

Informe de conclusiones

# Defensa y tecnologías duales: La consultoría ante el reto de la seguridad.





Empresas que integran la AEC:

ACCENTURE · ALTIA · ATMIRA · ATOS · AYESA · BLUETAB · CAPGEMINI · CEDEC · CEGOS · DELOITTE · DXC TECHNOLOGY  
EY · IBM · INETUM · IZERTIS · KPMG · MINSAIT · NTT DATA · GRUPO OESÍA · SEIDOR · SOPRA STERIA  
TATA CONSULTANCY SERVICES · UNISYS · VASS · VIEWNEXT · WORLDLINE

[Se permite la reproducción, con fines no comerciales, de los gráficos y/o textos que integran este documento, siempre que se cite expresamente como fuente la Asociación Española de Empresas de Consultoría.]

**Diciembre de 2025**

# Índice

I.	Introducción	04
II.	Retos en defensa y seguridad. Soluciones desde la consultoría:	06
	a) Ciberseguridad y ciberinteligencia: inversión estratégica	06
	b) Integración y adopción de tecnologías duales	07
	c) Desarrollo de capacidades, talento y conocimiento	08
III.	Tecnologías de doble uso y casos prácticos:	10
	a) IA y el Machine Learning como motor dual	10
	b) Analítica avanzada y gemelos digitales	11
	c) Telecomunicaciones 5G/IoT y conectividad multidisciplinar	12
IV.	Impacto en el sector y en el conjunto de la economía	13
V.	Consideraciones finales	15
	Reconocimientos	17

# I. Introducción

El Informe de *Conclusiones Defensa y tecnologías duales: la consultoría ante el reto de la seguridad* busca reflejar el papel estratégico que desempeña la consultoría tecnológica en el nuevo ciclo inversor en defensa y seguridad que tiene lugar en España y Europa. En un contexto marcado por la guerra en Ucrania, las crecientes amenazas a la ciberseguridad y un entorno geopolítico cada vez más complejo, la defensa se ha convertido en una prioridad europea que requiere soluciones tecnológicas avanzadas, innovación y colaboración entre el sector público y privado.

Por primera vez en su historia reciente, España ha alcanzado en 2025 el objetivo del 2% del PIB en gasto militar establecido por la OTAN. El Gobierno ha anunciado una inversión adicional de más de 10.000 millones de euros destinados, entre otras prioridades, a modernizar sistemas de telecomunicaciones, reforzar la ciberseguridad de infraestructuras críticas e impulsar las tecnologías duales, es decir, aquellas con aplicación tanto en el ámbito militar como en el civil.

En el ámbito europeo, la Comisión Europea ha establecido mecanismos de financiación comunitaria para el desarrollo de capacidades militares conjuntas, como el instrumento SAFE, del que España se beneficia con 1.000 millones de euros en préstamos.

Este compromiso representa una apuesta decidida por la modernización de las capacidades de defensa y seguridad, un ámbito en el que la tecnología, la innovación y el talento especializado de las empresas consultoras tienen mucho que aportar. Además, este nuevo marco refuerza la necesidad de consolidar la autonomía estratégica y la soberanía tecnológica europea, reduciendo la dependencia de terceros países en sectores críticos para la seguridad.

Es en este punto de inflexión cuando las empresas de consultoría tecnológica se consolidan como aliadas imprescindibles para la modernización de las Fuerzas Armadas. Las consultoras asociadas a la AEC prevén un crecimiento cercano al 30% en sus ingresos procedentes del sector de la defensa y la ciberseguridad en 2025. En concreto, se espera un aumento del 28,9%, pasando de 1.125 millones de euros en 2024 a 1.450 millones este año.

Este notable incremento refleja el papel cada vez más estratégico de la consultoría tecnológica en la transformación digital de las capacidades de defensa, en la protección de infraestructuras críticas y en el desarrollo de tecnologías duales. Las consultoras aportan capacidades avanzadas en ciberseguridad, inteligencia artificial, *cloud computing* de alta seguridad, incluida la nube de combate, computación cuántica, *blockchain*, IoT (Internet de las cosas), robótica, sistemas autónomos o *big data*; además de participar en el sector aeroespacial y los satélites de baja intensidad.

Estas tecnologías contribuyen a fortalecer la base industrial y tecnológica en España, generan empleo cualificado, impulsan la colaboración público-privada y posicionan a las empresas españolas en programas europeos de alto valor estratégico.

