CIBERSEGURIDAD

INFORME DE SITUACIÓN 2025

DISRUPTIVE Plataforma Tecnológica Española de Tecnologías Disruptivas

Ayuda PTR2024-002903 financiada por: MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · AGENCIA ESTATAL DE INVESTIGACIÓN

Secretaria técnica a cargo de: APTE Asociación de Parques Científicos y Tecnológicos de España

ÍNDICE

INTRODUCCIÓN

En 2025, la ciberseguridad ha dejado de ser un asunto meramente tecnológico para convertirse en un pilar estratégico de la competitividad, la soberanía digital y la resiliencia nacional. España afronta un escenario en el que la superficie de ataque se expande exponencialmente debido a la hiperconectividad, la proliferación de dispositivos IoT, la adopción de la nube híbrida y la integración masiva de inteligencia artificial generativa en procesos críticos. En este contexto, el Gobierno ha dado un paso decisivo con la creación del Centro Nacional de Ciberseguridad, una infraestructura destinada a coordinar la respuesta ante incidentes, fortalecer la protección de infraestructuras críticas y consolidar la colaboración entre los sectores público y privado.

La magnitud de la amenaza es global. Según el Global Cybersecurity Outlook 2025 del Foro Económico Mundial, los ciberataques se han incrementado un 38 % en el último año, impulsados por el uso ofensivo de la IA, el ransomware como servicio (RaaS) y las campañas de desinformación digital. En España, el Instituto Nacional de Ciberseguridad (INCIBE) gestionó más de 97.000 incidentes durante 2024, muchos de ellos dirigidos contra servicios esenciales y organismos públicos, lo que evidencia una presión constante sobre la infraestructura digital del país.

El tejido empresarial se enfrenta a un desafío de gran calado: la profesionalización de la ciberdefensa corporativa. Los sectores financiero, industrial, sanitario y tecnológico concentran la mayor parte de los ataques, motivados por su valor estratégico y la sensibilidad de los datos que gestionan. Las compañías están respondiendo con un aumento significativo de la inversión: seis de cada diez empresas españolas planean destinar más recursos a soluciones de ciberseguridad basadas en inteligencia artificial durante 2025, con el fin de detectar patrones anómalos, automatizar la respuesta ante incidentes y reforzar la ciberresiliencia operativa. No obstante, la escasez de talento especializado continúa siendo una de las principales brechas estructurales. Dos de cada tres empresas europeas reconocen dificultades para cubrir vacantes en seguridad digital, lo que pone en riesgo la capacidad de anticipar, mitigar y contener ciberamenazas avanzadas. Esta falta de expertos coincide con la necesidad urgente de cumplir con la Directiva NIS2, que exige una gestión más rigurosa de los riesgos y la notificación obligatoria de incidentes a nivel europeo.

El sector público tampoco escapa a la exposición. Un estudio reveló que el 99 % de los ayuntamientos españoles incumple la Ley de Ciberseguridad, lo que deja al descubierto vulnerabilidades críticas en sistemas de administración electrónica y gestión ciudadana. Esta realidad ha impulsado la creación de centros regionales de operaciones de ciberseguridad, como el anunciado por la Comunidad de Madrid, orientados a reforzar la monitorización y la respuesta ante amenazas.

En paralelo, la ciberseguridad industrial y la protección de la cadena de suministro se han posicionado como áreas prioritarias, impulsadas por foros como el Barcelona Cybersecurity Congress 2025 o el Gipuzkoa IndustrySec. La integración de tecnologías como la computación cuántica y la criptografía post-cuántica comienza a vislumbrarse como un elemento diferenciador frente a los riesgos de próxima generación.

El presente informe analiza los principales desafíos y oportunidades de la ciberseguridad en España en 2025, explorando cómo la combinación de innovación tecnológica, políticas públicas, inversión privada y capacitación del talento determinará el grado de resiliencia digital del país ante un entorno cada vez más complejo, interconectado y vulnerable

Este informe pretende ser una foto del momento actual en el que se encuentra dicha tecnología en España y que sirva para poder comparar la situación en un futuro próximo.

TENDENCIAS

El panorama de la ciberseguridad en España en 2025 refleja una etapa de madurez tecnológica y elevada complejidad táctica, donde las amenazas evolucionan con una velocidad inédita y las defensas requieren adaptabilidad constante. La hiperconectividad, el uso de inteligencia artificial generativa, la digitalización de infraestructuras críticas y la presión regulatoria europea están redefiniendo las prioridades estratégicas tanto en el sector público como en el privado.

- **Inteligencia Artificial y automatización ofensiva**

La inteligencia artificial (IA) se ha convertido en el epicentro de la ciberseguridad contemporánea. Las organizaciones emplean sistemas basados en aprendizaje automático y análisis predictivo para detectar comportamientos anómalos, anticipar ataques y automatizar la respuesta ante incidentes. Sin embargo, los ciberdelincuentes también han integrado la IA en sus arsenales, utilizando algoritmos generativos para crear malware indetectable, falsificar identidades digitales y ejecutar campañas de phishing hiperpersonalizadas. Este escenario ha llevado a que más del 60 % de las empresas españolas incremente su inversión en soluciones de seguridad basadas en IA, en un intento por equilibrar el poder tecnológico en este nuevo terreno de juego.

- **Ransomware 2.0 y sofisticación del phishing**

El ransomware sigue siendo la amenaza más rentable del cibercrimen. En 2025, se impone el modelo de "doble o triple extorsión", en el que los atacantes no solo cifran los datos de sus víctimas, sino que los exfiltran y amenazan con filtrarlos públicamente. Paralelamente, las campañas de phishing han alcanzado un nivel de sofisticación sin precedentes gracias a la IA generativa: los mensajes fraudulentos imitan con precisión la comunicación corporativa, e incluso utilizan deepfakes de voz y vídeo para ganar credibilidad. Las pymes y las administraciones locales continúan siendo los objetivos más frecuentes, dada su menor madurez tecnológica y la escasez de protocolos de respuesta.

