil y constante con el cliente ha sido un pilar fundamental para el éxito de este proyecto.

**Mantenemos un flujo continuo de información con los responsables del Museo, lo que nos permite adaptarnos rápidamente a cualquier necesidad o incidencia. Gracias a esta proximidad, hemos implementado soluciones efectivas que optimizan tanto la atención al visitante como la seguridad de las instalaciones.**

Nuestra capacidad de respuesta ágil ha sido clave para gestionar situaciones especiales, como eventos temporales o exposiciones de gran envergadura, asegurando siempre una experiencia satisfactoria para los asistentes.

**Otro aspecto destacado ha sido la coordinación con los distintos departamentos del Museo. La diversidad de actividades y espacios que engloba esta institución**



requiere un enfoque integral que facilite la interacción entre todas las áreas implicadas. Hemos trabajado estrechamente con departamentos de logística, eventos y seguridad, diseñando estrategias que aseguren la alineación de objetivos y la correcta ejecución de cada tarea. Este esfuerzo conjunto ha sido esencial para gestionar tan variadas actividades como exposiciones temporales, eventos institucionales y visitas de alto perfil, garantizando siempre un desarrollo impecable.

En este primer año de gestión, hemos logrado hitos significativos que nos llenan de orgullo.

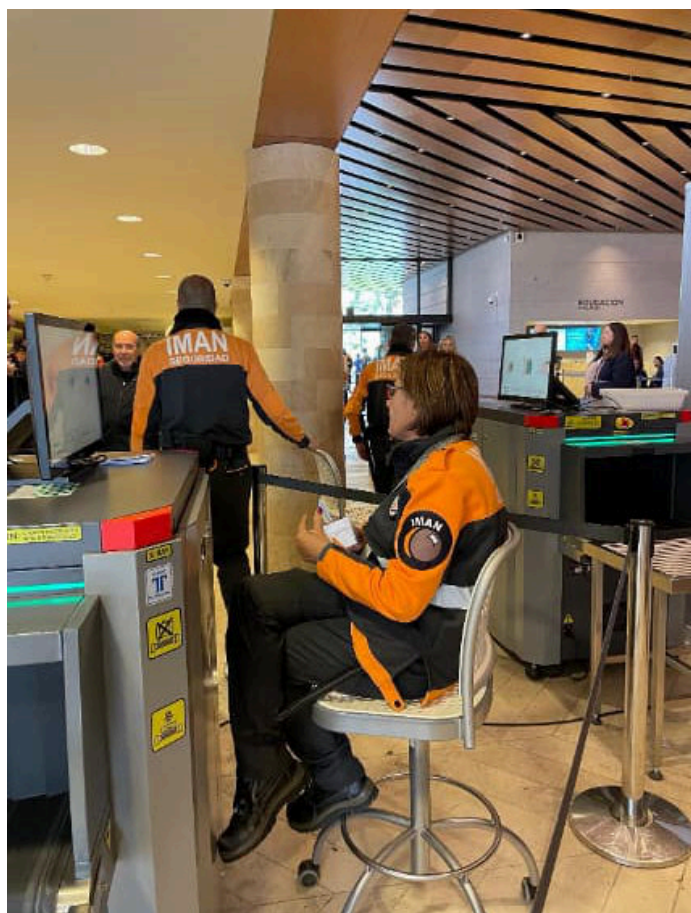
Hemos mejorado la experiencia de los visitantes mediante procesos más ágiles y un personal altamente capacitado, hemos reforzado la seguridad del Museo con tecnología de vanguardia y protocolos adaptados, y hemos establecido un sistema de comunicación y coordinación con el cliente que nos permite anticiparnos a sus necesidades.

Todo esto refleja nuestro compromiso con la excelencia y

nuestra capacidad para afrontar proyectos de gran envergadura.

Este proyecto no solo representa un logro significativo para nuestra organización, sino también una oportunidad de contribuir al desarrollo y preservación de un espacio cultural único. Cada día nos esforzamos por superar nuestras expectativas, garantizando que cada visitante disfrute de una experiencia enriquecedora y segura. Seguimos avanzando con el mismo entusiasmo que nos trajo hasta aquí, convencidos de que cada desafío es una oportunidad para innovar y aportar valor.