Todo ello es posible gracias al liderazgo que ejerce la consultoría en innovación, invirtiendo el 5,6% de sus ingresos en I+D+i, más de tres veces la media nacional; así como en formación, destinando más de 100 millones de euros anuales a la capacitación continua de sus profesionales.

Ante la oportunidad histórica para consolidar a España como referente europeo, el sector de la consultoría ha demostrado ser fundamental en el ecosistema de innovación y talento que, en colaboración con las instituciones públicas y las Fuerzas Armadas, contribuye a garantizar la seguridad, la competitividad y la soberanía tecnológica de nuestro país.

## Antecedentes

La Asociación Española de Empresas de Consultoría (AEC) es la referencia del sector en España y agrupa a 26 de las empresas más importantes de consultoría y tecnologías de la información. Este sector está liderando los procesos de transformación digital en España, contribuyendo al cambio del modelo productivo y a la modernización de la economía y de los servicios públicos. Con una aportación del 1,4 % al PIB y más de 285.000 profesionales, la consultoría es un motor esencial del crecimiento y la competitividad en España. La AEC, además, representa al sector en el ámbito europeo como miembro de la Federación Europea de Asociaciones de Consultoría (FEACO).

La AEC está comprometida con la producción y la divulgación de conocimiento especializado, abordando asuntos de actualidad e interés público. Para ello, organiza foros, encuentros con expertos y medios de comunicación, y genera informes y documentos de análisis que contribuyen a un debate informado en beneficio de la sociedad.

En ese marco de actividades, la AEC organizó el Desayuno informativo *Defensa y tecnologías duales: la consultoría ante el reto de la seguridad* en noviembre de 2025 en Madrid. Este informe recoge las conclusiones más relevantes expuestas durante el evento por diferentes especialistas de compañías asociadas a la AEC.

## II. Retos en defensa y seguridad. Soluciones desde la consultoría

### a) Ciberseguridad y ciberinteligencia: inversión estratégica

La ciberseguridad y la ciberinteligencia se han consolidado como elementos centrales en la estrategia de defensa y seguridad nacional. El Plan Industrial y Tecnológico para la Seguridad y la Defensa, dotado con 10.471 millones de euros en 2025, destina el 31% de la inversión a ciberseguridad, una cifra que evidencia que la seguridad nacional ya no depende únicamente de la capacidad armamentística, sino también de la capacidad para proteger la información, los sistemas de comunicación y las infraestructuras críticas.

En un panorama geopolítico cada vez más complejo, la información y la tecnología son instrumentos de poder y disuasión. Es necesario garantizar la continuidad operativa de los servicios y reforzar el concepto de resiliencia.

El año 2025 marca un cambio profundo en la evolución normativa con la implementación de NIS 2 (Directiva de ciberseguridad de redes y sistemas de información), DORA (Digital Operational Resilience Act), el Esquema Nacional de Seguridad (ENS) y la adopción generalizada del modelo Zero Trust (desconfianza por defecto). Además, la incorporación de IA segura certificada por ISO/IEC 42001 está redefiniendo la gobernanza de la ciberseguridad hacia un enfoque soberano, cooperativo y proactivo.

España enfrenta un desafío crítico: sufre más de 1.000 ciberataques anuales a servicios esenciales e infraestructuras críticas. Estos ataques no solo comprometen la seguridad nacional, sino que pueden paralizar sectores estratégicos, afectando a millones de ciudadanos y generando pérdidas económicas millonarias. Ante esta realidad, las consultoras tienen la capacidad de ofrecer soluciones que anticipen, protejan, recuperen y fomenten la resiliencia.

#### La ciberinteligencia como ventaja competitiva

En la actualidad, no es suficiente con reaccionar de manera idónea a los ciberataques. Es fundamental anticiparse. La ciberinteligencia actúa como factor preventivo, ayudando a analizar escenarios, detectar patrones de comportamiento, entender nuevos riesgos y amenazas emergentes, y anticiparse a su dinamización fruto de la evolución tecnológica.

La inversión en ciberseguridad y la ciberinteligencia representan una palanca de innovación, competitividad y crecimiento. Invertir en ellas es invertir en el futuro del tejido empresarial y en la evolución del concepto tradicional de la defensa hacia el nuevo orden mundial.