- **Brecha de talento y necesidad de ciberresiliencia**

La escasez de especialistas en ciberseguridad sigue siendo uno de los principales cuellos de botella del ecosistema digital español. Dos de cada tres empresas europeas reconocen dificultades para cubrir vacantes en seguridad, lo que limita la capacidad de prevención y contención de incidentes. En respuesta, entidades públicas, universidades y centros tecnológicos impulsan programas formativos y competiciones profesionales, como la selección española de ciberseguridad que participará en el ECSC 2025, con el objetivo de atraer talento joven y fomentar una cultura de ciberresiliencia sostenida.

- **Riesgos en infraestructuras críticas y despliegue del 5G**

La digitalización de los sistemas industriales y el despliegue de redes 5G han ampliado significativamente la superficie de ataque. La convergencia entre tecnologías operacionales (OT) y tecnologías de la información (IT) obliga a adoptar enfoques integrados de ciberseguridad industrial, donde un fallo en la red puede traducirse en consecuencias físicas. Eventos como el Barcelona Cybersecurity Congress 2025 o el Gipuzkoa IndustrySec subrayan la prioridad de proteger entornos industriales y cadenas de suministro ante ataques dirigidos y persistentes.

- **Seguridad de la cadena de suministro y dependencia de terceros**

Los ciberataques a proveedores y servicios en la nube se han convertido en un vector crítico de riesgo. La interdependencia entre empresas y plataformas externas ha impulsado la adopción de auditorías continuas, inventarios de software (SBOM) y protocolos de validación para minimizar vulnerabilidades. En 2025, la gestión del riesgo de terceros se consolida como un requisito esencial para garantizar la continuidad de negocio.

- **Cumplimiento normativo y gobernanza bajo NIS2**

La entrada en vigor de la Directiva NIS2 en Europa ha elevado los estándares de ciberseguridad, obligando a las organizaciones a mejorar su gobernanza interna, notificar incidentes con mayor transparencia y establecer mecanismos de evaluación de riesgos permanentes. En España, esta presión regulatoria ha impulsado el desarrollo de centros regionales de operaciones de ciberseguridad, como el de la Comunidad de Madrid, para reforzar la monitorización y la capacidad de respuesta de las administraciones públicas.

- **Ciberseguridad como ventaja competitiva**

Cada vez más empresas españolas perciben la ciberseguridad como un elemento diferencial en términos de confianza, reputación y sostenibilidad digital. El plan estatal de 1.157 millones de euros destinado a reforzar las capacidades nacionales en ciberseguridad y ciberdefensa impulsa la colaboración público-privada, el desarrollo de soluciones innovadoras y el crecimiento de startups especializadas. La seguridad deja de ser un coste y pasa a ser un activo estratégico que determina la credibilidad y la competitividad en el mercado digital.

Estas tendencias consolidan la visión de 2025 como un punto de inflexión: la ciberseguridad deja de ser una función reactiva para convertirse en un ecosistema inteligente, normativo y colaborativo, donde la anticipación, la automatización y la formación son las claves para fortalecer la resiliencia digital de España ante un entorno de amenazas en constante evolución.

ESTRATEGIA EN ESPAÑA

La estrategia nacional de ciberseguridad en 2025 refleja una evolución significativa hacia un modelo más coordinado, proactivo y con mayor respaldo institucional. España ha asumido que la ciberseguridad no solo es una cuestión técnica, sino un asunto de Estado y un pilar esencial para su soberanía digital, competitividad económica y seguridad ciudadana. El año ha estado marcado por el refuerzo del marco normativo, la creación de nuevas infraestructuras institucionales, la inversión histórica en capacidades de defensa digital y la consolidación de alianzas público-privadas.

- **Fortalecimiento del marco normativo y alineación europea**

El impulso regulatorio ha sido una de las bases de la estrategia española en 2025. La entrada en vigor de la Directiva NIS2 y del Reglamento de Cibersolidaridad Europeo ha llevado a España a adaptar su marco legal para reforzar la prevención, notificación y gestión de incidentes de seguridad. Las empresas de sectores esenciales —energía, transporte, sanidad, finanzas, tecnología y administraciones públicas— están ahora obligadas a disponer de planes de ciberresiliencia, auditorías periódicas y gobernanza directa desde la alta dirección.

El Esquema Nacional de Seguridad (ENS) ha sido actualizado para alinearse con las exigencias europeas y con los nuevos escenarios de riesgo, especialmente en entornos de nube, inteligencia artificial y 5G. Sin embargo, persisten desafíos estructurales: un informe reciente indica que el 99 % de los ayuntamientos españoles aún no cumple plenamente la Ley de Ciberseguridad, lo que ha impulsado la creación de mecanismos de apoyo técnico y financiero desde el Estado. A nivel de telecomunicaciones, la Ley de Ciberseguridad 5G mantiene un papel central, garantizando que los proveedores de infraestructura adopten medidas de seguridad reforzadas en entornos de conectividad avanzada. En paralelo, el Gobierno ha comenzado a trabajar en un Plan Nacional de Protección de la Cadena de Suministro Digital, inspirado en las recomendaciones de la ENISA y el Foro Económico Mundial, para controlar dependencias tecnológicas críticas.

- **Creación del Centro Nacional de Ciberseguridad y despliegue regional**

Uno de los hitos más destacados del año ha sido la creación del Centro Nacional de Ciberseguridad, anunciado oficialmente en enero de 2025. Este organismo, coordinado entre los ministerios competentes y el INCIBE, centraliza las operaciones de defensa, detección y respuesta ante incidentes graves, así como la cooperación con organismos internacionales y empresas estratégicas.

