CyberHubs

Análisis de las necesidades en ciberseguridad España 2026

Co-funded by the European Union

About CyberHubs

The European Network of Cybersecurity Skills Hubs (CyberHubs) is a 3-year project aiming to enhance the cybersecurity skills ecosystem in Europe. It will establish a network of seven Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce.

Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon and the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem.

Project consortium

The CyberHubs consortium brings together 21 full partners spanning 11 European Member States and 3 associated partners.

Full partners

DIGITALEUROPE | ADECCO FORMAZIONE SRL | AGORIA | AMETIC | Athens University of Economics and Business | Breyer Publico SL | Cyber Ireland | EIT Digital | GZS/CCIS | HOWEST | INFOBALT | ITL Estonia | IVSZ | Kaunas University of Technology | NUMEUM | SEPE | Solvay Brussels School of Economics and Management | Tallinn University of Technology | Universidad Internacional de La Rioja (UNIR) | Ludovika University of Public Service (NKE) | UNIVERZA V MARIBORU

Associated partners

Association of Applied Research in IT (AAVIT) | Digital Technology Skills (DTSL) | IT Ukraine

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Co-funded by the European Union

Copyright © 2024 by CyberHubs

All rights reserved.

Historial de versiones			
Version	**Fecha**	**Modificado por**	**Versión**
0.1	17/08/2026	Alejandro Velasquez (Universidad Internacional de La Rioja)	Draft version
0.2	18/08/2026	Ignacio Vilela (Universidad Internacional de La Rioja)	Revision and comments
0.3	24/08/2026	Shila Ganguly (Universidad Internacional de La Rioja)	Revision and comments
0.4	26/08/2026	Alejandro Velasquez (Universidad Internacional de La Rioja)	Updated version integrating the above comments
0.5	27/08/2026	Shila Ganguly (Universidad Internacional de La Rioja)	Final version

Tabla de contenidos

Resumen ejecutivo 6
1. Introducción 8
1.1. Ciberseguridad en España 8
1.2. Tendencias globales y regionales en ciberseguridad 9
1.3. Visión 9
2. Situación actual y objetivos estratégicos 10
2.1. Actores clave en el ámbito de la ciberseguridad 10
2.2. Panorama Educativo 10
2.3. Evaluación de las necesidades en ciberseguridad 12
Evidencia actual de demanda en España: 13
3. Análisis de las necesidades. 16
3.1. Análisis por perfiles 16
Prospectiva de necesidades 17
3.2. Análisis prospectivo (amenazas y riesgos) 19
Amenazas principales 20
Matriz de impacto cruzado enfocada en los riesgos cibernéticos para el sector privado en España 2026-2028. 22
4. Análisis prospectivo de Amenazas vs Necesidades 25
4.1. Relación entre amenazas y perfiles más requeridos 25
6. Conclusiones 28
7. Referencias 29

Lista de tablas

Tabla 1. Instituciones y programas en España que combinan seguridad + IA 11
Tabla 2. Programas formativos en España por prioridades Ciberseguridad+IA 11
Tabla 3. Número de ofertas de empleo en ciberseguridad 13
Tabla 4. Número de ofertas de empleo combinando ciberseguridad + IA 14
Tabla 5. Matriz de impacto de amenazas cibernéticas 23
Tabla 6. Clasificación estratégica de la matriz de impacto cruzado 23

Lista de abreviaturas

Term	Definition
Ciber Cog	La ciberseguridad cognitiva es la protección de los procesos mentales, perceptivos y decisionales de las personas frente a amenazas que usan medios digitales para manipular creencias, emociones, comportamientos o decisiones.
SOC	Centro de Operaciones de Seguridad (*Security Operations Center*)
MLS	Machine Learning Security
SIEM	*Security Information and Event Management* o Gestión de Información y Eventos de Seguridad
XSIAM	Extended Security Intelligence and Automation Management
MITRE ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
MSP	*Managed Service Provider* o Proveedor de Servicios Gestionados
SaaS	*Software as a Service* o Software como Servicio
DLP	*Data Loss Prevention* o Prevención de Pérdida de Datos
IAM/PAM	Identity and Access Management/ Privileged Access Management

Resumen ejecutivo

Introducción

Este informe actualiza el análisis elaborado por CyberHubs España en 2024 sobre las necesidades y brechas de la ciberseguridad nacional, con especial atención al mercado laboral, los perfiles profesionales más relevantes y la oferta formativa de las instituciones educativas.

Para este estudio se actualizaron los datos y se integraron los resultados de 2024 con el fin de proyectar las necesidades de los próximos dos años. El análisis también incorpora las amenazas y los riesgos actuales y emergentes, lo que permite identificar los perfiles que requieren medidas prioritarias y orientar el fortalecimiento de los programas educativos, la conciencia situacional y la resiliencia digital de los sectores productivos españoles.

Objetivo

Identificar, analizar y documentar las necesidades actuales y futuras de educación, formación y talento humano en ciberseguridad en España durante los próximos dos años, partiendo del análisis realizado en 2024 y actualizando los datos en base a la situación actual. El análisis considera la evolución de las amenazas y los riesgos actuales y emergentes, las brechas entre la oferta formativa y las competencias demandadas por el mercado laboral, y los perfiles profesionales que requieren una atención prioritaria. Asimismo, busca orientar el diseño y la actualización de programas educativos, iniciativas de capacitación y acciones de colaboración entre el sector público, el sector privado y la academia, con el fin de fortalecer las capacidades nacionales, reducir la escasez de talento especializado y mejorar la resiliencia digital del país.

Enfoque

Para desarrollar este estudio, se volvió a realizar una revisión de la literatura basada en informes y análisis sobre el estado actual de la ciberseguridad en España. Esta revisión permitió examinar las principales amenazas y los riesgos que afectan a los distintos sectores. A partir de la información recopilada, se elaboraron matrices de análisis para identificar y evidenciar, tanto cuantitativa como cualitativamente, las necesidades actuales. El informe de 2024 se utilizó como referencia para comparar los resultados y valorar su evolución.

Resultados

El análisis identifica tres resultados principales:

1. **Mayor demanda de perfiles híbridos**. Se observa un aumento de la necesidad de profesionales con competencias en ciberseguridad e Inteligencia Artificial, complementadas con capacidades de estrategia, liderazgo y respuesta frente a amenazas híbridas.
2. **Actualización de la oferta educativa.** Es necesario revisar y orientar los programas de formación en ciberseguridad para integrar de manera explícita el uso de la Inteligencia Artificial y fortalecer las competencias relacionadas con la Ciber Cog (ciberseguridad cognitiva).
3. **Coordinación y cultura de ciberseguridad**. Resulta fundamental mantener una comunicación continua, reforzar el apoyo entre los distintos sectores y consolidar estrategias de conciencia situacional y cultura de ciberseguridad en los ámbitos nacional y regional. Este constituye uno de los principales aportes del CyberHub español.

Conclusiones

El análisis permite extraer tres conclusiones principales sobre la evolución de la ciberseguridad:

1. **Impacto de la inteligencia artificial.** La IA está transformando el presente y el futuro de la ciberseguridad: amplía y potencia las amenazas, aumenta su capacidad para afectar la continuidad del negocio y eleva la exposición de entidades e instituciones.

2. **Evolución de los perfiles profesionales.** Los especialistas en ciberseguridad deben prepararse no solo para proteger sistemas y datos, sino también para responder a amenazas híbridas cada vez más avanzadas que utilizan el ciberespacio como vector de ataque.

3. **Ampliación de la educación y la capacitación.** La formación de los profesionales requiere una visión más integral del ciberespacio, cuyo alcance es cada vez más transversal a la vida cotidiana y a la sociedad. Fortalecer este conocimiento es esencial para avanzar hacia una sociedad digital segura, preparada y resiliente.

1. Introducción

El presente informe actualiza el análisis de necesidades elaborado en 2024 al inicio del proyecto CyberHubs: Network of European Cybersecurity Skills Hubs. Mientras que el informe anterior se centró en la creación e implantación del CyberHub español y en el estado de la ciberseguridad en ese momento, esta edición examina la situación actual y ofrece una perspectiva para los próximos dos años. El análisis aborda las necesidades educativas y los programas de formación, la demanda de profesionales según los perfiles de ENISA y las amenazas y riesgos actuales y emergentes. Su objetivo es mostrar cómo se relacionan estos factores y facilitar, junto con los sectores que integran el CyberHub español, la definición de medidas y acciones para reforzar la ciberseguridad en España.