Las consultoras están trasladando cada vez más sus servicios de ciberseguridad al sector de la defensa, especializándose en la implementación de sistemas de carácter clasificado y desarrollando nuevas herramientas que permiten la gestión integral, unificando conceptos como inteligencia artificial, cumplimiento normativo y análisis de exposición.

Los nuevos retos incluyen la demanda de interconexiones cada vez más complejas, servicios en la nube e interdependencias entre operadores críticos. Esto implica que el sector privado debe garantizar infraestructuras seguras y operativas que respondan a necesidades emergentes. Además, la seguridad digital exige cooperación público-privada y visión a largo plazo. Por todo ello, la inversión en ciberseguridad y ciberinteligencia en el presente es una inversión en la defensa del futuro.

## b) Integración y adopción de tecnologías duales

Las tecnologías duales son el principal motor de innovación, transformación y creación de capacidades militares en España y Europa. Su característica definitoria es su doble aplicación: desarrolladas inicialmente en el ámbito civil, estas tecnologías encuentran aplicaciones estratégicas en el mundo militar, y viceversa. Este fenómeno ha invertido el paradigma tradicional donde la innovación fluía únicamente desde el sector militar hacia el civil.

La consultoría tecnológica ha evolucionado de ser un simple integrador a convertirse en un socio estratégico esencial para que un país como España transforme la innovación civil en capacidad operativa real y soberanía tecnológica. Las empresas consultoras actúan como catalizadores, acelerando la capacidad táctica y garantizando la autonomía estratégica del país.

### Contexto y retos del entorno actual

El entorno de defensa y seguridad es ahora multidominio e híbrido. Los conflictos actuales combinan operaciones convencionales con ciberespacio, guerra electrónica, desinformación y amenazas asimétricas. Este contexto está marcado por una explosión de datos procedentes de sistemas C5ISR (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance), que requieren procesamiento en tiempo real para la toma de decisiones operativas.

Además, la obsolescencia tecnológica acelerada presenta un desafío crítico: los ciclos tradicionales de adquisición militar, que pueden durar entre 10 y 15 años, no pueden seguir el ritmo de innovación del sector civil, donde las tecnologías se renuevan cada 2 o 3 años. Este desfase temporal pone en riesgo la competitividad tecnológica de las Fuerzas Armadas.

### Tecnologías de doble uso clave

Las nuevas tecnologías innovadoras y relevantes provienen cada vez más del sector civil, y pueden aportar nuevas capacidades de manera ágil al sector de defensa y seguridad:

- Inteligencia artificial y machine learning: para el análisis de grandes volúmenes de información en tiempo real, la toma de decisiones y la mejora de la eficiencia operativa.
- *Cloud computing* de alta seguridad: incluidas las nubes soberanas, infraestructuras de computación en la nube que garantizan el control nacional sobre los datos críticos y reducen la dependencia de proveedores extranjeros.
- Ciberseguridad avanzada: con implementación de modelos Zero Trust y arquitecturas de defensa adaptativa.
- 5G/6G: para comunicaciones tácticas de alta velocidad y baja latencia.
- Drones y sistemas autónomos: tanto aéreos (UAV) como terrestres (UGV), ya experimentados en brigadas del Ejército de Tierra.
- Tecnología cuántica: con aplicaciones en cifrado, posicionamiento y sincronización.
- Robótica y gemelos digitales: para simulación de escenarios, mantenimiento predictivo y optimización de operaciones.

## Cómo contribuyen las consultoras tecnológicas

Las consultoras actúan en dos dimensiones complementarias:

### 1. Acelerando la capacidad táctica:

- Adaptando tecnología civil a requisitos militares específicos.
- Implantando metodologías Agile para reducir tiempos de desarrollo y despliegue.
- Implementando modelos de seguridad Zero Trust para proteger infraestructuras críticas.
- Desarrollando soluciones personalizadas que respondan a necesidades operativas concretas.

### 2. Garantizando la autonomía estratégica:

- Fomentando el ecosistema local de empresas tecnológicas, universidades y centros de investigación.
- Creando nubes soberanas y arquitecturas de datos nacionales.
- Diseñando arquitecturas abiertas.
- Desarrollando capacidades nacionales de I+D+i que reduzcan la dependencia de terceros países.

Las consultoras tecnológicas aportan conocimiento experto y experiencia previa acumulada en todas las industrias y sectores económicos, lo que facilita la agilidad en el despliegue de estas nuevas capacidades. Este conocimiento transversal permite transferir soluciones exitosas del ámbito civil al militar con rapidez, eficiencia y control soberano.