**Agradecemos al Museo Nacional del Prado por su confianza ya todo nuestro equipo por su dedicación y esfuerzo diario. Este caso de éxito refuerza nuestra misión de ser un referente en la prestación de servicios de atención y seguridad, demostrando que, con compromiso y excelencia, somos capaces de marcar la diferencia. ■**





## Producción bajo control en el sector del automóvil gracias a la tecnología de vídeo

Esta empresa automotriz ha dado un paso adelante implementando una solución innovadora de videovigilancia SCATI que eleva la seguridad y eficiencia en cada proceso productivo.



### Reto

Esta empresa del sector de la automoción se enfrentaba a varios desafíos en distintas áreas de su planta de producción, todos relacionados con la necesidad de una supervisión precisa y una gestión eficiente de los procesos automatizados. En su línea de producción laser, se requería una supervisión constante y eficaz para garantizar la calidad y la eficiencia, con el objetivo de mantener una visión clara de los puntos críticos y detectar cualquier incidencia. Además, en la zona del almacén vertical, era necesario implementar una solución para la supervisión detallada y en tiempo real de la manipulación de piezas en un entorno dinámico.

Por otro lado, esta empresa también buscaba un sistema de videograbación portátil para reportar visualmente averías en sus máquinas, que fuera compacto, fácil de transportar y adaptable para su uso en diferentes áreas de la planta. Finalmente, en la zona de prensas y el foso se necesitaba modernizar su sistema de videovigilancia, migrando de cámaras analógicas a una solución IP estandarizada para gestionar cámaras y grabadores en una única plataforma.

La solución debía garantizar una operación continua y confiable, incluso durante fallos eléctricos, evitando interrupciones en la producción.

### Solución

SCATI diseñó y proporcionó una solución llave en mano totalmente personalizada para esta empresa del sector de la automoción, atendiendo a sus necesidades específicas y exigencias operativas. La solución se organizó en diversas aplicaciones según las áreas de uso de las cámaras:

#### Supervisión de línea de producción

En la línea de producción laser, se instalaron cuatro cámaras IP de alta resolución, ubicadas estratégicamente para supervisar cada paso del proceso automatizado. Tres de estas cámaras se utilizaron para el control detallado de las áreas críticas como el manejo de piezas por parte del operario y el almacenamiento o extracción de estas, facilitando la identificación de anomalías en tiempo real.



La cuarta cámara ofrece una visión general de este entorno de trabajo.

Además, SCATI integró un monitor de 55 pulgadas, que permite al equipo visualizar en directo todos los ángulos de la línea de producción, optimizando el flujo de trabajo mediante la conexión a un grabador SCATI VISION Serie G500 con capacidad para gestionar hasta 8 canales y 8TB de almacenamiento. Con el software SCATI WALL, los operadores pueden gestionar las cámaras de manera intuitiva y rápida.

### Control del almacén vertical

SCATI implementó dos cámaras de última generación, compactas, de alto rendimiento para controlar el movimiento de piezas, asegurando la trazabilidad. Estas cámaras están conectadas a un sistema de grabación que permite la visualización y control en tiempo real desde el área administrativa.

### Grabación portátil para inspección y mantenimientos

Además de la instalación fija, SCATI implementó un sistema de grabación portátil para las tareas de inspección y mantenimiento. Este sistema, compuesto por cámaras compactas Pinhole IP y un grabador, permite a los operarios registrar y documentar visualmente las inspecciones de las máquinas. El sistema ofrece flexibilidad para capturar imágenes en lugares de difícil acceso y permite moverlo a cualquier área que sea necesaria.

### Migración y centralización en la zona de prensas y el foso

SCATI realizó una migración de cámaras analógicas a cámaras IP. El sistema de grabación actual está compuesto por tres grabadores SCATI VISION que

permiten gestionar 16 cámaras. Gracias a este sistema, los operarios tienen acceso centralizado a las imágenes de las cámaras de las prensas y del foso, facilitando una gestión homogénea y mejorando la capacidad de respuesta ante cualquier incidencia.

Un aspecto clave en cada una de las fases, fue la implementación de cuatro Sistemas de Alimentación Ininterrumpida (SAI), asegurando el funcionamiento continuo de todas las cámaras y grabadores, incluso ante cortes de energía. Esto garantiza que las operaciones de vigilancia nunca se vean interrumpidas, protegiendo tanto la integridad de las imágenes como el control del proceso productivo.