Para este informe se han tenido en cuenta y se han consultado los informes y estudios de diferentes entidades e instituciones, con el propósito de obtener un análisis lo más real posible del estado actual, referenciados en este documento.

Tanto el proyecto como el desarrollo de cada informe desarrollado se ha basado en el ENISA ECSF – European Cybersecurity Skills Framework. Aunque el informe está fechado en 2022, sigue constituyendo el marco europeo vigente para clasificar roles.

Así mismo, el informe se basa en un estudio de fuentes utilizadas como referencias, listadas a continuación:

- Institucionales: ENISA, INCIBE, CCN-CERT/CNI, Europol, NIS Cooperation Group.
- Consultoras: Deloitte, PwC, Accenture, KPMG, EY, WEF.
- Empresas de ciberseguridad: Microsoft, Google/Mandiant, CrowdStrike, Palo Alto Unit 42, Fortinet, Check Point, IBM X-Force, Verizon DBIR.
- Academia/think tanks: universidades españolas/europeas, IEEE, Elcano, CSIS, Oxford Cyber Policy, NATO CCDCOE.

1.1. Ciberseguridad en España

Actualmente, España posee un ecosistema de ciberseguridad relativamente maduro, pero presenta una serie de necesidades debido a una presión creciente por la constante evolución de las amenazas existentes. Posee una buena estructura institucional, de la que forman parte INCIBE, INCIBE-CERT, CCN-CERT/CNI, DSN o el Mando Conjunto del Ciberespacio, con una estrategia nacional consolidada y un sector privado activo. La principal problemática radica en la velocidad con la que crecen las amenazas frente a la disponibilidad de talento, más específicamente en profesionales especializados en las áreas más requeridas. Asimismo, ha mejorado en coordinación gracias al trabajo de los diferentes sectores, pero aún requiere un impulso en esta área para consolidarse. Por último, pero no menos importante, es necesaria una adopción práctica en las pequeñas y medianas empresas (PYMEs) para disponer de un nivel de ciberseguridad que permita una defensa más profunda.

España sigue siendo objetivo de "ransomware", fraude digital, phishing, robo de credenciales, ataques a administraciones públicas, PYMEs e infraestructuras críticas, pero son precisamente las PYMEs el punto débil: muchas empresas pequeñas dependen de servicios digitales, pero poseen una baja madurez en gestión de riesgos, backups, respuesta a incidentes y, sobre todo, en cumplimiento.

No obstante, España continúa adaptándose a las normativas más importantes tales como la Directiva NIS2, a través de la Ley de Coordinación y Gobernanza de la Ciberseguridad que se encuentra en proyecto. Se pretende con ello establecer más y mejores obligaciones, con el propósito de cerrar las brechas legales y de cumplimiento que les permita a las entidades esenciales/importantes el reporte de incidentes, la gestión de riesgos y una mayor supervisión.

Dentro de sus principales debilidades se encuentra la falta personal especializado, especialmente en arquitectura de ciberseguridad, implementación técnica o respuesta a incidentes.

Cabe resaltar que la comunicación y coordinación entre sectores se ha fortalecido, gracias al buen trabajo de INCIBE. El Cyberhub español ha contribuido en este punto, ya que se ha trabajado con el objetivo de establecer una comunicación más directa entre sectores, así como en el aumento de la conciencia situacional del ciberespacio y la ciberseguridad.

1.2. Tendencias globales y regionales en ciberseguridad

La ciberseguridad global está marcada por el aumento exponencial del "ransomware", ataques a la cadena de suministro, uso ofensivo de Inteligencia Artificial (IA), amenazas contra infraestructuras críticas, ataques de guerra cognitiva mediante el uso del ciberespacio y una gran escasez de talento especializado. En Europa, la respuesta se concentra en fortalecer la resiliencia digital mediante regulación —NIS2, DORA, Cyber Resilience Act—, cooperación público-privada y desarrollo de capacidades. Sin embargo, persisten brechas importantes entre la formación disponible y las necesidades reales del mercado.

En este contexto, el proyecto CyberHubs cumple un papel clave. Consiste en una red europea de centros de competencias en ciberseguridad presente en siete países (Estonia, letonia, Eslovenia, Grecia, Bélgica, España y Hungría) que busca cerrar la brecha de habilidades profesionales en el área. Su trabajo se enfoca en conectar academia, industria y gobierno, desarrollar estrategias nacionales de talento, promover formación práctica y preparar profesionales frente a amenazas emergentes como IA, "ransomware" e incidentes en infraestructuras críticas.

1.3. Visión

El objetivo del CyberHub español se centra en fortalecer de forma continua la cooperación, la comunicación y la conciencia situacional en materia de ciberseguridad nacional mediante la resiliencia, la educación y el desarrollo del talento. Para ello, impulsar programas de formación más sólidos, acciones de prevención y cultura digital, y una colaboración intersectorial que favorezca la mejora permanente del ecosistema de seguridad digital y la consolidación de una sociedad digital segura.

2. Situación actual y objetivos estratégicos

En la última etapa del proyecto CyberHubs, el CyberHub español actualiza el informe de necesidades como parte de su estrategia para reforzar la comunicación, la colaboración y la conciencia situacional en el ciberespacio. Esta actualización, reflejada en el presente informe, analiza la evolución del mercado nacional y la brecha de profesionales en ciberseguridad, además de anticipar las necesidades, amenazas y riesgos actuales y potenciales de España. Su objetivo es orientar acciones oportunas que reduzcan esta brecha y fortalezcan las áreas más críticas de la ciberseguridad nacional.

2.1. Actores clave en el ámbito de la ciberseguridad

En España, la ciberseguridad constituye un esfuerzo en el que participan múltiples partes interesadas, entre las que se incluyen diversas entidades públicas, privadas y académicas. Cada una de ellas tiene funciones y responsabilidades específicas para garantizar la protección de las infraestructuras nacionales, las empresas y los ciudadanos frente a las amenazas cibernéticas. A continuación, se presenta una lista de los principales actores del ámbito de la ciberseguridad en España.

1. Instituto Nacional de Ciberseguridad (INCIBE[IV6.1]): Entidad de referencia en España encargada de ejecutar y promover los pilares clave de la Estrategia Nacional de Ciberseguridad (ENCS)
2. Ministerio de Defensa
3. Agencia Española de Protección de Datos (AEPD)
4. Empresas españolas de ciberseguridad y sector privado
5. Universidades e instituciones de investigación
6. Cyberhub España

2.2. Panorama Educativo

El sistema educativo español, a través de instituciones públicas y privadas, ofrece una amplia gama de programas de ciberseguridad, desde grados universitarios hasta másteres y doctorados, tanto oficiales como no oficiales. Asimismo, existen diversas instituciones que imparten cursos y formación especializada en ciberseguridad, pudiendo cursarse en diferentes modalidades: online, presencial o mixta.

España cuenta con instituciones y entidades que certifican en ciberseguridad, como "Ethical Hacking", "Chief Information Security Officer" (CISO) o"Incident Responder", entre otras temáticas. Esto permite a los profesionales formados en ciberseguridad obtener certificaciones en distintas áreas, según su especialidad.

La evolución tecnológica ha transformado el ciberespacio y, en particular, la ciberseguridad. Tecnologías como la Inteligencia Artificial ofrecen nuevas ventajas a los atacantes, pero también se utilizan cada vez más para fortalecer y optimizar las distintas áreas de la ciberseguridad.

Pese a que actualmente en España algunos programas de ciberseguridad están empezando a incluir conocimientos relacionados con IA (ver tabla 1), no existen programas oficiales “Ciberseguridad + IA”. Por ello, es importante identificar aquellas instituciones y programas que pueden tener oferta formal en ciberseguridad y donde incluyan temáticas en IA, a nivel grado, máster o doctorado.