## c) Desarrollo de capacidades, talento y conocimiento

El desarrollo de capacidades tecnológicas en defensa no puede disociarse del desarrollo del talento humano que las impulsa. En defensa, la tecnología evoluciona a gran velocidad y exige algo más que sistemas avanzados: necesita personas preparadas, ecosistemas colaborativos y una visión estratégica que impulse la innovación continua. El talento, el conocimiento y la capacitación son la base que garantiza la soberanía tecnológica y la competitividad de España en el ámbito de la defensa.

España cuenta con un sistema educativo que genera profesionales de alta cualificación: matemáticos, ingenieros y expertos en tecnología que son perfiles muy demandados en Europa. Sin embargo, el reto del presente es retener el talento en España en el ámbito de la defensa, ofrecer oportunidades de carrera profesional atractivas y permitir que los profesionales desarrollen su potencial.

### Diversidad como ventaja competitiva

La transformación del sector de la defensa, impulsada por la innovación y las tensiones de seguridad a nivel global, abre la oportunidad de atraer talento muy diverso. La inclusión de nuevas perspectivas y formas de pensamiento es fundamental, y en este sentido, dar mayor valor y visibilidad al trabajo de las mujeres en ingeniería, innovación, liderazgo y ciberseguridad es una prioridad. Más allá de la necesaria igualdad, es un elemento de competitividad.

## **Nuevos planes de estudio y especialización tecnológica**

Los nuevos planes de estudio deben adaptarse a las corrientes tecnológicas emergentes y a las necesidades reales del sector defensa. Las áreas prioritarias de especialización incluyen:

- Inteligencia artificial y ciberseguridad: para anticipar amenazas, proteger infraestructuras críticas y desarrollar sistemas autónomos seguros.
- Analítica de datos: aplicada a la interconexión de sensores, sistemas logísticos y conciencia situacional.
- Control de sistemas autónomos: incluyendo radares, inteligencia operativa, mando y control.
- Robótica y gemelos digitales: para labores de vigilancia, simulación de escenarios y mejora de la operatividad en terreno.

Estas disciplinas representan los perfiles profesionales que las Fuerzas Armadas y la industria de defensa necesitarán en los próximos años. La redefinición hacia competencias digitales y tecnológicas es una prioridad estratégica para garantizar la operatividad en el entorno de defensa moderno.

## **Colaboración público-privada y empleo de calidad**

El desarrollo de talento solo puede consolidarse mediante la colaboración público-privada entre empresa, universidad y administración. Es esencial establecer vínculos sólidos entre la industria y las instituciones educativas para generar empleo de calidad y de larga duración, formar talento especializado y transferir conocimiento de forma eficaz. Las consultoras tecnológicas actúan como catalizador en la formación de talento y la transferencia de conocimiento.

Así, se debe profundizar en la estrategia de descentralización de la industria de defensa impulsada por el Gobierno, que busca crear polos tecnológicos fuera de las grandes ciudades, revitalizando la economía local, reteniendo talento nacional y mitigando la fuga de cerebros hacia Europa.

Este desarrollo de capacidades, talento y conocimiento no es solo una cuestión tecnológica, es una apuesta por las personas y por el futuro de España.

# III. Tecnologías de doble uso y casos prácticos

## a) IA y Machine Learning como motor dual

La inteligencia artificial se ha consolidado como una de las tecnologías más disruptivas tanto en el ámbito civil como en el militar. Como tecnología estratégica de doble uso, sus aplicaciones abarcan desde la optimización de procesos logísticos en el sector civil hasta el apoyo al mando y control en operaciones militares.

La IA potencia tanto vehículos militares como civiles, incluyendo aviones, drones y buques, permitiendo operaciones autónomas, detección temprana de amenazas y toma de decisiones en tiempo real. Las aplicaciones específicas en el ámbito de defensa incluyen:

- Mando y control: mejorando la toma de decisiones en tiempo real mediante análisis predictivo y simulación de escenarios.
- Reconocimiento de imagen y análisis multisensor.
- Mantenimiento predictivo: anticipando fallos en equipos, permitiendo optimizar la rotación y disponibilidad operativa.
- Gestión documental inteligente.
- Gestión del dato.
- Ciberdefensa.
- Operación autónoma de vehículos y sistemas de armas.