El equipo técnico de SCATI se encargó de la puesta en marcha de todos los sistemas, realizando ajustes específicos y asegurando que cada dispositivo estuviera correctamente configurado y operando a pleno rendimiento. Estos servicios incluyeron rondas de supervisión, revisiones periódicas del funcionamiento de los equipos y la entrega de informes detallados sobre el estado de las aplicaciones, permitiendo una implementación rápida y optimizando el uso de los sistemas desde el primer día.

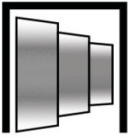
## Beneficios

La solución de SCATI ha transformado las operaciones de esta empresa automotriz, permitiendo una supervisión detallada y precisa de las áreas críticas de la planta. Las cámaras han facilitado la identificación y corrección de errores en tiempo real, optimizando la precisión y eficiencia en la producción, reduciendo tiempo de inactividad y mejorando la productividad general. La implementación en el almacén vertical ha transformado el control y la trazabilidad de piezas y ha disminuido errores de manipulación.

El respaldo de energía con el Sistema de Alimentación Ininterrumpida (SAI) asegura que las operaciones de vigilancia y monitoreo continúen sin interrupciones, proporcionando tranquilidad al mantener el control sobre la producción en todo momento.

En conclusión, la solución integral de SCATI no solo refuerza la seguridad física de las instalaciones, sino que también impulsa la eficiencia y mejora los procesos operativos de esta empresa del sector de la automoción. Con la combinación de cámaras de alta calidad, un sistema de gestión de video intuitivo y una infraestructura respaldada por un SAI, esta empresa ha optimizado su operación diaria, maximizando tanto la seguridad como la eficiencia en sus procesos. ■





## **Puertas Gismero consigue la certificación EI-120 para puertas de 2 hojas con mirilla**

Desde el inicio de nuestra trayectoria, nos hemos distinguido por el alto nivel de implicación en cada proyecto que acometemos.

Concebimos cada obra como única y por ello producimos específicamente para ella, y dada la gran variedad de soluciones que se nos plantean cada día, surge la necesidad de realizar con frecuencia ensayos de nuevas tipologías de puertas o incorporar prestaciones añadidas a las tipología más solicitadas, como pueden ser distintos herrajes, mirillas, cierres de seguridad, tipo de apertura, etc., en definitiva, aquellas que demanden nuestros clientes para sus proyectos, tanto para obra nueva como para rehabilitación de edificios existentes, con los más variados usos.

Por ello, llevamos años contando con los mejores laboratorios de ensayos de resistencia al fuego, que nos ofrecen las mayores garantías de calidad, que así mismo trasladamos a nuestros clientes. El último ensayo se ha realizado para certificar la resistencia al fuego de puertas de 1 y 2 hojas a 120 min, el cual ha resultado un gran éxito al haberse superado holgadamente este límite como puede comprobarse en las imágenes. ■



**Puertas antes del ensayo**



**Ensayo resistencia al fuego de puerta de 2 hojas 1800 x 2200 mm con mirillas** →





## El impacto de la directiva NIS2 en infraestructuras críticas

“En el marco de la Directiva Europea NIS2, las empresas españolas se enfrentan a un reto crucial: reforzar la ciberseguridad de sus infraestructuras críticas y cumplir con normativas estrictas que buscan proteger sectores clave.”



Conversamos con Óscar Rubí, Director del Departamento de Ingeniería de By Demes, sobre las implicaciones de esta normativa en el mercado español y las soluciones tecnológicas que su equipo está liderando.

### ¿Cómo afecta la Directiva NIS2 al mercado español?

La Directiva NIS2 supone un cambio significativo en cómo las empresas españolas abordan la ciberseguridad. Esta normativa **refuerza los requisitos de protección** en sectores estratégicos como la energía,

las telecomunicaciones, la sanidad y el transporte, que son pilares esenciales de la economía española.

España ya cuenta con experiencia en la protección de infraestructuras críticas gracias a la Ley 8/2011, pero NIS2 amplía considerablemente los sectores obligados a cumplir con estas medidas. **Esto incluye a empresas medianas que, hasta ahora, no estaban obligadas a implementar medidas avanzadas de ciberseguridad.** Desde By Demes, trabajamos para ofrecer soluciones adaptadas al nuevo paradigma, ayudando a nuestros clientes a cumplir con los nuevos requisitos y a estar mejor preparados ante posibles amenazas.