La nueva entidad se integra dentro de una arquitectura distribuida que incluye centros regionales de operaciones (SOC) en comunidades como Madrid, Cataluña y Andalucía. Estos centros actuarán como nodos de detección avanzada, análisis forense y formación especializada, conectados a la Red Nacional de SOC gestionada por el CCN-CERT. Este modelo descentralizado busca reforzar la capacidad de respuesta local y aumentar la coordinación entre administraciones y operadores críticos

- **Inversión pública y apoyo a la ciberindustria nacional**

El Gobierno ha aprobado en mayo un plan de inversión de 1.157 millones de euros para reforzar la ciberseguridad y la ciberdefensa nacional. Esta inversión histórica forma parte del esfuerzo por situar a España como líder europeo en capacidades digitales seguras, e incluye financiación para infraestructuras de vigilancia y análisis de amenazas, programas de concienciación y ayudas a la innovación empresarial. Una parte significativa de este presupuesto se destinará a impulsar el tejido empresarial español en ciberseguridad, mediante apoyo a startups y pymes del sector. Iniciativas como el Cybersecurity Ventures, organizado para fomentar el emprendimiento innovador en seguridad digital, y los fondos FEDER canalizados a través de las Cámaras de Comercio, están permitiendo que pequeñas empresas accedan a programas de auditoría y mejora de sus sistemas defensivos. Además, la estrategia fomenta la soberanía tecnológica y el talento nacional, promoviendo la cooperación entre universidades, parques tecnológicos y centros de innovación para desarrollar soluciones propias en ámbitos como la criptografía post-cuántica, la detección de amenazas mediante IA o la protección de sistemas OT/SCADA.

- **Colaboración público-privada e internacional**

La cooperación entre el INCIBE, el CCN-CERT y las principales empresas tecnológicas del país se ha reforzado para intercambiar inteligencia sobre amenazas y coordinar respuestas a ciberataques de gran escala. El modelo de colaboración público-privada se ha extendido a nuevos sectores, con especial énfasis en la ciberseguridad industrial, la protección del sector sanitario y la banca digital.

En el plano internacional, España ha intensificado su participación en la European Cybersecurity Competence Centre (ECCC) y en las redes de cooperación de la ENISA, alineando su estrategia con los objetivos europeos de autonomía estratégica y ciberdefensa compartida. A nivel bilateral, continúan los acuerdos con países del entorno europeo y latinoamericano para compartir experiencias, buenas prácticas y soluciones tecnológicas.

- **Desarrollo de talento y cultura de ciberresiliencia**

El déficit de talento especializado sigue siendo un reto estructural, por lo que la estrategia nacional ha redoblado sus esfuerzos en capacitación y sensibilización. El INCIBE, junto con universidades y clústeres tecnológicos, impulsa programas de formación avanzada y hackathones para captar y retener talento joven. Iniciativas como la Cátedra INCIBE-UPV de Ciberseguridad y los programas de certificación profesional contribuyen a generar una cantera de especialistas. Asimismo, el Gobierno está apostando por la concienciación ciudadana mediante campañas de educación digital que promueven la ciberhigiene, el uso seguro de la identidad digital y la protección frente a estafas online. En paralelo, programas como Activa Ciberseguridad continúan ofreciendo diagnóstico gratuito y asesoramiento a pymes, uno de los segmentos más expuestos a los ataques.

- **Protección de infraestructuras críticas y capacidades defensivas**

La protección de infraestructuras críticas constituye uno de los ejes estratégicos de la política nacional. La creciente interconexión de redes industriales, la digitalización de los servicios públicos y el auge de las tecnologías 5G han incrementado la vulnerabilidad de los sistemas. España ha fortalecido la cooperación entre los operadores críticos y las Fuerzas y Cuerpos de Seguridad del Estado, integrando inteligencia cibernética y medidas preventivas avanzadas. El CCN-CERT mantiene un papel central en la monitorización y respuesta ante ciberincidentes que afectan a la Administración. Su trabajo, junto con el Mando Conjunto del Ciberespacio (MCCE), garantiza una defensa coordinada entre los ámbitos civil y militar, en línea con las estrategias europeas de ciberdefensa.

- **Una estrategia hacia la resiliencia y la autonomía digital**

En conjunto, la estrategia española de ciberseguridad en 2025 muestra un avance claro hacia la resiliencia digital, la soberanía tecnológica y la cohesión territorial en materia de defensa digital. La creación del Centro Nacional de Ciberseguridad, la inversión pública sin precedentes, la integración de la IA en la vigilancia de amenazas y el fortalecimiento de las capacidades humanas e industriales sitúan a España en una posición de liderazgo regional.

Sin embargo, los retos persisten: la brecha de talento, el cumplimiento desigual entre administraciones locales y la rápida evolución de la amenaza cibernética obligan a mantener una estrategia dinámica, basada en la colaboración continua, la innovación y la anticipación.

RETOS Y OPORTUNIDADES

En 2025, España encara una etapa decisiva en su evolución hacia una sociedad y una economía digitales seguras. El avance de la conectividad 5G, la integración masiva de la inteligencia artificial, la dependencia tecnológica global y la irrupción de nuevas amenazas híbridas han configurado un panorama de riesgos interconectados. Frente a este entorno dinámico, el país se enfrenta a desafíos estructurales que exigen una respuesta coordinada y sostenida, pero también a oportunidades únicas para reforzar su liderazgo en ciberseguridad y soberanía digital.

Retos:

Expansión de la superficie de ataque y sofisticación de las amenazas

El despliegue de la red 5G y la creciente digitalización de los sistemas industriales han incrementado la superficie de ataque de manera exponencial. Cada nuevo dispositivo conectado —desde sensores IoT en entornos industriales hasta aplicaciones en la nube— se convierte en un potencial punto de entrada. Los ataques actuales combinan técnicas de ransomware, phishing avanzado, deepfakes y manipulación algorítmica mediante inteligencia artificial generativa. El auge del ransomware como servicio (RaaS) y la profesionalización del cibercrimen están poniendo a prueba la capacidad defensiva de empresas, administraciones y ciudadanos. La ciberseguridad industrial y la protección de entornos OT/SCADA se presentan como ámbitos críticos. Los incidentes en estos sistemas no solo comprometen datos, sino que pueden tener consecuencias físicas, económicas y medioambientales, especialmente en sectores como la energía, el transporte o la sanidad.