### Uso responsable y regulación

El papel de las consultoras en este ámbito es crítico. Para comenzar, contribuyen a identificar casos de uso reales y evaluar si la implementación de IA es realmente necesaria en cada caso o si, por ejemplo, con un desarrollo de código convencional sería suficiente. Esta capacidad de discernimiento técnico es fundamental para evitar la aplicación indiscriminada de tecnología y garantizar soluciones eficientes y sostenibles.

Otro aspecto crítico es la legislación. Las consultoras deben impulsar, junto con el usuario final, una base legislativa sólida que regule el uso de la IA en defensa y seguridad. Es una herramienta cuyo uso debe ser ético y responsable.

### Reducción de la carga de trabajo y mejora de la eficiencia

Uno de los mayores beneficios de la IA en defensa es la reducción de tareas repetitivas y la disminución de la carga de trabajo en muchos departamentos de las Fuerzas Armadas. La carga administrativa asociada a la gestión documental, los procesos de mantenimiento y los informes es elevada. Con la IA aplicada a la gestión documental se puede reducir entre un 60% y un 70% la carga de trabajo operativa, liberando tiempo para que el personal se dedique a tareas de mayor valor estratégico.

### Gestión del conocimiento y preservación de la experiencia

Otro aspecto crítico es la gestión del conocimiento. En las Fuerzas Armadas existe una alta rotación de personal, y cuando una persona alcanza la edad de retiro, puede perderse todo su conocimiento acumulado durante décadas de servicio. Las consultoras han desarrollado chatbots especializados basados en IA generativa, como las originalmente diseñados para banca o seguros, adaptados a los perfiles técnicos de las Fuerzas Armadas para transmitir ese conocimiento y evitar su pérdida.

## Calidad del dato como fundamento de la IA

Finalmente, las consultoras ayudan en la calidad y gestión del dato, ya que la IA actúa en base a la información con la que ha sido entrenada. Un dato de calidad es imprescindible para garantizar resultados fiables. Sin datos precisos, actualizados y bien estructurados, cualquier sistema de IA generará resultados incorrectos o sesgados que pueden comprometer la seguridad operativa.

## b) Analítica avanzada y gemelos digitales

El gemelo digital es una representación virtual de un objeto, proceso o sistema del mundo real que se alimenta con datos reales y en tiempo real. Esta tecnología permite monitorizar, simular, optimizar y predecir el comportamiento de sistemas complejos sin necesidad de intervenir físicamente en ellos. Su aplicación en defensa es especialmente valiosa, ya que reduce costos, aumenta la seguridad y mejora la toma de decisiones.

En el ámbito civil, los gemelos digitales se están aplicando con éxito en múltiples sectores:

- Monitorización del estado y rendimiento de activos: por ejemplo, en validadoras de transporte público para anticipar fallos antes de que ocurran.
- Mantenimientos predictivos: en sanidad, para anticipar fallos en equipamiento médico crítico, evitando interrupciones en la atención sanitaria.
- Optimización de procesos: en transporte, para optimización de rutas y reducción de tiempos de entrega.
- Toma de decisiones: en aplicaciones de seguridad, donde aportan gran valor añadido para mejorar la respuesta ante incidentes.
- Diseño y prototipado: para validar diseños antes de llevarlos a la etapa de fabricación, reduciendo costos y riesgos.

En el ámbito militar, el gemelo digital tiene aplicaciones estratégicas de alto impacto:

- Monitorización del rendimiento y estado de sistemas de mando y control: permitiendo detectar anomalías en tiempo real y anticipar fallos críticos antes de que comprometan la operativa.
- Optimización de procesos logísticos: por ejemplo, determinando la ubicación óptima de repuestos en los distintos almacenes del Ejército para minimizar tiempos de respuesta y costos de transporte.
- Toma de decisiones en entornos de guerra electrónica: colaborando con el Ejército de Tierra en entornos de comunicaciones para decidir en qué banda operar o en cuál evitar interferencias enemigas.
- Simulación de escenarios operativos: para entrenar personal en entornos virtuales realistas y validar estrategias sin poner en riesgo recursos reales o vidas humanas.

Un componente fundamental del gemelo digital es la simulación, que une el mundo físico y virtual para optimizar procesos y decisiones antes de su implementación real. Esta capacidad es especialmente valiosa en defensa, donde los errores pueden tener consecuencias fatales.