A continuación, quedan listadas aquellas instituciones y programas que poseen temáticas que combinan o se relacionan ciberseguridad + IA:

Tabla 1. Instituciones y programas en España que combinan seguridad + IA

Institución	Ciberseguridad	Ciber + IA / Data / ML
Universidad Carlos III de Madrid – UC3M	Máster Univ. en Ciberseguridad	Máster Univ. en Inteligencia Artificial Aplicada
Universidad Politécnica de Madrid – UPM	Programas TIC/seguridad/ciberseguridad	IA, ciencia de datos, sistemas inteligentes
Universitat Politècnica de Catalunya – UPC	Másteres/itinerarios en seguridad TIC/ciberseguridad	Grado y máster en Inteligencia Artificial
Universitat Oberta de Catalunya – UOC	Máster Univ. en Ciberseguridad y Privacidad	Programas en IA, ciencia de datos y tecnologías de información
Universidad de Granada – UGR	Ciberseguridad dentro de TIC/ingeniería informática	Grado/área fuerte en IA, data science, soft computing
Universitat Politècnica de València – UPV	Seguridad informática/ciberseguridad en	Máster Univ. en Inteligencia Artificial
Universidad de Málaga – UMA	Máster Univ. en Ciberseguridad	IA, software, data science, TIC
Universidad de Deusto	Máster/posgrado en ciberseguridad	Grado en Inteligencia Artificial
Universidad Internacional de La Rioja - UNIR	Máster en Ciberseguridad	Máster en Inteligencia Artificial
Universidad Europea - UE	Grados/másteres en ciberseguridad	Programas en IA, data y tecnologías digitales

Estas instituciones tienen ofertas universitarias o posgrados relevantes en ciberseguridad y en IA/ML/data, especialmente donde se ha podido articular trayectorias de grado–máster–doctorado.

La tabla 2 a continuación refleja se presenta una lista de programas formativos reflejando el nivel de encaje entre ciberseguridad + IA, teniendo en cuenta la siguiente referencia de prioridades:

- **Alta**: ciberseguridad + IA explícita o muy cercana.
- **Media:** ciberseguridad sólida con analítica, automatización, privacidad, datos o IA aplicada.

Tabla 2. Programas formativos en España por prioridades Ciberseguridad+IA

Curso	Programa	Institución	Encaje	Fuente
Formación especializada	MOOCs en ciberseguridad, con contenidos actuales sobre IA	INCIBE	Alta	https://www.incibe.es/incibe/formacion/moocs
Máster Universitario en Ciberseguridad	Máster Universitario	UNIR	Media-Alta	https://www.unir.net/ingenieria/master-ciberseguridad/
Máster Universitario de Ciberseguridad y Privacidad	Máster Universitario	UOC	Media-Alta	https://www.uoc.edu/es/estudios/masters/master-universitario-ciberseguridad-privacidad
Máster en Ciberseguridad	Máster Universitario	UC3M	Media-Alta	https://www.uc3m.es/master/ciberseguridad

Máster Universitario en Ciberseguridad	Máster Universitario	UPM	Media-Alta	https://www.upm.es
Máster Profesional en Dirección de Ciberseguridad	Hacking Ético y Seguridad Ofensiva	EIP International Business School	Media-Alta	https://eiposgrados.com/programas/master-en-ciberseguridad
Máster en Inteligencia Artificial	Complemento útil para perfiles cyber/ia	EIP International Business School	Media	https://eiposgrados.com/programas/master-en-inteligencia-artificial/
Cursos y másteres	Ciberseguridad y Cloud Computing	Euroinnova International Online Education	Media	https://www.euroinnova.com/ciberseguridad-y-cloud-computing
Área de Ciencia de Datos e Inteligencia Artificial	Complemento para Cyber analytics	Euroinnova	Media	https://www.euroinnova.com/ciencia-de-datos-e-inteligencia-artificial
Cursos de ciberseguridad	IA dentro de formación digital subvencionada	SEPE / Fundae – Digitalízate Plus	Media	https://www.fundae.es / https://www.sepe.es

Ahora bien, es importante resaltar que hoy la ciberseguridad e Inteligencia Artificial ya no son áreas separadas. De hecho, no deberían aislarse, ya que se potencian. En el caso de las ciberamenazas. sirven como agentes donde incrementan su impacto, pero también, como se indicó anteriormente, permiten amplificar, incrementar y potenciar la prevención, detección y neutralización de amenazas para la ciberseguridad.

Teniendo en cuenta lo anterior, una combinación de ciberseguridad e Inteligencia Artificial en programas educativos permite:

- Formar profesionales más completos: que entiendan sobre seguridad, datos, automatización, riesgos y toma de decisiones.
- Responder a amenazas modernas: phishing automatizado, deepfakes, malware asistido por IA, desinformación, ataques a modelos de IA.
- Uso de la IA para una mejor defensa: detección de anomalías, análisis de logs, respuesta a incidentes, inteligencia de amenazas y automatización SOC.
- Proteger los propios sistemas de IA: evitar manipulación de datos, sesgos, robo de modelos, ataques adversariales y uso indebido.
- Desarrollar pensamiento crítico: no solo aprender herramientas, sino entender riesgos éticos, legales, estratégicos y sociales.
- Preparar talento para el mercado actual: gobiernos, empresas y defensa necesitan perfiles híbridos capaces de unir seguridad, IA y estrategia.

En resumen, la IA aumenta las capacidades del atacante y del defensor. Por ello, educar en ciberseguridad sin IA queda incompleto; y enseñar IA sin seguridad puede ser arriesgado.

2.3. Evaluación de las necesidades en ciberseguridad

El primer reporte de necesidades elaborado por CyberHubs España entre 2023 y 2024 elaboró un análisis del mercado laboral donde se buscó identificar en España los perfiles y competencias más demandados. Esta clasificación de perfiles profesionales se basó en el European Cybersecurity Skills Framework (ECSF) de ENISA de 2022.

En primer lugar, destacan los implementadores y arquitectos de ciberseguridad, que concentran la mayoría de las ofertas laborales por la afinidad de sus competencias, principalmente en "compliance". En segundo lugar, se identificó una necesidad significativa de profesionales en respuesta a incidentes. Finalmente, también se observó una demanda de perfiles con "soft skills" orientadas a la gestión, el análisis y el liderazgo, especialmente desde la perspectiva del CISO.

Para actualizar el análisis y evaluar los resultados, la demanda actual en España se contrastó con ofertas activas a julio de 2026 en InfoJobs, LinkedIn Jobs, Tecnoempleo.com, Trabajos.com y Talent.com. El análisis de la información se realizó en dos fases: primero, con ofertas centradas únicamente en ciberseguridad; y, después, con ofertas que combinan ciberseguridad e inteligencia artificial. Este enfoque responde al impacto creciente de la IA en el ciberespacio, tanto en defensa y seguridad como en ataques y ciberamenazas. Para ello, se consideraron el Reglamento Europeo de Inteligencia Artificial, la norma ISO/IEC 42001:2023 y el OWASP GenAI Security Project.

Evidencia actual de demanda en España:

Plataformas de empleo activas consultadas que reflejaron resultados significativos:

- LinkedIn Jobs España: 3066 ofertas.
- LinkedIn Jobs: 603 ofertas específicas de ciberseguridad + inteligencia artificial.
- Tecnoempleo: 260 ofertas de ciberseguridad revisadas.
- Trabajos.com: 66 ofertas de ciberseguridad.
- Talent.com España: 56 ofertas específicas de ciberseguridad + inteligencia artificial

La información se extrajo de dichas plataformas utilizando los perfiles del ENISA ECSF como referencia. Los números son aproximados y pueden solaparse entre perfiles, teniendo en cuenta que hay competencias que se requieren en uno o varios perfiles.

Tabla 3. Número de ofertas de empleo en ciberseguridad

Perfil ENISA / ECSF	Role	Ofertas
Cybersecurity Implementer	Cybersecurity Engineer	1.033
Penetration Tester	Penetration Tester	523
Cybersecurity Architect	Security Architect	488
Cybersecurity Researcher	Security Researcher	334
Cybersecurity Educator	Security Awareness	204
Cyber Legal, Policy & Compliance Officer	Cybersecurity Compliance	195
Cybersecurity Risk Manager	Information Security Risk	174
CISO	“CISO”	155
Cyber Incident Responder	Incident Response Cybersecurity	104
Digital Forensics Investigator	Digital Forensics	59
Cyber Threat Intelligence Specialist	Cyber Threat Intelligence	45
Cybersecurity Auditor	Cybersecurity Auditor	25

Se conluyó que el mercado español está concentrado en perfiles técnicos-operativos: implementación, ingeniería, "pentesting" y arquitectura. La tendencia se mantiene. El mayor porcentaje de profesionales requeridos son aquellos con conocimientos y competencias para ser implementadores de ciberseguridad, evidenciando la necesidad que están requiriendo las empresas, compañías e instituciones para la implementación de sistemas de ciberseguridad, teniendo en

cuenta estándares de seguridad y el "compliance". Asimismo, queda patente que la necesidad detectada en 2024 de arquitectos de ciberseguridad sigue vigente.