Brecha de talento y capacidades técnicas

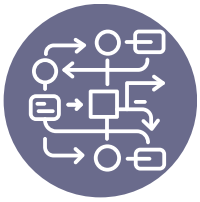
La escasez de profesionales especializados sigue siendo uno de los principales obstáculos del ecosistema nacional. Dos de cada tres empresas europeas afirman tener dificultades para cubrir vacantes en seguridad digital, una cifra que se replica en España y que afecta con especial intensidad a las pymes y administraciones locales. Esta carencia limita la capacidad de anticipación, análisis forense y respuesta ante incidentes. Aunque el INCIBE, las universidades y las empresas tecnológicas están impulsando programas de formación y certificación, la velocidad de desarrollo tecnológico supera la del talento disponible. Reducir esta brecha es esencial para sostener el crecimiento del sector y garantizar la resiliencia digital del país.

Vulnerabilidad de las pymes y administraciones locales

Las pymes continúan siendo el eslabón más débil del ecosistema. Muchas operan sin departamentos de seguridad o estrategias de protección estructuradas, lo que las convierte en objetivos prioritarios para los ciberdelincuentes. Las campañas de fraude, ransomware y robo de identidad digital afectan a la continuidad de sus operaciones y, en muchos casos, conducen al cierre empresarial. A este problema se suma el déficit estructural de ciberseguridad en la administración local. Según datos de 2025, el 99 % de los ayuntamientos españoles aún incumple la Ley de Ciberseguridad, lo que revela la necesidad urgente de apoyo técnico, financiero y de formación especializada

Cumplimiento normativo y presión regulatoria

LLa implementación de la Directiva NIS2, junto con las exigencias del Reglamento de Cibersolidaridad Europeo y la adaptación del Esquema Nacional de Seguridad, ha elevado el nivel de exigencia para las organizaciones. Si bien estas normativas fortalecen la ciberresiliencia, su cumplimiento representa un reto para muchas empresas —especialmente las pymes— que carecen de recursos para auditar, actualizar y certificar sus infraestructuras. Además, la trazabilidad y la gobernanza del dato se han convertido en requisitos imprescindibles para las empresas que manejan información sensible, en un contexto donde la protección de la identidad digital y el cumplimiento del RGPD son más complejos que nunca.



Riesgo de dependencia tecnológica y seguridad en la cadena de suministro

La interdependencia entre proveedores, plataformas en la nube y servicios tecnológicos externos incrementa el riesgo sistémico. Un fallo o brecha en un proveedor puede propagarse en cascada por toda la cadena. El país aún enfrenta el desafío de garantizar la soberanía tecnológica, promoviendo el desarrollo de soluciones nacionales y la certificación de terceros mediante modelos de transparencia como el Software Bill of Materials (SBOM).

Amenazas híbridas y dimensión geopolítica

Los conflictos internacionales, la desinformación y los ciberataques patrocinados por Estados han convertido la ciberseguridad en un asunto de defensa nacional. La frontera entre ciberdelito y ciberespionaje se diluye, y las infraestructuras críticas —energía, agua, salud o transporte— se han convertido en objetivos estratégicos. España, en colaboración con la UE y la OTAN, trabaja en reforzar su capacidad de respuesta ante ataques híbridos que combinan sabotaje digital, manipulación informativa y guerra económica.

Oportunidades:

Inversión pública y liderazgo institucional

La aprobación de un plan de inversión de 1.157 millones de euros marca un punto de inflexión en la política nacional de ciberseguridad. Este presupuesto refuerza la protección de infraestructuras críticas, la modernización de los centros de operaciones de seguridad (SOC) y el impulso de la investigación y el desarrollo tecnológico. La creación del Centro Nacional de Ciberseguridad y los SOC regionales consolida una arquitectura de defensa distribuida que mejora la detección, coordinación y respuesta ante incidentes en todo el territorio.

Fortalecimiento de la colaboración público-privada

El ecosistema español avanza hacia un modelo de cooperación más ágil entre administraciones, empresas y universidades. El INCIBE, el CCN-CERT, las comunidades autónomas y el tejido empresarial están trabajando conjuntamente en proyectos de innovación, intercambio de inteligencia sobre amenazas y protocolos de actuación coordinada. Este enfoque colaborativo ha permitido mejorar la ciberdefensa en sectores estratégicos como el sanitario, financiero e industrial, donde la protección de datos y servicios es crítica.

Innovación tecnológica y adopción de IA defensiva

La aplicación de la inteligencia artificial y el análisis predictivo en la ciberseguridad ofrece una ventaja sin precedentes. Las empresas están utilizando algoritmos de aprendizaje automático para identificar patrones anómalos, prevenir intrusiones y automatizar la respuesta ante incidentes. Al mismo tiempo, la IA contribuye a optimizar la gestión de recursos y priorizar las amenazas más críticas. España se posiciona así como un entorno favorable para el desarrollo de startups y soluciones de cyber defense basadas en inteligencia artificial.

Desarrollo del talento y empleabilidad

La escasez de profesionales se transforma también en una oportunidad para impulsar nuevas carreras, programas formativos y certificaciones. Iniciativas como la Cátedra INCIBE-UPV, los programas de capacitación en parques tecnológicos y las competiciones nacionales de ciberseguridad fomentan la vocación técnica y la especialización de jóvenes profesionales. Además, la alta demanda laboral en este sector está atrayendo inversión y consolidando una comunidad profesional altamente cualificada.

Crecimiento del mercado nacional de ciberseguridad

El mercado español de soluciones y servicios de ciberseguridad atraviesa un momento de expansión. Grandes corporaciones y nuevas empresas emergentes están desarrollando tecnologías en ámbitos como el cifrado post-cuántico, la ciberseguridad industrial, la detección de amenazas en tiempo real o la protección de identidades digitales. Esta dinámica impulsa la creación de un ecosistema de innovación con potencial de exportación y posiciona a España como un referente europeo en seguridad digital.

Cultura ciudadana y resiliencia social

La ciberseguridad comienza a percibirse como una responsabilidad compartida. El aumento de campañas de concienciación ciudadana y la incorporación de la ciberhigiene en la educación digital están reduciendo progresivamente la exposición de los usuarios a fraudes y estafas en línea. Los programas de diagnóstico gratuito para pymes y la labor pedagógica del INCIBE y otros organismos contribuyen a crear una cultura de seguridad más sólida y sostenible.