### Analítica avanzada: inteligencia en tiempo real

Además del gemelo digital, las consultoras están desarrollando soluciones de analítica avanzada que combinan IA y aprendizaje automático para realizar predicciones, automatización y mejora de la conciencia situacional. Ejemplos claros de la analítica avanzada son proyectos como el Sistema de Información de Superficie (SIS) del Ejército de Tierra, o el SICONDEF, Sistema de Inteligencia Conjunto de la Defensa.

## **Ciberseguridad y gestión de identidades**

La gestión de identidades, incluida la gestión de identidades no humanas (dispositivos, sistemas autónomos, sensores, drones) es crítica para reducir riesgos de seguridad en infraestructuras complejas y distribuidas.

Un caso de éxito es la gestión de identidad avanzada al Ministerio de Defensa, implementando soluciones de PKI (Public Key Infrastructure) para garantizar la autenticación segura de usuarios, dispositivos y sistemas; el cifrado de comunicaciones extremo a extremo; la trazabilidad completa en el acceso a sistemas clasificado; y el control de acceso granular basado en roles y contexto.

El gemelo digital, combinado con analítica avanzada y ciberseguridad, representa una de las tecnologías duales con mayor potencial de transformación en el sector defensa, permitiendo optimizar recursos, anticipar amenazas y mejorar la resiliencia operativa de forma integral.

## **c) Telecomunicaciones 5G/IoT y conectividad multidisciplinar**

Las telecomunicaciones avanzadas son el pilar que sostiene el ecosistema tecnológico de defensa y seguridad. Sin comunicaciones eficaces que enlacen toda la información y la hagan llegar a cualquier punto de despliegue, la operativa se complica significativamente o resulta inviable.

Las consultoras tecnológicas cuentan con capacidades y equipamiento para establecer burbujas tácticas en zonas de operaciones o en áreas donde no existe cobertura comercial (4G, 5G). Estas burbujas permiten dotar a los operativos, tanto civiles como militares, de la capacidad de estar interconectados y compartir información estratégica en tiempo real con las unidades superiores y los mandos responsables de la toma de decisiones.

Estos sistemas de comunicación táctica en tiempo real permiten:

- Empleo de redes públicas y privadas.
- Comunicación segura de extremo a extremo.
- Respuesta rápida en zona de operaciones.

Un caso de éxito es la burbuja táctica 5G desarrollada e implementada para la Unidad Militar de Emergencias (UME), que permite desplegar comunicaciones privadas y seguras en zonas de emergencia donde las redes convencionales han colapsado o están saturadas por el uso civil. Esta capacidad es directamente trasladable a zonas de operaciones militares, donde es fundamental disponer de comunicaciones propias, seguras y resilientes.

Las consultoras tienen amplia experiencia trabajando con la Guardia Civil y el Ministerio de Defensa en la elaboración de sistemas de mando y control que integran información procedente tanto del operativo en campo como de los sensores desplegados. Estos sistemas centralizan y presentan la información de forma clara, visual y procesable, facilitando la toma de decisiones operativas en tiempo real mediante cuadros de mando, mapas interactivos y alertas automatizadas.

La capacidad de comunicarse es una pieza fundamental del ecosistema de defensa. Sin ella, no es posible obtener información de todos los sensores y operativos en zona, ni dentro de un buque, ni en un teatro de operaciones complejo. La conectividad multidisciplinar, que integra redes terrestres, aéreas, marítimas y satelitales, es esencial para garantizar la interoperabilidad entre fuerzas y el éxito de las misiones en entornos operativos cada vez más exigentes.

## IV. Impacto en el sector y en el conjunto de la economía

El impacto del nuevo ciclo inversor en seguridad, defensa y tecnologías duales deberá medirse en los próximos años a partir de un enfoque capaz de integrar sus efectos en diferentes sectores, incluyendo también su función tractora sobre el talento o el desarrollo de I+D+i. En el ámbito de la consultoría tecnológica, las empresas que integran la AEC prevén un crecimiento cercano al 30% en sus ingresos procedentes del sector de la defensa y la ciberseguridad en 2025. En concreto, cuando se publica este informe, se espera un aumento del 28,9% para 2025.