En segundo lugar, se observa un aumento en la demanda de profesionales con conocimientos y competencias en "penetration testing", especialmente en LinkedIn Jobs. En tercer lugar, se mantiene la necesidad de perfiles orientados a la gestión, el análisis y las "soft skills", donde roles como "researcher", "educator" y "compliance" se complementan con gestores de riesgo y perfiles CISO.

Posteriormente a este análisis, se realizó una búsqueda sobre ofertas en el mercado laboral para relacionar el impacto de la Inteligencia Artificial en la ciberseguridad, partiendo de los siguientes datos:

LinkedIn jobs. IA + ciberseguridad:

"Artificial Intelligence Cybersecurity" → 603 ofertas, donde se destacan 48 ofertas específicas de Inteligencia Artificial con conocimientos de ciberseguridad.

Realizando una búsqueda más amplia, se pudo encontrar lo siguiente:

En "Machine Learning Security" aparecen más de 1.000 ofertas, pero combinando seguridad, ML engineering y roles no necesariamente de ciberseguridad.

Tecnoempleos. IA + ciberseguridad:

"AI security": 38 ofertas

"Machine learning security": 9

"LLM security": 6

Combinando estas fuentes, las ofertas más específicas de ciberseguridad por perfil ENISA + IA quedan reflejadas en la siguiente tabla:

Tabla 4. Número de ofertas de empleo combinando ciberseguridad + IA

Perfil ENISA / ECSF	N.º ofertas	Ofertas ciberseguridad+ IA	% aprox.
Cybersecurity Implementer	95	12	12,6%
Cyber Incident Responder / SOC	28	8	28%
Cybersecurity Risk Manager	23	5–11	22-48%
Cyber Legal, Policy & Compliance Officer	31	2–3	6-10%
Cybersecurity Architect	12	10–11	83-92%*
Cyber Threat Intelligence Specialist	30	5	16,6%
Cybersecurity Auditor	17	1	6%*
Penetration Tester / Red Team	3	1	33%*
CISO / Cybersecurity Manager	35	5	14,2%*

**En perfiles donde el número de ofertas es limitado, el porcentaje puede quedar distorsionado.*

La IA aplicada a la ciberseguridad se requiere en el mercado laboral español, aunque aparece más como una competencia transversal que como un perfil laboral independiente y consolidado. La combinación explícita de ciberseguridad e IA sigue siendo limitada en las ofertas, pero se concentra principalmente en:

1. Cybersecurity Architect + IA
2. Cybersecurity Risk Manager + IA
3. Compliance / AI Governance
4. SOC / Incident Response con IA
5. AI Security / LLM Security / Red Team IA

De forma más descriptiva y clara, los perfiles más requeridos en la demanda actual en España, según ENISA + IA se reflejan como sigue:

1. Cybersecurity Implementer
   - En España aparece como: técnico/a, ingeniero/a, especialista de ciberseguridad.
   - Evidencia: ofertas de técnico junior, ingeniero, especialista N3, DLP, IAM/PAM.
   - Con IA: automatización defensiva, integración de IA en controles, seguridad de APIs, cloud y datos.

2. Cyber Incident Responder
   - En España aparece como: analista SOC, SOC Manager, responsable de monitorización.
   - Evidencia: ofertas SOC, SIEM, XSIAM, MITRE ATT&CK.
   - Con IA: detección asistida, triaje automático, correlación de alertas y respuesta automatizada.

3. Cybersecurity Risk Manager
   - En España aparece como: consultor GRC, riesgos IT, responsable de riesgos tecnológicos.
   - Muy demandado por ENS, ISO 27001, NIS2 y gestión de terceros.
   - Con IA: evaluación de riesgos de modelos, datos, proveedores IA y automatización.

4. Cyber Legal, Policy & Compliance Officer
   - En España aparece como: consultor ENS, compliance, auditoría normativa, privacidad.
   - Con IA: AI Act, RGPD, ISO 42001, gobierno de IA, políticas de uso seguro de IA.

5. Cybersecurity Architect
   - En España aparece como: arquitecto/a de ciberseguridad, cloud security architect, security solution architect.

6. Con IA: arquitectura segura para LLMs, MLOps/LLMOps, Zero Trust, IAM/PAM, protección de datos.
   Cyber Threat Intelligence Specialist
   - En España aparece como: responsable de inteligencia de ciberseguridad, CTI analyst.
   - Evidencia: ofertas con MITRE, MISP, inteligencia de amenazas.
   - Con IA: análisis de phishing automatizado, deepfakes, malware asistido por IA, campañas híbridas.

7. Cybersecurity Auditor
   - En España aparece como: auditor/a de riesgos IT, auditor/a ENS/ISO, auditor/a de IA & Data.
   - Con IA: auditoría de modelos, datasets, trazabilidad, sesgos, privacidad y controles.

8. Penetration Tester / AI Security Tester
   - Menos visible en volumen, pero estratégico.
   - Con IA: pruebas contra LLMs, prompt injection, jailbreaks, data leakage, plugins inseguros, agentes autónomos.

3. Análisis de las necesidades.

Una vez recolectada la información y habiéndola procesado para mayor claridad, se establece el siguiente análisis sobre los perfiles que cuya demanda será previsiblemente mayor en España en los siguientes años, teniendo en cuenta cómo la Inteligencia Artificial ira tomando mayor relevancia en el campo de la ciberseguridad.

3.1. Análisis por perfiles

1. Cybersecurity Architect: seguirá siendo un perfil muy importante por su relevancia dentro del diseño y la aplicación de modelos de ciberseguridad. Las organizaciones requerirán arquitecturas que les permitan integrar IA sin tener el riesgo de exponer o perder datos, identidades, modelos o procesos críticos. Nuevas competencias:

    - Seguridad en MLOps.
    - Protección de APIs de IA.
    - Zero Trust aplicado a sistemas inteligentes.
    - Model governance.
    - Seguridad de agentes autónomos.

2. Cybersecurity Risk Manager: la IA ha introducido nuevos riesgos y amenazas, por lo que serán necesarios expertos en toma de decisiones y análisis para destrezas opacas, fuga de datos, dependencia de proveedores, errores automatizados y vulnerabilidades en modelos. Será clave para responder a las siguientes preguntas:

    - ¿Qué procesos pueden usar IA?
    - ¿Qué datos pueden entrar en modelos?
    - ¿Qué decisiones no deben automatizarse?
    - ¿Cuál es el impacto si un modelo es manipulado?

3. Cyber Legal, Policy & Compliance Officer: este perfil está creciendo bastante por la actualización de nuevas tecnologías y la necesidad de regular el accionar de las mismas lo que generado sobre las organizaciones mayor presión regulatoria. En Europa, el AI Act, NIS2, DORA, GDPR y normas sectoriales harán que la ciberseguridad y la gobernanza de IA se crucen cada vez más. Nuevas funciones:

    - Evaluación de cumplimiento de sistemas IA.
    - Políticas internas de uso de IA.
    - Auditoría de proveedores IA.
    - Responsabilidad por decisiones automatizadas.

4. Cyber Threat Intelligence Specialist: la IA ha transformado la inteligencia de amenazas, ya que las amenazas están y podrán mejorar la automatización de campañas de phishing, influencia, reconocimiento y explotación. La IA potencia la guerra cognitiva coadyubando a la creación e innovación de los deepfakes, bots personalizados, microsegmentación psicológica y manipulación informativa a escala.

5. Cybersecurity Educator: la educación será crítica, ya que los usuarios se enfrentan a amenazas más creíbles, que con el tiempo serán cada vez más complejas y sofisticadas para la detección: correos perfectos, voces clonadas, videos falsos y asistentes maliciosos.

Es en este punto donde la concienciación tradicional, la cultura digital y la búsqueda de una sociedad digital requieren una adaptación a las nuevas tecnologías como la IA generativa, permitiendo que los ataques cognitivos sean prevenidos y detectados desde el conocimiento y la experiencia en todos los niveles.

Prospectiva de necesidades

La IA no eliminará la ciberseguridad, pero sí la va a reconfigurar profundamente, teniendo en cuenta las competencias y las necesidades de los perfiles laborales. Las tareas repetitivas, documentales y de primer nivel estarán siendo automatizadas; en cambio, crecerá la demanda de perfiles capaces de:

- Supervisar sistemas autónomos de defensa.
- Validar decisiones generadas por IA.
- Investigar amenazas potenciadas por IA.
- Proteger modelos, datos y cadenas de suministro de IA.
- Traducir riesgo técnico en decisiones estratégicas. La ventaja competitiva no será "saber usar IA", sino saber gobernarla, auditarla y contrarrestarla en contextos de ciberseguridad.