En conjunto, 2025 representa un año de madurez estratégica y transformación estructural en el ámbito de la ciberseguridad en España. Aunque los retos son profundos —desde la escasez de talento hasta la presión regulatoria y la complejidad tecnológica—, las oportunidades de crecimiento, innovación y cooperación sitúan al país en una posición ventajosa para consolidarse como un referente europeo en ciberresiliencia y soberanía digital.

ECOSISTEMA

En 2025, España consolida un ecosistema de ciberseguridad robusto, articulado en torno a un modelo de colaboración público-privada, una inversión pública sin precedentes y un tejido empresarial que combina grandes corporaciones, startups tecnológicas y pymes altamente especializadas. Este ecosistema, cada vez más interconectado y maduro, refleja la apuesta del país por reforzar su soberanía digital, aumentar su resiliencia ante las amenazas globales y liderar la innovación en tecnologías de protección digital.

La creación del Centro Nacional de Ciberseguridad, los nuevos centros regionales de operaciones (SOC) y el plan de inversión de 1.157 millones de euros aprobado por el Gobierno han actuado como catalizadores para el desarrollo del sector. A ello se suma el impulso del INCIBE, que refuerza su papel como motor de dinamización del ecosistema mediante programas de aceleración, apoyo a startups y colaboración con universidades y centros tecnológicos.

Principales Actores Empresariales

1. Telefónica Tech

Telefónica Tech continúa siendo uno de los pilares del ecosistema nacional e internacional de ciberseguridad. En 2025 ha reforzado su división de ciberinteligencia predictiva e IA generativa aplicada a la detección de amenazas, integrando algoritmos de análisis de comportamiento y respuesta automática ante incidentes. Su participación en la protección de redes 5G, servicios en la nube y sistemas IoT industriales consolida su papel estratégico en la defensa de sectores críticos como las telecomunicaciones, las finanzas y la sanidad.

2. BBVA Next Technologies

El brazo tecnológico del BBVA ha escalado posiciones dentro del ecosistema español gracias a su enfoque en seguridad de datos, identidad digital y antifraude en tiempo real. En 2025, BBVA Next Tech ha lanzado nuevas soluciones basadas en machine learning para la detección de comportamientos anómalos en operaciones financieras y sistemas de pago. Su modelo interno de "seguridad por diseño" se ha convertido en una referencia para el sector bancario y *fintech* en Europa.

3. ACCENTURE Security

Accenture ha ampliado su presencia en España con un hub de ciberseguridad en Málaga, especializado en servicios de respuesta ante incidentes (IR), threat hunting y simulaciones de ataques avanzados para grandes corporaciones. Desde este centro se coordinan proyectos de defensa digital en sectores energéticos, industriales y de infraestructuras críticas, impulsando la colaboración con administraciones públicas y universidades andaluzas.

4. TrC (Tecnologías de la Red y Comunicaciones)

La compañía gallega TrC ha irrumpido en el ecosistema nacional con fuerza tras su participación en programas de defensa y ciberseguridad vinculados al Ministerio de Defensa y al Mando Conjunto del Ciberespacio. En 2025, TrC ha desarrollado soluciones avanzadas de detección de intrusiones en entornos OT y defensa digital perimetral, posicionándose como un referente en la seguridad aplicada al sector de defensa y comunicaciones críticas.

5. SecureIT

SecureIT, consultora española en pleno crecimiento, se ha consolidado como uno de los principales proveedores de servicios de ciberseguridad gestionada (MSSP) y auditorías ENS/NIS2. En 2025 ha liderado el debate sobre la gobernanza del riesgo tecnológico, organizando encuentros empresariales para analizar las oportunidades del mercado y promover la ciberresiliencia como activo competitivo.

6. OneCyber / Telefónica & ElevenPaths

Dentro del grupo Telefónica, la evolución de ElevenPaths hacia OneCyber ha dado lugar a una nueva estructura orientada a la gestión integral de ciberamenazas, con servicios específicos para organismos públicos y pymes. En 2025, la compañía ha lanzado soluciones modulares que integran IA, threat intelligence y zero trust architectures, alineadas con los estándares europeos de ciberseguridad.

Startups y pymes innovadoras

El panorama emprendedor en ciberseguridad española ha alcanzado un punto álgido en 2025. El crecimiento de programas de apoyo como Cybersecurity Ventures (INCIBE), FEDER Ciberseguridad Pymes, o la alianza Startup Valencia–Cátedra INCIBE-UPV, ha permitido que un número creciente de startups desarrollen soluciones disruptivas en inteligencia de amenazas, identidad digital, seguridad en la nube y ciberdefensa industrial.

- **Redborder**, con sede en Salamanca, se ha posicionado como una de las principales plataformas de análisis y visualización de ciberamenazas en tiempo real, adoptada por empresas y administraciones. Su tecnología basada en *big data* e IA permite correlacionar millones de eventos por segundo para identificar patrones anómalos.
- **Ciberseg**, nacida en 2023 en el ecosistema andaluz, ha ganado protagonismo en 2025 con soluciones de auditoría automatizada y cumplimiento ENS/NIS2 para pymes y administraciones locales.
- **BeDisruptive**, con oficinas en Madrid, Roma y Dubái, se consolida como un actor relevante en ciberdefensa ofensiva, *ethical hacking* y simulación de ataques, colaborando con instituciones europeas y empresas energéticas.
- **AIUKEN Cybersecurity**, con centros en España y América Latina, ha crecido en el mercado de servicios SOC multicliente y protección de infraestructuras críticas, destacando por su integración de IA y aprendizaje federado para la detección avanzada de amenazas.
- **Realsec**, especializada en criptografía post-cuántica y protección de transacciones financieras, colabora con entidades bancarias españolas y latinoamericanas para el desarrollo de soluciones seguras ante la inminente transición hacia la computación cuántica.
- **Tarlogic Security**, con sede en Galicia, mantiene su liderazgo en ciberinteligencia, análisis forense y consultoría técnica, con un crecimiento sostenido en proyectos europeos de ciberdefensa industrial.