De acuerdo con estas estimaciones de la AEC, que representa en torno al 70% del sector, en 2024 los ingresos de las consultoras en defensa y ciberseguridad alcanzaron los 1.125 millones de euros, una cifra que se elevará hasta los 1.450 millones en 2025. Este crecimiento de la consultoría trasciende al sector gracias al impacto positivo de estas compañías tecnológicas en el conjunto de la economía española, la generación de empleo de calidad, el impulso a la innovación y a la formación.

La defensa no es solo el rearme, sino la incorporación de nueva tecnología, de inteligencia para tomar las mejores decisiones y la capacidad de adaptación y gestión del cambio. El ecosistema de personas de la consultoría ayuda a poder afrontar esos cambios y al reskilling de responsabilidades y perfiles que necesitan España y Europa en los próximos años.

### Un modelo más ágil para la contratación en el sector público

En el nuevo paradigma, la velocidad en la que evoluciona la tecnología es mucho más rápida que la capacidad de absorción que tiene actualmente la administración. Por tanto, debe repensarse el modelo, con la colaboración de la consultoría, para que sea mucho más ágil y permita que las tecnologías disponibles lleguen a las Fuerzas Armadas en el momento en que se necesitan.

La Ley de Contratos del Sector Público es más restrictiva que lo que exige la Unión Europea, y la propia Comisión Europea está analizando cómo modificar la normativa de contratación para hacer mucho más ágiles este tipo de procesos.

En España no se han generalizado todavía los contratos de mantenimiento evolutivo, que pueden ser clave en el futuro. Se trata de acompañar a las Fuerzas Armadas para implementar mejoras en procesos, procedimientos y software de manera continua, con un trabajo conjunto entre los operadores y aquellos que desarrollan la innovación.

Además, es conveniente avanzar hacia un mercado único europeo de defensa para alcanzar el volumen necesario para abordar los desafíos del futuro cercano, superando la competencia entre los llamados campeones nacionales.

### Gap entre universidad e industria

Como es sabido, España genera una gran cantidad de conocimiento en las universidades y posee una industria potente, pero se mantiene un gap crítico entre ambos segmentos. Faltan centros especializados en la transformación del conocimiento que generan las universidades en conocimiento práctico que puedan utilizar las empresas. Además, es necesario un ecosistema donde startups y pequeñas empresas generen innovación disruptiva con agilidad.

Es imprescindible introducir la innovación y el conocimiento científico en la cadena de producción industrial, y para ello las consultoras tecnológicas aportan un conocimiento de primera mano de las necesidades de las cadenas de valor, las soluciones que aporta el mercado, las integraciones que funcionan y las que no, y los retos de la puesta en marcha de la operación.

Para que la inversión en defensa constituya realmente una palanca productiva, rentable y transformadora en Europa, debe destinarse a proyectos que, más allá del consumo, se centren en tecnología, innovación y reconversión de la industria.

## V. Consideraciones finales

Las reflexiones producto del foro organizado por la AEC ponen de manifiesto el papel estratégico que desempeña el sector de la consultoría tecnológica en el nuevo ciclo inversor en defensa que vive España y Europa. Las conclusiones reflejan un sector comprometido con la seguridad, la innovación tecnológica y la colaboración institucional en un momento histórico de profunda transformación.

La guerra en pleno territorio europeo ha puesto en cuestión muchos aspectos de la seguridad, rompiendo el principio básico de respeto a las fronteras europeas con preocupantes consecuencias en el ámbito militar. La situación dista mucho de ser transitoria, aun cuando finalice el conflicto entre Ucrania y Rusia. Los países europeos seguirán fortaleciendo y modernizando sus capacidades de defensa. A nivel mundial tiene lugar una escalada generalizada de inversiones, con gran protagonismo de nuevas tecnologías duales, emergentes y disruptivas.

Conceptos como disuasión, fuerza o reservas estratégicas han regresado al discurso geopolítico. Junto a ellos, han reaparecido nociones hoy imprescindibles como las capacidades industriales y tecnológicas. La logística estratégica y de base industrial, la soberanía tecnológica y la resiliencia son más críticas que nunca y, en este contexto, las tecnologías duales son clave.

Este escenario abre oportunidades extraordinarias para las empresas de consultoría tecnológica, que prevén un crecimiento cercano al 30% en sus ingresos procedentes de defensa y ciberseguridad en 2025, pasando de 1.125 millones de euros en 2024 a 1.450 millones este año.