Es por esto por lo que los perfiles más amenazados por automatización parcial no desaparecerán, pero sí cambiarán. La IA hará gran parte del análisis inicial de alertas. El valor humano estará en:

- Juicio operacional.
- Priorización.
- Coordinación con negocio.
- Manejo de crisis.
- Decisiones bajo incertidumbre.

¿Cómo evolucionaran los perfiles acuerdo las necesidades?

CISO La IA aumentará la presión estratégica: gobernanza de IA, riesgo algorítmico, cumplimiento, ciberresiliencia y amenazas automatizadas. **Alta demanda estratégica**
Cyber Incident Responder La IA automatizará el triaje, correlación de alertas y respuesta inicial. El valor humano quedará para decisiones críticas, contención compleja y coordinación. **Transformación fuerte**
Cyber Legal, Policy & Compliance Officer Crecerá por regulación de IA, NIS2, AI Act, privacidad, responsabilidad algorítmica y auditoría de modelos. **Crecimiento alto**
Cyber Threat Intelligence Specialist La IA mejorará recolección y análisis, pero también multiplicará desinformación, deepfakes, phishing avanzado y operaciones cognitivas. **Crecimiento alto**
Cybersecurity Architect Deberá diseñar arquitecturas seguras con IA integrada: Zero Trust, seguridad de modelos, pipelines MLOps, protección de datos y APIs. **Muy alta demanda**
Cybersecurity Auditor Crecerá la auditoría de IA, explicabilidad, trazabilidad, sesgos, seguridad de modelos y cumplimiento técnico-regulatorio. **Crecimiento medio-alto**

Cybersecurity Educator Requerirá una formación adicional en higiene digital frente a ataques con IA: deepfakes, ingeniería social automatizada, prompts maliciosos, uso seguro de IA. **Crecimiento alto**
Cybersecurity Implementer La IA automatizará la configuración, hardening, scripting y monitoreo básico, pero aumentará la demanda de implementación segura de herramientas IA. **Alta demanda, perfil transformado**
Cybersecurity Researcher Crecerá en áreas como adversarial ML, ataques a LLMs, poisoning, model theft, prompt injection, privacidad y seguridad de agentes autónomos. **Crecimiento especializado**
Cybersecurity Risk Manager Será clave para evaluar riesgo de IA, dependencia tecnológica, exposición de datos, terceros, continuidad y riesgo sistémico. **Muy alta demanda**
Digital Forensics Investigator La IA ayudará en análisis forense, pero complicará la atribución por deepfakes, logs sintéticos y malware generado dinámicamente. **Demanda estable-alta**
Penetration Tester La IA automatizará el reconocimiento, explotación básica y generación de payloads. El valor humano se centrará en la creatividad, cadenas de ataque y validación real. Las pruebas básicas serán cada vez más automatizadas. El pentester competitivo deberá pasar de "ejecutar herramientas" a: • Diseñar escenarios complejos. • Encadenar vulnerabilidades. • Evaluar impacto real. • Simular adversarios avanzados. • Probar sistemas IA. **Transformación fuerte**

Asimismo, se crearán nuevos sub-perfiles emergentes que permitirán potenciar los ya conocidos mediante el uso de IA. Aunque ENISA no los separe todavía como perfiles independientes, se espera que los siguientes roles mostrarán un crecimiento moderado:

1. AI Security Architect
2. LLM Security Specialist
3. Adversarial Machine Learning Analyst
4. AI Governance & Cyber Risk Officer
5. Prompt Injection / Agent Security Tester
6. Synthetic Media Threat Analyst
7. AI-Enabled SOC Analyst
8. Model Supply Chain Security Specialist

Es importante resaltar, una vez más, que la IA desplazará tareas, no necesariamente profesiones completas. Los perfiles más operativos deberán desarrollar y elevar su nivel analítico, mientras que los perfiles estratégicos, de riesgo, arquitectura, inteligencia y cumplimiento ganarán importancia.

En términos laborales, la ciberseguridad previsiblemente evolucionará hacia tres grandes bloques:

1. Ciberseguridad asistida por IA SOC, respuesta, monitoreo, pentesting, forense.
2. Ciberseguridad de la IA, Protección de modelos, datos, pipelines, agentes y APIs.
3. Ciberseguridad frente a amenazas potenciadas por IA, Deepfakes, phishing autónomo, malware generado, manipulación cognitiva e influencia informativa.

Los profesionales que combinen ciberseguridad + IA + análisis estratégico de riesgo tendrán una posición muy relevante en el mercado europeo, especialmente en España y la UE. La demanda actual ya no necesita solo "más técnicos de ciberseguridad". La gran necesidad se centrará en perfiles capaces de combinar ciberseguridad + IA + datos + regulación europea + análisis + liderazgo. Es en este punto donde el desarrollo y creación de nuevos programas educativos, así como la comunicación entre los sectores, es fundamental para obtener y permitir la obtención de nuevos y mejores profesionales de la ciberseguridad.

3.2. Análisis prospectivo (amenazas y riesgos)

A partir del análisis realizado sobre las tendencias de los perfiles profesionales y la capacitación en España para los próximos años, también es necesario desarrollar un análisis prospectivo de las amenazas y riesgos actuales y potenciales. Este análisis debe considerar cómo dichas amenazas pueden evidenciarse y potenciarse debido a las brechas existentes y a las necesidades que aún no han sido cubiertas.

Cabe destacar que muchas necesidades del mercado laboral no se han cubierto por la falta de profesionales cualificados. Esto responde principalmente a dos factores: en primer lugar, la escasez de perfiles con la formación y las competencias específicas requeridas para acceder a estas ofertas; y, en segundo lugar, unos salarios y remuneraciones económicas que siguen siendo inferiores a los de otros países de la región, especialmente dentro de la Unión Europea. Esta diferencia impulsa a muchos profesionales a buscar mejores oportunidades económicas fuera de España.

Asimismo, desde la perspectiva de la capacitación y la educación, aunque se observa una mejora en los programas existentes, sigue siendo necesario reforzar los esfuerzos para cubrir las necesidades actuales. Además de los programas de pregrado, máster y doctorado, resulta clave desarrollar y fortalecer microcredenciales y certificaciones en competencias específicas de ciberseguridad, que atraigan a un público más amplio y contribuyan a ampliar la fuerza laboral en ciberseguridad. Aunque algunas instituciones ya ofrecen este tipo de formación, se requiere un mayor impulso, especialmente para seguir apoyando la innovación.

Durante los próximos dos años, España afrontará la convergencia de cibercrimen financiero, ransomware, hacktivismo geopolítico, espionaje estatal y manipulación informativa asistida por IA. El riesgo no se limitará a la intrusión técnica; también dependerá de la capacidad de los atacantes para erosionar la confianza pública, interrumpir servicios esenciales y afectar la estabilidad institucional.

España será un objetivo atractivo por cinco factores:

1. Elevada digitalización pública y privada.
2. Pertenencia a la OTAN y a la UE.
3. Infraestructura crítica altamente conectada: energía, transporte, salud y telecomunicaciones.
4. Mayor exposición de PYMEs y ayuntamientos con menor madurez en ciberseguridad.
5. Valor geopolítico como puente europeo hacia América Latina y el Mediterráneo.

Amenazas principales

1. **Ransomware y extorsión múltiple**

Probabilidad: Muy alta
Impacto: Muy alto

El ransomware seguirá siendo la amenaza dominante para empresas, hospitales, administraciones locales, universidades y proveedores tecnológicos. La Inteligencia Artificial permite a las amenazas el modelamiento de las mismas para la sofisticación de los ataques.

Desde el punto de vista del riesgo prospectivo, éste podrá estar focalizado a un aumento de ataques contra proveedores medianos que sirven a grandes instituciones. El atacante preferirá el eslabón débil antes que atacar directamente al objetivo estratégico.

La evolución esperada no será solo cifrada de sistemas, sino:

- Robo previo de datos.
- Amenaza de filtración pública.
- Presión a clientes y proveedores.
- Ataques DDoS complementarios.
- Extorsión reputacional y regulatoria.

Los sectores más expuestos en España podrán ser los siguientes:

- Sanidad.
- Gobiernos autonómicos y ayuntamientos.
- Educación superior.
- Despachos legales y consultoras.
- Industria y logística.
- Turismo y hotelería.