El impulso de eventos como el Gipuzkoa IndustrySec 2025, el Barcelona Cybersecurity Congress, o el Congreso del LISA Institute 2025, centrado en inteligencia, ciberseguridad y prospectiva estratégica, ha fortalecido la conexión entre el talento emprendedor, la investigación y la inversión. Estas citas se consolidan como puntos de encuentro internacionales donde España proyecta su capacidad tecnológica y su liderazgo regional en innovación en ciberseguridad.

Colaboración institucional y público-privada

El éxito del ecosistema español descansa sobre una estructura institucional sólida y coordinada. El INCIBE, el CCN-CERT y los centros regionales de operaciones de ciberseguridad son los principales ejes de esta red colaborativa.

- El INCIBE, con sede en León, ha reforzado su estrategia de apoyo a pymes y startups, ofreciendo programas de asesoramiento, auditoría y aceleración de proyectos innovadores. En 2025 también ha ampliado su presencia internacional con iniciativas conjuntas con CEIN y organismos europeos.

- El CCN-CERT, dependiente del Centro Criptológico Nacional, mantiene su papel de coordinación nacional en defensa de las infraestructuras públicas. Su integración con la Red Nacional de SOC permite una respuesta más rápida y coordinada frente a ciberincidentes de gran magnitud.

- Las comunidades autónomas, especialmente Madrid, Cataluña, Andalucía y País Vasco, han desarrollado sus propios centros regionales de ciberseguridad, enfocados en la formación avanzada, el análisis forense y la protección de infraestructuras críticas.

Innovación, I+D y cooperación internacional

España es hoy un nodo europeo de referencia en innovación en ciberseguridad. Su participación en programas como el European Cybersecurity Competence Centre (ECCC) y el Digital Europe Programme ha permitido la financiación de proyectos de vanguardia en criptografía post-cuántica, automatización de defensa y ciberseguridad industrial. Además, la colaboración con universidades y parques científicos —como el Barcelona Supercomputing Center, el Málaga TechPark, el Parc Científic de la UPV y el Asturias Digital Innovation Hub— ha fomentado la creación de laboratorios de simulación, bancos de pruebas (cyber ranges) y programas de formación dual. La creciente participación española en misiones internacionales, proyectos transfronterizos y redes de innovación tecnológica refuerza el papel del país como exportador de conocimiento y soluciones en ciberseguridad, no solo en el entorno europeo, sino también en América Latina, el norte de África y Oriente Medio.

Un ecosistema consolidado y en expansión

El ecosistema de ciberseguridad en España en 2025 se distingue por su madurez, diversidad e integración internacional. Grandes corporaciones, startups, administraciones públicas y centros de investigación conforman un entramado resiliente que combina innovación, talento y cooperación estratégica.

España no solo ha reforzado su posición como referente europeo en seguridad digital, sino que avanza hacia un modelo sostenible, donde la ciberseguridad se consolida como motor económico, tecnológico y social, capaz de anticipar amenazas, generar empleo cualificado y proyectar la influencia tecnológica del país más allá de sus fronteras.

PROSPECTIVA

El futuro inmediato de la ciberseguridad en España se configura en un entorno caracterizado por la interconexión total, la automatización inteligente y la irrupción de nuevas tecnologías disruptivas que reconfiguran tanto las oportunidades como las amenazas. En 2025, los riesgos digitales se han consolidado como una de las principales preocupaciones globales, no solo por su impacto económico, sino por su capacidad para alterar el equilibrio geopolítico y erosionar la confianza en las instituciones. La seguridad digital ya no es un asunto técnico limitado a los departamentos de TI: es un componente esencial de la estabilidad nacional y de la soberanía tecnológica de los países.

España se encuentra en un momento decisivo. La digitalización masiva de sus sectores estratégicos —energía, finanzas, salud, transporte, defensa o administración pública— ha incrementado la superficie de exposición y exige una estrategia de defensa adaptativa capaz de anticipar los ataques antes de que se materialicen. Los ciberataques automatizados, impulsados por inteligencia artificial generativa, están redefiniendo la naturaleza de la amenaza: ya no se trata de simples vulnerabilidades explotadas por actores individuales, sino de operaciones automatizadas que combinan ingeniería social, manipulación algorítmica y ataques a la integridad de los datos. Las técnicas de prompt injection y data poisoning están siendo empleadas para alterar los modelos de lenguaje y sistemas de decisión basados en IA, comprometiendo su fiabilidad y exponiendo datos sensibles de instituciones y empresas.

Esta nueva realidad está impulsando el surgimiento de un campo cada vez más relevante: la seguridad algorítmica. En España, tanto el Instituto Nacional de Ciberseguridad (INCIBE) como el Centro Criptológico Nacional (CCN) trabajan junto a universidades y empresas en el desarrollo de estándares de auditoría de inteligencia artificial y mecanismos de certificación que garanticen la trazabilidad y seguridad de los modelos generativos. La regulación europea, liderada por el *AI Act* y complementada por la Directiva NIS2, servirá como eje de coordinación para que los Estados miembros adopten marcos comunes de defensa digital y gobernanza algorítmica.

A la vez, la llegada de la computación cuántica plantea un desafío sin precedentes. La posibilidad de que los ordenadores cuánticos rompan los sistemas criptográficos tradicionales acelera la transición hacia la criptografía post-cuántica (PQC). España ya participa activamente en proyectos europeos de investigación para desarrollar nuevos algoritmos resistentes a este tipo de ataques, con la colaboración de empresas como Realsec o GMV y el liderazgo del CCN. Paralelamente, la adopción de tecnologías que preservan la privacidad, como la criptografía homomórfica, la computación multipartita segura o el *federated learning*, permite entrenar modelos de inteligencia artificial sin necesidad de exponer los datos de los usuarios, una tendencia que empieza a consolidarse especialmente en sectores como la sanidad o la energía.