Las tecnologías duales han emergido como el principal motor de innovación en defensa. Inteligencia artificial, ciberseguridad, cloud computing, gemelo digital, conectividad 5G, robótica, satélites, analítica avanzada o el desarrollo de la computación cuántica están transformando las capacidades operativas de las Fuerzas Armadas y generando un ecosistema de innovación que impacta al conjunto de la economía española. La defensa va mucho más allá del armamento y de las plataformas convencionales: las nuevas tecnologías, el análisis de grandes volúmenes de datos y la capacidad de traducir en estrategia la información y el conocimiento son imprescindibles.

Las consultoras tecnológicas han demostrado su capacidad para acompañar a las Administraciones Públicas y las Fuerzas Armadas en procesos de transformación complejos, cubriendo el ciclo de vida completo de las soluciones tecnológicas. Su experiencia en múltiples sectores económicos e industrias les permite transferir conocimiento, metodologías y soluciones con rapidez y eficiencia.

Sin embargo, existen desafíos estructurales que deben abordarse con urgencia. Es necesario repensar el modelo de relaciones entre empresa, universidad y administración. Las tecnologías disponibles deben ponerse a disposición de las Fuerzas Armadas de manera más ágil, reformando la Ley de Contratos del Sector Público. Y debe extenderse el modelo de mantenimiento evolutivo, implementando mejoras de manera continua, en lugar de apostar por programas que quedan obsoletos cada día de forma más temprana.

Se mantiene un gap crítico entre la universidad y la industria. Es indispensable construir un ecosistema que integre a universidades, pymes innovadoras, startups, consultoras tecnológicas e industria tradicional de defensa, con la Administración como agente que genere las condiciones óptimas para su desarrollo. La colaboración público-privada es esencial para el éxito de la transformación digital de la defensa y la seguridad.

Una mayor inversión en defensa y ciberseguridad debe proteger a España de nuevas amenazas, y también debe impulsar el crecimiento económico y el fortalecimiento de la industria. Es una oportunidad para estimular la innovación, generar empleo cualificado, impulsar la productividad y posicionar a España como referencia en el ámbito europeo de defensa y tecnología.

Ante este punto de inflexión histórico, el sector de la consultoría tecnológica ha demostrado estar preparado para liderar esta transformación, aportando innovación, talento y compromiso con la seguridad, la competitividad y la soberanía tecnológica. España y Europa pueden construir un sistema de defensa moderno, tecnológicamente avanzado y autónomo, que reduzca la brecha con otras potencias como Estados Unidos y China. Este desafío requiere un esfuerzo conjunto y acierto en la toma de decisiones estratégicas, para lo cual la AEC continúa promoviendo la reflexión, la generación de conocimiento y fomentando un debate informado en la sociedad.

# Reconocimientos

La Asociación Española de Empresas de Consultoría (AEC) organizó el 19 de noviembre de 2025 en Madrid un foro de reflexión sobre el nuevo escenario en defensa, seguridad y tecnologías duales.

La contribución de todos los ponentes de empresas asociadas a la AEC ha sido imprescindible para la elaboración de esta publicación:

- José María Beneyto, presidente de la AEC.
- Pablo Pérez Román, director de Defensa y Seguridad para el sector público en Accenture en España.
- Natalia García, directora de Sector Público en ALTIA.
- Óscar Fraguas, responsable de Operaciones de Defensa y Seguridad en Atos.
- Salvador Magán, responsable del sector Aeroespacial y Defensa en Capgemini España.
- Daniel Gallardo, director de Operaciones de Defensa en Inetum.
- Sindhia Olmo, jefa de Seguridad del Servicio de Protección de Izertis.
- Juan Gómez Gallego, socio responsable de Seguridad y Defensa en NTT DATA.
- Alfredo Sanz, director de Riesgos y Seguridad Global en Grupo Oesía.
- Pablo Carrera, asesor de Defensa y Aeroespacial en Sopra Steria Next.

Además, el encuentro contó con una ponencia del **Teniente General Raimundo Rodríguez Roca, Jefe del Mando de Apoyo Logístico del Ejército de Tierra**, quien ha aportado su visión sobre los retos operativos y tecnológicos de las Fuerzas Armadas en el contexto actual.



ASOCIACIÓN ESPAÑOLA DE  
EMPRESAS DE CONSULTORÍA

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

C/Monte Esquinza, 34 - 2ºB  
28010 Madrid

Tlf.: +34 91 308 01 61

[aec@aecconsultoras.com](mailto:aec@aecconsultoras.com)