2. **Ataques a disponibilidad: DDoS, sabotaje digital y presión hacktivista**

Probabilidad: Alta
Impacto: Medio-alto / Alto

ENISA ya identifica las amenazas contra la disponibilidad como una de las principales tendencias europeas. En España esto se puede traducir en campañas contra:

- Webs gubernamentales.
- Bancos.
- Puertos y aeropuertos.
- Empresas energéticas.
- Medios de comunicación.
- Organizaciones vinculadas a OTAN, Ucrania, Israel/Palestina, migración o crisis diplomáticas.

Actores probables:

- Grupos hacktivistas prorrusos.
- Colectivos ideológicos.
- Grupos criminales alquilando botnets.
- Operaciones de influencia encubiertas.

Riesgo clave: aunque muchos DDoS tienen bajo impacto técnico, generan percepción de vulnerabilidad estatal.

3. **Espionaje cibernético estatal y robo de información estratégica en grandes corporaciones.**

Probabilidad: Alta
Impacto: Muy alto

España podrá ser objetivo de actores estatales o patrocinados por Estados interesados en:

- Política exterior y defensa.
- Industria militar.
- Energía.
- Telecomunicaciones.
- Investigación universitaria.
- Relaciones UE-OTAN.
- Información sobre América Latina, Norte de África y Mediterráneo.

Vectores esperados:

- Spear phishing contra funcionarios, militares, académicos, gerentes, CEO, y periodistas.
- Compromiso de correos corporativos.
- Malware en dispositivos móviles.
- Ataques a proveedores de software.
- Explotación de vulnerabilidades zero-day o n-day.

Se puede esperar un aumento en el espionaje contra centros de investigación, think tanks y universidades españolas, especialmente en áreas de IA, defensa, energía, semiconductores, ciberseguridad y geopolítica.

4. **Fraude digital, phishing y deepfakes**

Probabilidad: Muy alta
Impacto: Alto

La IA generativa reduce el coste del engaño, apareciendo campañas más creíbles, personalizadas y multilingües.

Amenazas esperadas:

- Phishing bancario más sofisticado.
- Suplantación de directivos por voz.
- Deepfakes para fraude corporativo.
- Estafas a ciudadanos usando identidad de instituciones públicas.
- Falsos trámites, multas, becas, ayudas o campañas tributarias.
- Romance scams y fraudes a adultos mayores.

5. **Ataques a cadena de suministro**

Probabilidad: Alta
Impacto: Muy alto

España podrá sufrir más incidentes indirectos. El objetivo final no será atacado directamente, sino a través de:

- Proveedores TIC.
- Software de gestión.
- MSP/MSSP.
- Plataformas cloud.
- Integradores industriales.
- Empresas de mantenimiento.
- Proveedores de ayuntamientos o sanidad.

Escenario probable: un proveedor regional comprometido permite acceso simultáneo a múltiples clientes públicos y privados.

Implicación: la ciberseguridad dejará de ser un asunto interno. La madurez de terceros será parte del riesgo nacional.

6. **Infraestructura crítica y sistemas industriales**

Probabilidad: Media-alta
Impacto: Muy alto

No todos los ataques buscarán destrucción. Muchos podrán buscar reconocimiento, preposicionamiento o capacidad latente.

Sectores prioritarios:

- Energía eléctrica.
- Agua.
- Puertos.
- Transporte ferroviario.
- Telecomunicaciones.
- Sanidad.
- Industria alimentaria.
- Satélites y servicios espaciales.

Riesgo prospectivo: crecimiento de ataques híbridos donde se combinan intrusión técnica, filtraciones, desinformación y presión política.

Teniendo en cuenta que para este informe se realizó una revisión literaria de diferentes estudios y análisis de la ciberseguridad en España, se pudo establecer que el consenso de estos se evidencian las siguientes cinco tendencias estructurales:

1. Los atacantes cada vez más rápidos. CrowdStrike evidencia que los tiempos de “breakout” son cada vez más cortos, así como, más intrusiones sin malware, lo que reduce la ventana para una defensa efectiva.

2. La identidad toma mayor relevancia que nunca y es catalogada como "el nuevo perímetro". IBM, Microsoft y Verizon evidencian la necesidad de trabajar en credenciales, tokens, MFA débil, identidades no humanas y abuso de accesos cloud, siendo estos vectores críticos.

3. La IA amplificará el poder de los atacantes para el engaño, no solo el malware. El principal impacto inmediato se reflejará en el phishing personalizado, fraude por voz, deepfakes, automatización de reconocimiento y reducción de barreras para actores menos sofisticados.

4. La cadena de suministro se evidencia como un vector altamente estratégico. Mandiant/Google, ENISA y Verizon evidencian la importancia de los proveedores tecnológicos, MSP, SaaS y software vulnerable los cuales se convertirán en los principales puntos de entrada preferentes.

5. La ciberseguridad para la geopolítica. España, por su posición UE-OTAN, Mediterráneo, relación con América Latina y peso en sectores críticos, podrá ser objetivo tanto de crimen organizado como de actores estatales o proxies, donde la ciberseguridad cognitiva tendrá un papel determinante.

Matriz de impacto cruzado enfocada en los riesgos cibernéticos para el sector privado en España 2026-2028.

Teniendo en cuenta las principales amenazas analizadas, a continuación se muestra una matriz de impacto cruzado con el propósito de establecer su impacto, relevancia y clasificación.

Tabla 5. Matriz de impacto de amenazas cibernéticas

Riesgo / Amenaza	Ransomware	Identidad digital	Fraude IA	Cadena suministro	Vulnerabilidades	Cloud/ SaaS	Fuga datos	OT/ICS	DDoS	Desinformación	Influencia total
Ransomware y extorsión múltiple	*	2	1	2	2	2	3	3	1	3	**19**
Abuso de identidad digital	3	*	3	2	1	3	3	2	1	2	**20**
Fraude digital asistido por IA	2	3	*	1	0	2	2	0	0	3	**13**
Ataques a cadena de suministro	3	3	1	*	3	3	3	3	2	2	**23**
Explotación de vulnerabilidades	3	1	0	2	*	2	3	2	2	1	**16**
ataque Cloud/SaaS	3	3	2	2	2	*	3	1	1	2	**19**
Fuga de datos / sanciones RGPD	2	2	2	2	2	2	*	1	0	3	**16**
Ataques a OT/ICS	2	1	0	3	2	1	2	*	1	2	**14**
ataque de DDoS / disponibilidad	1	0	0	1	1	1	0	1	*	3	**8**
Desinformación y daño reputacional	2	2	3	1	1	1	3	1	2	*	**16**
Dependencia total	**21**	**17**	**12**	**16**	**14**	**17**	**22**	**14**	**10**	**21**	

Escala utilizada:
0: sin impacto directo
1: impacto bajo
2: impacto medio
3: impacto alto

Análisis de la matriz de impacto cruzado.

La siguiente tabla refleja la clasificación estratégica de la matriz de impacto cruzado (tabla 5):

Tabla 6. Clasificación estratégica de la matriz de impacto cruzado

Categoría	Amenazas
Variables motrices	Cadena de suministro, identidad digital, ransomware, cloud/SaaS
Variables dependientes	Fuga de datos, desinformación reputacional, ransomware
Variables críticas	Ransomware, identidad digital, cadena de suministro, fuga de datos
Variables de apoyo / amplificación	DDoS, fraude IA, vulnerabilidades expuestas, OT/ICS

España podrá enfrentar una amenaza híbrida, donde la cibernética estará marcada por la convergencia y la sofisticación del ransomware, la explotación de vulnerabilidades y el abuso de identidad digital, todo con el uso de una IA ofensiva, potenciando principalmente los ataques a cadena de suministro, ciberespionaje empresarial y estatal y las operaciones de influencia.

Las amenazas más importantes y prioritarias para España son:

1. Cadena de suministro. Es el mayor multiplicador de todo el sistema. Un proveedor comprometido puede afectar a muchas empresas al mismo tiempo. Se destacan aquí los proveedores medianos como puerta de entrada a grandes organizaciones, compañías o instituciones privadas y públicas.

2. Abuso de identidad digital. El fraude digital aumentará su sofisticación mediante el uso de IA, que funciona como puerta de entrada para ransomware, fraude, cloud compromise, fuga de datos y accesos persistentes. El phishing, smishing, vishing, deepfakes a directivos, impactará mediante el riesgo de suplantación institucional y fraudes bancarios. Esta amenaza será muy relevante y de alto impacto principalmente para ciudadanos, la banca, aseguradoras y la administración pública.