El principio de *Secure by Design*, o seguridad desde el diseño, se impone como una filosofía transversal en la construcción de infraestructuras digitales, vehículos conectados, dispositivos médicos o sistemas industriales automatizados. España avanza en esta dirección a través de auditorías preventivas y entornos de simulación que permiten evaluar la resistencia de los sistemas antes de su despliegue real. La ciberresiliencia industrial se perfila así como uno de los pilares estratégicos de la próxima década, impulsando el tránsito desde una seguridad reactiva hacia un modelo predictivo y autosuficiente.

El papel de la inteligencia artificial en la defensa cibernética también está experimentando una profunda transformación. Los sistemas de orquestación y respuesta automatizada, conocidos como SOAR, combinados con algoritmos de aprendizaje profundo, permiten correlacionar millones de eventos por segundo y ejecutar contramedidas en tiempo real. España lidera varios proyectos piloto en esta línea, integrando capacidades de IA generativa en los Centros de Operaciones de Seguridad (SOC) regionales y nacionales para anticipar comportamientos maliciosos y mitigar su

impacto. Del mismo modo, el uso de gemelos digitales de ciberdefensa —entornos virtuales que replican infraestructuras críticas— permite simular ataques complejos y entrenar a los equipos de respuesta, reduciendo los tiempos de detección y contención.
A nivel normativo, 2025 marca un punto de inflexión con la entrada en vigor del Reglamento de Cibersolidaridad y la plena aplicación de la Directiva NIS2, que establecen obligaciones más estrictas de reporte, trazabilidad y gestión del riesgo para todos los operadores de servicios esenciales. España, alineada con el nuevo marco de la Unión Europea, refuerza su cooperación con la ENISA y la OTAN, posicionándose como un referente en la implementación de estrategias nacionales de ciberresiliencia civil y militar. La soberanía tecnológica se convierte en un eje vertebrador de esta nueva etapa: el país apuesta por reducir su dependencia de proveedores externos, desarrollar software certificado europeo y fomentar tecnologías seguras fabricadas en territorio nacional, con el objetivo de alcanzar una autonomía estratégica digital plena.

El factor humano sigue siendo una de las claves más determinantes en este escenario. La brecha de talento especializado en ciberseguridad, aunque todavía considerable, está comenzando a estrecharse gracias al impulso del Plan Nacional de Competencias Digitales, las cátedras universitarias del INCIBE y los programas de formación en parques tecnológicos. El nuevo paradigma de capacitación no se limita a formar técnicos, sino que busca crear una cultura transversal de ciberseguridad, extendida a pymes, administraciones y ciudadanos. En un entorno donde las amenazas se automatizan, la conciencia y la responsabilidad humana continúan siendo la primera línea de defensa.

De cara a los próximos años, el futuro de la ciberseguridad en España se orienta hacia la convergencia de tecnologías disruptivas que actuarán de forma coordinada: la inteligencia artificial defensiva, la criptografía post-cuántica, el edge computing y la automatización total de la respuesta cibernética. Estas herramientas permitirán construir un modelo de seguridad predictivo, autosostenible y resiliente, donde las infraestructuras sean capaces de aprender y defenderse de manera autónoma. La cooperación internacional, el intercambio de inteligencia y la formación continua se consolidarán como los pilares fundamentales para afrontar un escenario en el que la seguridad digital será sinónimo de estabilidad, competitividad y soberanía tecnológica.
España, con un ecosistema cada vez más maduro y un liderazgo creciente en el ámbito europeo, avanza hacia una ciberseguridad autónoma, sostenible y estratégica, capaz de anticipar las amenazas antes de que estas se materialicen y de proteger los valores fundamentales de una sociedad digital interconectada.

CASOS DE USO

El 2025 ha marcado un año crucial para el avance de la Ciberseguridad en España, con nuevos desarrollos tecnológicos y normativos que buscan integrar a todas las personas en la era digital.

SOC-as-a-Service para PYMES y administraciones públicas

Protagonistas: BeDisruptive, CounterCraft, Enigmedia, GoCyber
Sectores implicados: PYMES multisectoriales y ayuntamientos

El déficit de especialistas ha impulsado la externalización de centros de operaciones de seguridad basados en inteligencia artificial y sistemas SOAR. Este modelo facilita que empresas sin recursos internos cuenten con monitorización 24/7, detección avanzada y respuesta rápida ante incidentes. Programas con financiación pública están permitiendo su adopción en administraciones locales, mejorando la protección de servicios públicos esenciales.

Gemelos digitales para la protección OT

Protagonistas: Keytron, Cybentia
Sectores implicados: energía, transporte e industria 4.0
La simulación de ciberataques en entornos virtuales idénticos a las instalaciones reales permite analizar la resiliencia industrial sin poner en riesgo la producción. Estas soluciones, apoyadas por modelos de deep learning, ofrecen un marco predictivo capaz de anticipar vulnerabilidades en sistemas de control y reducir tiempos de respuesta frente a incidentes en redes OT. El uso de esta tecnología se está extendiendo en operadores energéticos y de transporte.

Seguridad cuántica en la cadena de suministro tecnológico y financiero

Protagonistas: Realsec + CCN + EuroQCI
Sectores implicados: banca, proveedores TIC, operadores críticos
Con el objetivo de preparar al país frente a amenazas de descifrado cuántico, España está desplegando pruebas piloto de criptografía post-cuántica y distribución cuántica de claves (QKD) para la protección de comunicaciones y transacciones de alta sensibilidad. Esta iniciativa sitúa a España entre los países más avanzados en el marco europeo de infraestructuras cuánticas seguras.

Formación inmersiva para gestión de cibercrisis

Protagonistas: INCIBE + Tarlogic Research + Ackcent Cybersecurity
Sectores implicados: infraestructuras críticas, banca, sector público
Los simuladores de crisis digitales y plataformas de realidad virtual están transformando la capacitación en ciberseguridad. Estos entornos reproducen ataques complejos en tiempo real, fortalecen la coordinación entre equipos y aceleran la toma de decisiones en incidentes de gran impacto. Este enfoque contribuye a reducir la brecha de talento al fomentar un entrenamiento más práctico y efectivo.