## ¿Cómo ayuda By Demes a las empresas a cumplir con la NIS2?

En By Demes contamos con una **gama de productos y servicios diseñados específicamente para cumplir con los requisitos de la Directiva NIS2**. Por ejemplo, nuestras soluciones de videovigilancia de Honeywell, Mobotix o TYCO, cumplen los más exigentes estándares de ciberseguridad, como el cifrado avanzado, el monitoreo de amenazas cibernéticas o las actualizaciones de software automáticas. Estas características garantizan que las infraestructuras críticas estén protegidas contra ataques externos y cumplan con las normativas europeas más exigentes.

Además, trabajamos mano a mano con nuestros clientes para ofrecer asesoramiento personalizado, **analizando las necesidades específicas de cada instalación**. Esto incluye desde el diseño del sistema hasta su implementación, asegurándonos de que todos los componentes, como cámaras, control de accesos y plataformas de gestión centralizada, sean compatibles con las directrices de NIS2.

## ¿Qué papel juega la videovigilancia en la protección de infraestructuras críticas?

La videovigilancia es uno de los pilares clave en la protección de infraestructuras críticas. Más allá de la mera captura de imágenes, hoy en día estos sistemas ofrecen análisis inteligente de vídeo, detección de anomalías y capacidades de integración con otras tecnologías de seguridad, como alarmas y controles de acceso.

Con la NIS2, es fundamental que estos sistemas sean robustos en términos de ciberseguridad. Por ello, trabajamos con las marcas mencionadas anteriormente, que integran cifrado avanzado y herramientas de monitoreo en tiempo real. Estos elementos no solo protegen la infraestructura física, sino también los datos sensibles que podrían ser objeto de un ataque cibernético.

## ¿Cómo perciben los clientes de By Demes los retos que plantea la NIS2?

En general, las empresas son **cada vez más conscientes de la importancia de proteger sus sistemas frente a ciberamenazas**. Sin embargo, muchos desconocen la complejidad de la implementación de medidas que cumplan con la NIS2. Aquí es donde By Demes marca la diferencia: no solo ofrecemos los productos, sino también la experiencia y el soporte técnico necesarios para garantizar que los proyectos estén alineados con esta normativa.

Hemos visto un **aumento significativo en la demanda de soluciones integradas**, donde la ciberseguridad y la videovigilancia trabajan juntas. Los clientes buscan sistemas que no solo cumplan con los requisitos legales, sino que también aporten un valor añadido en términos de eficiencia operativa y gestión centralizada.

## ¿Qué mensaje le daría a las empresas que aún no se han adaptado a la NIS2?

El cumplimiento de la NIS2 **no es solo una obligación legal, sino también una inversión en el futuro de sus operaciones**. Las amenazas cibernéticas y los riesgos asociados a la falta de preparación son demasiado altos como para ignorarlos. En By Demes estamos preparados para guiar a las empresas en este proceso, ofreciéndoles soluciones a medida que no solo cumplen con la normativa, sino que también potencian su seguridad y competitividad.

Invitamos a todas las empresas a explorar nuestras soluciones, desde videovigilancia avanzada hasta herramientas de monitoreo y análisis, que están diseñadas para proteger las infraestructuras más críticas. ■



# DIRECCIÓN DE SEGURIDAD DIGITAL Y GESTIÓN DE CRISIS

FORMACIÓN PARA NO TÉCNICOS

**10%**  
Desuento Socios ADSI

TERCERA EDICIÓN

**MÁS  
INFORMACIÓN**



## MÁSTER UNIVERSITARIO EN PROMOCIÓN PROFESIONAL PARA LA GESTIÓN DE CRISIS EN SEGURIDAD Y DEFENSA

UNIVERSIDAD CATÓLICA DE ÁVILA

DIRECTOR: Dr. Alberto Barea Vera

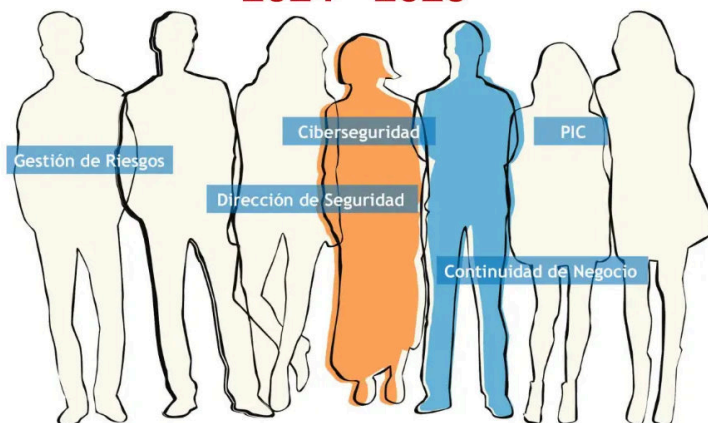
CODIRECTOR: Coronel José Luis Calvo Albero