3. Ransomware y extorsión múltiple. Es la amenaza de mayor impacto y ocurrencia para la continuidad del negocio, la reputación y el cumplimiento regulatorio. Su alta probabilidad de ocurrencia será potenciada mediante el uso de IA, especialmente contra sanidad, ayuntamientos, universidades, PYMEs, logística, turismo y proveedores TIC.

4. Fuga de datos / RGPD crecerá como el principal efecto acumulativo. Muchas amenazas terminan produciendo exposición de información, multas o pérdida de confianza. Es aquí donde también entra el ciberespionaje empresarial o estatal. Se establecen por tanto como objetivos la defensa, energía, telecomunicaciones, universidades, think tanks, diplomacia, industria dual, investigación en IA/ciber/espacio.

5. Desinformación y daño reputacional. Convertir un incidente cibernético en una crisis pública y reputacional, especialmente si hay filtraciones, deepfakes, DDoS o manipulación narrativa. Este aspecto fortalece a las operaciones híbridas de influencia mediante filtraciones reales o manipuladas, DDoS simbólicos y narrativas polarizantes para erosionar confianza pública.

6. Ataques a infraestructuras críticas y OT, como la energía, agua, transporte, puertos, salud, telecomunicaciones e industria, constituyendo un riesgo creciente para el reconocimiento/preposicionamiento más que sabotaje inmediato.

4. Análisis prospectivo de Amenazas vs Necesidades

Las amenazas actuales en España influyen directamente en todo el sistema y por ende en la demanda de profesionales de ciberseguridad. No se trata de una demanda genérica, sino de una necesidad especifica donde los perfiles capaces de responder a diferentes tipos de riesgos y amenazas como la cadena de suministro, el abuso de identidad digital, el ransomware, la fuga de datos y la desinformación son primordiales para el entendimiento, la toma de decisiones y el liderazgo tecnológico dentro de las compañías y entidades.

Al mismo tiempo, el déficit de los perfiles más demandados aumenta la probabilidad y el impacto de estas amenazas. La relación es, por tanto, bidireccional: las amenazas elevan la demanda de talento, mientras que su escasez incrementa la exposición frente a ellas.

4.1. Relación entre amenazas y perfiles más requeridos

1. Cadena de suministro

El riesgo de que la cadena de suministro sea atacada por las amenazas como los ataques a la OT o el ramsoware exige profesionales capaces de evaluar proveedores, gestionar riesgos de terceros, auditar controles y diseñar arquitecturas seguras. Por eso impacta especialmente en la demanda de los siguientes roles:

- Cybersecurity Implementer
- Cybersecurity Risk Manager
- Cyber Legal, Policy & Compliance Officer
- Cybersecurity Architect
- Cyber Threat Intelligence Specialist

En España, esta necesidad se refleja en la demanda de consultores GRC, responsables de riesgos tecnológicos, perfiles ENS, ISO 27001, NIS2, arquitectos cloud y especialistas en seguridad. Con IA, el riesgo se incrementa porque muchas organizaciones dependen de proveedores y modelos que ofrecen APIs y plataformas externas con uso de IA, obligando a las compañías e instituciones a evaluar no solo proveedores tecnológicos tradicionales, sino también los riesgos asociados a datos, automatización y modelos inteligentes.

2. Abuso de identidad digital

El abuso de identidad digital es la principal puerta de entrada para amenazas como el ransomware, fraude, compromiso cloud, fuga de datos y accesos persistentes. incrementando la necesidad de profesionales en áreas como las siguientes:

- Cybersecurity Implementer
- Cyber Incident Responder
- Cybersecurity Architect
- Cyber Threat Intelligence Specialist

En España, esta demanda se especializa en técnicos, ingenieros, especialistas en IAM/PAM, analistas SOC, perfiles N3 y arquitectos de seguridad. La IA potencializa esta necesidad porque permite la mejora de la detección de accesos anómalos contra la sofisticación de los ataques de phishing, suplantación y fraude.

Por ello, los profesionales en esta área específica precisan de las capacidades necesarias para automatización defensiva, detección asistida y controles de identidad más robustos.

3. Ransomware y extorsión múltiple:

Esta amenaza exige que el profesional tenga capacidades para entender, analizar y establecer medidas de prevención, detección, respuesta, recuperación y gestión de crisis. Por eso impacta sobre:

- Cyber Incident Responder
- Cybersecurity Implementer
- Cybersecurity Architect
- Cyber Threat Intelligence Specialist
- Cybersecurity Risk Manager
- Cyber Legal, Policy & Compliance Officer

Las ofertas relacionadas con SOC, SIEM, XSIAM, MITRE ATT&CK, continuidad, cumplimiento y gestión de incidentes, son aquellas que buscan este conocimiento en prevención, detección, respuesta, recuperación y gestión.

Aun así, la IA modificará estos perfiles en dos sentidos, ya que permitirá asistencia en la automatización, correlación de alertas y respuesta; pero queda patente que su uso potenciará cada vez más la rapidez de los ataques, impulsando amenazas como el phishing, volviéndolo más creíble, así como el malware, haciéndolo más sofisticado. Por tanto, se requieren profesionales capaces de combinar operación técnica, inteligencia y gestión estratégica.

4. Fuga de datos / RGPD:

Como se ha explicado anteriormente, esta amenaza constituye el resultado final de la explotación de las anteriores, como el abuso de identidad, ransomware, proveedores comprometidos o errores en cloud. Se incrementa de esta manera la necesidad de profesionales en:

- Cyber Legal, Policy & Compliance Officer
- Cybersecurity Risk Manager
- Cybersecurity Implementer
- Cybersecurity Architect
- Cyber Incident Responder

En España, el peso de las normativas de RGPD, ENS, NIS2 e ISO 27001 hace que los perfiles de compliance, privacidad, auditoría normativa y riesgos tecnológicos sean altamente requeridos e importantes.

Con el uso IA en la ciberseguridad, esta dimensión se vuelve más crítica, ya que los modelos requieren procesar grandes volúmenes de datos e información sensibles. Por eso aparecen nuevas necesidades, principalmente el gobierno de IA, ISO 42001, y protección de datos en modelos, donde el uso seguro de IA y la evaluación de proveedores IA es clave para la implementación de estrategias, planes y campañas de ciberseguridad.

5. Desinformación y daño reputacional:

Actualmente vivimos en la era de la "pos-verdad", donde la desinformación convierte un incidente técnico en crisis y daño reputacional difícil de reparar. Los actores que quieren amplificar o modificar filtraciones utilizan el ransomware como principal arma para la obtención de información, de esta manera realizar deepfakes, DDoS o narrativas manipuladas. Esta amenaza incrementa la necesidad de profesionales como:

- Cyber Threat Intelligence Specialist
- Cyber Incident Responder
- Cyber Legal, Policy & Compliance Officer
- Cybersecurity Risk Manager
- Cybersecurity Architect

Aquí el perfil de inteligencia de amenazas es donde toma especial relevancia, ya que permite el análisis de actores, campañas, narrativas, indicadores y posibles impactos reputacionales.

Actualmente se ha evidenciado a nivel mundial cómo esta amenaza se vuelve más compleja por el uso de la IA, donde los deepfakes, la generación automatizada de contenido, el phishing avanzado y la manipulación narrativa generan un alto impacto. Por eso, la ciberseguridad ya no puede limitarse a proteger sistemas: también debe proteger confianza, reputación e información pública, pero principalmente enfocarse en una ciberseguridad cognitiva.

En síntesis, los perfiles ENISA a los que se aplica la IA más demandados en España responden directamente a las amenazas prioritarias:

- Cybersecurity Implementer: necesario para materializar controles frente a identidad, ransomware, fuga de datos y cloud.
- Cybersecurity Implementer: necesario para materializar controles frente a identidad, ransomware, fuga de datos y cloud.
- Cyber Incident Responder: clave para contener ransomware, accesos indebidos, fugas y crisis técnicas.
- Cybersecurity Risk Manager: fundamental para cadena de suministro, NIS2, ENS, ISO 27001 y riesgos de IA.
- Cyber Legal, Policy & Compliance Officer: esencial frente a RGPD, AI Act, ENS, privacidad y obligaciones regulatorias.
- Cybersecurity Architect: necesario para diseñar entornos seguros, Zero Trust, IAM/PAM, cloud, LLMs y protección de datos.
- Cyber Threat Intelligence Specialist: transversal para anticipar ransomware, abuso de identidad, campañas híbridas, deepfakes y amenazas contra proveedores.