Inteligencia de amenazas para anticipar ataques

Protagonistas: Blueliv (Outpost24)
Sectores implicados: banca, telecomunicaciones, administraciones públicas
La evolución hacia modelos de defensa proactiva se refleja en sistemas de análisis continuo de indicadores de compromiso en la dark web y otras fuentes. Las organizaciones pueden detectar filtraciones y planificaciones de campañas de ransomware antes de que se materialicen, reforzando así sus capacidades preventivas y su visibilidad sobre el ecosistema criminal.

ENLACES DE INTERÉS

Aquí os remitimos a enlaces de noticias, webs, documentos normativos o informes de interés, así como a bibliografía sobre este ámbito.

El Gobierno presenta la futura Ley de Coordinación y Gobernanza de la Ciberseguridad

Cybersecurity Predictions for 2025: Challenges and Opportunities

España refuerza su ciberseguridad con la creación del Centro Nacional de Ciberseguridad

Global Cybersecurity Outlook 2025

Málaga acogerá el IV Congreso de Ciberseguridad de Andalucía el 2 y 3 de abril

Expertos en ciberseguridad o analistas de riesgos, algunas de las profesiones que necesita el mercado laboral español

Computación cuántica y ciberseguridad: tendencias clave en 2025

Ciberseguridad: reflexiones y estrategias para un futuro seguro

INCIBE presenta su balance de ciberseguridad 2024 con más de 97 000 incidentes gestionados

Ciberseguridad en 2025: tendencias, amenazas y desafíos

Ciberseguridad: un reto estratégico ineludible para startups y emprendedores

Las 10 empresas referentes en ciberseguridad en España

Las 30 mujeres referentes en Ciberseguridad en España

Pulso legal a la ciberseguridad en 2025: novedades y desafíos

Siete tendencias clave que definen el mercado de la ciberseguridad actual

El estado de la ciberseguridad en España 2025

El 99% de los ayuntamientos españoles incumplen la ley de ciberseguridad

Qué es la directiva NIS2, cómo afecta y sanciones que conlleva

Las pymes impulsan el empleo mientras lidian con retos de ciberseguridad

Barcelona Cybersecurity Congress 2025 impulsará la ciberseguridad industrial

La inversión en ciberseguridad es clave para librar las guerras del siglo XXI

Darias conoce los últimos avances de ciberseguridad que promueve el Ministerio para la Transformación Digital

Ciberseguridad y geopolítica: los retos de los CIO en tiempos de hackers

La ciberseguridad como necesidad estratégica

Secure&IT analiza las tendencias alrededor del mundo de la ciberseguridad

El Gobierno aprueba destinar 1.157 millones de euros para reforzar la ciberseguridad

La Cátedra de Ciberseguridad INCIBE-UPV junto a Startup Valencia apuesta por el talento joven para un futuro digital más seguro

Principales tendencias en torno a la ciberseguridad en 2025, a debate

El mapa interactivo de estrategias nacionales de ciberseguridad de ENISA se actualiza para mostrar los avances en Europa en este ámbito

Las promesas incumplidas del Gobierno de España en materia de ciberseguridad e innovación

¿Puede la ciberseguridad ser una amenaza en sí misma?

Tendencias de ciberseguridad

Principales tendencias en torno a la ciberseguridad en 2025, a debate

Tendencias en ciberseguridad y ciberriesgo en España

Próximo foro sobre la importancia de la ciberseguridad en la estrategia empresarial

En 2025, adopción empresarial masiva de la ciberseguridad

5º edición de Gipuzkoa IndustrySec 2025

Ejecución de oportunidades en ciberseguridad y protección tecnológica en la estrategia empresarial

La ciberseguridad en las empresas, a debate en el próximo encuentro de Ejecución de Oportunidades

TRC emerge en el ecosistema de defensa y ciberseguridad español en plena fase de rearme

Cybersecurity Ventures se celebra para impulsar la ciberseguridad

Congreso LISA Institute 2025: innovación en inteligencia, ciberseguridad y prospectiva estratégica

España impulsa la innovación en defensa con startups tecnológicas en IA, ciberseguridad y aeroespacial

Las 10 empresas de ciberseguridad más potentes en la actualidad

Cómo los principales fabricantes impulsan la resiliencia cibernética

Fondos FEDER financian ayudas de ciberseguridad para pymes a través de las Cámaras de Comercio

CEIN e INCIBE buscan 20 proyectos para mejorar su ciberseguridad

Las debilidades que condicionan la ciberseguridad y la soberanía digital de Europa

Los ciberataques se disparan en 2025 y revelan la falta de expertos en ciberseguridad

INCIBE presenta a la selección española de ciberseguridad que competirá en los ECSC 2025 en Polonia

Los retos de la IA y la ciberseguridad en Sevilla Es Feria, que se traslada por primera vez a FIBES

La Comunidad de Madrid creará un Centro Regional de Operaciones de Ciberseguridad para reforzar la protección de los sistemas críticos de la Administración

Replantearse la ciberseguridad: cómo pueden protegerse realmente las empresas en 2025

Factura electrónica, IA y ciberseguridad: las claves de la cuarta edición de Accountex España 2025

Dos de cada tres empresas en Europa tienen problemas para cubrir sus vacantes en ciberseguridad

Estado de la Ciberseguridad 2025

Qué tendencias y amenazas de ciberseguridad han marcado el primer semestre de 2025

Tendencias tecnológicas 2025

©

Informe realizado por la **Asociación de Parques Científicos y Tecnológicos de España (APTE),** entidad que gestiona la secretaría técnica de la **Plataforma Tecnológica Española de Tecnologías Disruptivas (DISRUPTIVE)** con la colaboración de su **grupo de trabajo de Ciberseguridad** durante durante el último trimestre de 2025

DISRUPTIVE Plataforma Tecnológica Española de Tecnologías Disruptivas

Ayuda PTR2024-002903 financiada por: MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · AGENCIA ESTATAL DE INVESTIGACIÓN

Secretaria técnica a cargo de: APTE Asociación de Parques Científicos y Tecnológicos de España