**20%  
descuento  
ADSI**

**DESCARGAR  
INFORMACIÓN**

## CURSOS PARA LA ESPECIALIZACIÓN DE DIRECTIVOS DE SEGURIDAD 2024 - 2025



Aumento de la Profesionalización de la Seguridad GRUPO ESTUDIOS TÉCNICOS diseña e imparte desde 1988 convocatorias (cursos, seminarios, congresos, jornadas y presentaciones) para la formación, capacitación y especialización.

Dirigido a: Directores de Seguridad, Fuerzas y Cuerpos de Seguridad Pública, Jefes y Responsables de empresas de Seguridad, Ingenieros, Consultores, Técnicos y Prescriptores, Instaladores, mantenedores y operadores, Responsables de gestión y Profesionales, Usuarios de sistemas y servicios.

Gracias al acuerdo de colaboración entre GET y ADSI, los asociados a ADSI disponen de un 20% de descuento en Cursos bonificables. Desde GET, realizan la consulta del crédito disponible, así como la tramitación de la bonificación en caso de realizar algún curso.



**Curso de Especialista en Seguridad en Infraestructuras Críticas y Estratégicas**

[Enlace](#)



**Curso Superior de Dirección y Gestión de Seguridad Integral 23/24**

[Enlace](#)



**Master de Formación Permanente en Cibersecurity Management**

[Enlace](#)



UNIVERSITAT DE BARCELONA

**Máster en Dirección de Seguridad Privada**

[Enlace](#)



**Grado en Prevención y Seguridad Integral (100% a distancia)**

[Enlace](#)



**Grado de Criminología y Dirección de Seguridad**

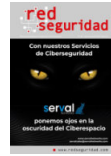
[Enlace](#)





**Revista Seguritecnia.**  
Nº 510 Nov-Dic 2024.

[Enlace](#)



**Revista Red Seguridad.**  
Nº 107 4º Trimestre 2024.

[Enlace](#)



**Revista Cuadernos de Seguridad.**  
Nº 378 Noviembre 2024.

[Enlace](#)



**Revista Logos G.C.**  
Nº 3 2º Semestre 2024.

[Enlace](#)



**Guardia Civil. Dirección Adjunta Operativa. Policía Judicial.**  
**Documento de Análisis de Riesgos y Difusión Operativa DARDO 10/2024**

[Enlace](#)



**Informe sobre la situación y las tendencias del terrorismo en la Unión Europea (TE-SAT) 2024**

[Enlace](#)



**Ciberseguridad 2025. Amenazas, desafíos, tendencias y oportunidades.**

[Enlace](#)



**La ONU y la Organización Meteorológica Mundial reclaman más esfuerzos en adaptación frente a eventos extremos como la DANA.**

[Enlace](#)



**Grande-Marlaska anuncia que Cádiz acogerá la próxima cumbre de la Coalición contra el Crimen Organizado**

[Enlace](#)



**Despliegue de Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad del Estado en el exterior diciembre 2024.**

[Enlace](#)



**El Gobierno invertirá cerca de 62 millones de euros en la primera fábrica de Inteligencia Artificial en España.**

[Enlace](#)



**INCIBE presenta un informe pionero sobre la seguridad de los juguetes conectados en el marco de la Ley de Ciberresiliencia de la UE.**

[Enlace](#)



**DSN**

**La Resiliencia en el Marco de la Seguridad Nacional.**

[Enlace](#)



**DSN**

**Estrategia Nacional de Seguridad Marítima 2024**

[Enlace](#)