6. Conclusiones

En conclusión, la incorporación de la IA al panorama de las ciberamenazas está aumentando la sofisticación de los ataques y dificultando su detección. Este escenario eleva los riesgos para la continuidad del negocio y los costes asociados a la ciberseguridad, al tiempo que confirma la necesidad urgente de formar profesionales capaces de integrar competencias técnicas, estratégicas y de Inteligencia Artificial para responder con eficacia a los desafíos actuales y futuros.

La colaboración sostenida entre los sectores público y privado y la academia será determinante para anticipar las necesidades de talento en ciberseguridad y responder a su evolución. Este diálogo debe traducirse en programas formativos actualizados y alineados con la demanda real del mercado laboral, capaces de preparar profesionales con las competencias necesarias para afrontar los desafíos presentes y futuros.

Las amenazas prioritarias que afronta España exigen una respuesta basada en perfiles de ciberseguridad más especializados, híbridos y estratégicos. La Inteligencia Artificial refuerza las capacidades defensivas mediante la automatización, la detección asistida y el análisis avanzado, pero también amplifica riesgos como el phishing, la desinformación, el abuso de identidad, las fugas de datos y los ataques a proveedores. Por ello, resulta esencial formar profesionales que combinen las funciones definidas por ENISA con competencias en IA, gestión de riesgos, cumplimiento y anticipación de amenazas. Reducir la escasez de este talento será determinante para contener riesgos cada vez más sistémicos y fortalecer la resiliencia digital del país.

Se estima que en 2026 y 2028 España afrontará un panorama de ciberamenazas cada vez más híbrido, en el que convergerán dimensiones técnicas, económicas, geopolíticas y cognitivas. El principal riesgo no será únicamente la interrupción de sistemas y servicios esenciales, sino también los ataques cognitivos, desde un enfoque cibernético, que genera efectos sistémicos en democracias, la erosión de la confianza en la capacidad del Estado, las empresas y las instituciones para protegerlos y diferenciar la información veraz de la manipulación. Por ello, es necesario implementar un modelo de *Ciberseguridad cognitiva* que permita integrar defensa técnica, inteligencia narrativa y resiliencia social, además de todos los factores característicos de la ciberseguridad como la hemos conocido hasta hoy, reforzando la protección de los datos, los sistemas y las infraestructuras para preservar la confianza pública y garantizar la continuidad democrática, económica e institucional.

Es imperativo preparar talento para el mercado actual, teniendo en cuenta las actuales y potenciales amenazas de carácter hibrido a las que se enfrenta Espala. Se necesitan perfiles híbridos capaces de unir ciberseguridad, IA y estrategia. Como refleja este informe, la IA aumenta las capacidades del atacante y del defensor. Por eso, educar en ciberseguridad sin IA queda incompleto; y enseñar IA sin seguridad puede ser arriesgado.

Cyberhubs constituye un canal de comunicación y un brazo fuerte de la conciencia situacional en ciberseguridad, mediante su constante apoyo a eventos, reuniones y charlas en busca de incrementar el apoyo interinstitucional e intersectorial para el fortalecimiento de la ciberseguridad en España. Así, se han podido evidenciar las necesidades actuales y potenciales del mercado laboral al igual que educativas, además de servir de apoyo a pequeñas y medianas entidades que requieren visibilidad y soporte.

Mantener iniciativas como CyberHubs, centradas en la conciencia situacional, la colaboración y la comunicación estratégica, apoya a España en el refuerzo de sus capacidades para afrontar nuevos retos. Asimismo, favorecerá la cooperación entre sectores, la innovación y el intercambio de conocimiento necesarios para responder a los desafíos emergentes del ciberespacio y fortalecer la ciberseguridad nacional.

7. Referencias

Accenture. (s. f.). *Cyber threat intelligence report*. https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report

CCN-CERT/CNI. (s. f.). *Informes públicos CCN-CERT*. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html

Center for Strategic and International Studies. (s. f.). *Cybersecurity and governance*. https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance

Check Point Research. (s. f.). *Cyber security research*. https://research.checkpoint.com/

CrowdStrike. (2026). *Global threat report*. https://www.crowdstrike.com/en-us/global-threat-report/

Deloitte. (s. f.). *Future of cyber*. https://www.deloitte.com/global/en/Industries/technology/research/future-of-cyber.html

European Union. (2024). *Regulation (EU) 2024/1689: Artificial Intelligence Act*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

European Union Agency for Cybersecurity. (2022a). *European cybersecurity skills framework (ECSF): User manual*. ENISA. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf European Union Agency for Cybersecurity. (2022b). *European cybersecurity skills framework role profiles*. ENISA. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Europol. (s. f.). *Main reports*. https://www.europol.europa.eu/publications-events/main-reports EY. (s. f.). *Cybersecurity*. https://www.ey.com/en_gl/cybersecurity

Fortinet. (s. f.). *FortiGuard Labs threat research*. https://www.fortinet.com/fortiguard/labs/threat-research

Google Cloud. (2026). *M-Trends report*. https://cloud.google.com/security/resources/m-trends

IBM. (2026). *Cost of a data breach report*. https://www.ibm.com/reports/data-breach

INCIBE. (s. f.). *Sala de prensa*. Instituto Nacional de Ciberseguridad. https://www.incibe.es/incibe/sala-de-prensa

International Organization for Standardization. (2023). *ISO/IEC 42001:2023: Artificial intelligence management system*. https://www.iso.org/standard/42001

LinkedIn. (s. f.). *LinkedIn Jobs España*. https://www.linkedin.com/jobs/

Microsoft. (2024). *Microsoft digital defense report 2024*. Microsoft Security Insider. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports

MITRE. (s. f.). *MITRE ATLAS: Adversarial threat landscape for artificial-intelligence systems*. https://atlas.mitre.org/

NATO Cooperative Cyber Defence Centre of Excellence. (s. f.). *Publications*. https://ccdcoe.org/library/publications/

NIS Cooperation Group & European Commission. (s. f.). *NIS Cooperation Group*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

National Institute of Standards and Technology. (s. f.). *AI risk management framework*. https://www.nist.gov/itl/ai-risk-management-framework

OWASP Foundation. (s. f.). *OWASP Top 10 for Large Language Model Applications / GenAI Security Project*. https://owasp.org/www-project-top-10-for-large-language-model-applications/

Palo Alto Networks Unit 42. (s. f.). *Unit 42 threat research*. Palo Alto Networks. https://unit42.paloaltonetworks.com/

PwC. (s. f.). *Global digital trust insights*. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html

Real Instituto Elcano. (s. f.). *Cybersecurity*. https://www.realinstitutoelcano.org/en/topic/cybersecurity/

Tecnoempleo. (s. f.). *Ofertas de empleo tecnológico*. https://www.tecnoempleo.com/

Universidad Carlos III de Madrid. (s. f.). *Máster universitario en ciberseguridad*. https://www.uc3m.es/master/ciberseguridad

Universidad Carlos III de Madrid. (s. f.). Máster universitario en inteligencia artificial aplicada. https://www.uc3m.es/master/inteligencia-artificial-aplicada

Universidad de Granada. (s. f.). Doctorado en tecnologías de la información y la comunicación. https://doctorados.ugr.es/tic/

Universidad de Málaga. (s. f.). Máster universitario en ciberseguridad. https://www.uma.es/master-en-ciberseguridad/

Universitat Oberta de Catalunya. (s. f.). Máster universitario en ciberseguridad y privacidad. https://www.uoc.edu/es/estudios/masters/master-universitario-ciberseguridad-privacidad

Universitat Politècnica de Catalunya. (s. f.). Grado en inteligencia artificial. https://www.upc.edu/es/grados/inteligencia-artificial-barcelona-fib

Universitat Politècnica de València. (s. f.). Máster universitario en inteligencia artificial. https://www.upv.es/estudios/master/muiarfid/

Unión Europea. (s. f.). Regulatory framework on artificial intelligence. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Velasquez (2026). Ciberseguridad Cognitiva: Cuando el ciberataque es dirigido a la mente. https://institutohispanoamericanorrii.com/ciberseguridad-cognitiva-cuando-el-ciberataque-es-dirigido-a-la-mente-2/.

Verizon. (2026). Data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/

World Economic Forum. (s. f.). Publications. https://www.weforum.org/publications/



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.