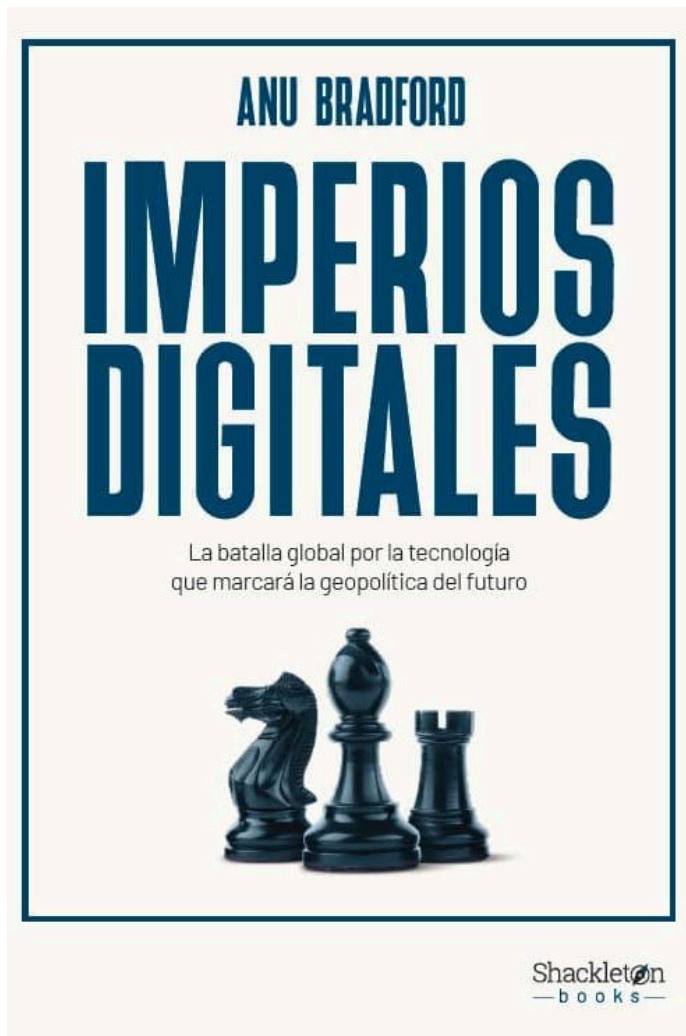


**Consulta sobre el proyecto de acto de ejecución en virtud de la Directiva SRI2.**

[Enlace](#)



# Imperios digitales: La batalla global por la tecnología que marcará la geopolítica del futuro



## **Autor: Anu Bradford**

Un brillante ensayo que analiza las estrategias de Estados Unidos, la UE y China por el control de la tecnología, el recurso que marcará la agenda geopolítica del futuro.

Para la sociedad industrial del siglo XX, el petróleo fue uno de los recursos más codiciados y poderosos. No se puede entender la historia reciente (alianzas internacionales, golpes de Estado, guerras...) sin tener en cuenta los intereses de las compañías petroleras y los intentos de diversos países por asegurarse este precioso suministro.

En el siglo XXI, las personas, empresas y Estados dependen cada vez más de las tecnologías digitales, que a su vez están condensadas en manos de un puñado de empresas. La rápida adopción de estas tecnologías da paso a una economía excesivamente concentrada, en la que las empresas del sector tecnológico y digital controlan el mercado y la política, socavan la privacidad y amplían la brecha entre ganadores y perdedores económicos. Nadie duda de que los líderes mundiales deben poner límites a la actividad de estas grandes corporaciones digitales.

Este es el escenario en el que está llamada a desarrollarse la nueva batalla geopolítica mundial. Una guerra invisible en la que tres potencias globales (Estados Unidos, China y la Unión Europea) intentan controlar el nuevo "petróleo digital", al tiempo que luchan por ampliar su esfera de influencia en el incierto mundo tecnológico.

La prestigiosa investigadora Anu Bradford examina las tres estrategias que caracterizan a cada uno de estos bloques (el modelo estadounidense, impulsado por el mercado; el modelo chino, impulsado por el Estado; y el modelo europeo, impulsado por los derechos civiles) y analiza cómo gobiernos y empresas tecnológicas sortean los conflictos que surgen cuando estos enfoques tan diferentes chocan en el ámbito internacional.

¿Qué imperio digital prevalecerá en la pugna por la influencia global? En este magnífico ensayo, Bradford explora la determinante rivalidad que configurará nuestro mundo durante las próximas décadas. ■





# ADSI

asociación de directivos  
de seguridad integral