ESPAÑA,
HUB DE CIBERSEGURIDAD EUROPEO

OPORTUNIDADES Y PROPUESTAS

2025

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

NIPO (edición on-line): 143-24-072-0
Fecha de edición: marzo 2025

ESPAÑA,
HUB DE CIBERSEGURIDAD EUROPEO

OPORTUNIDADES Y PROPUESTAS

Los expertos participantes en los Grupos de Trabajo lo son a título personal y no a título institucional. Por lo tanto, sus opiniones y recomendaciones no representan ni comprometen a las instituciones a las que pertenecen. El resultado de los trabajos es producto de un ejercicio de reflexión colectivo, si bien, no tiene por qué representar la opinión individual de todos los participantes, quienes no necesariamente comparten todas las conclusiones o propuestas.

EL FORO NACIONAL DE CIBERSEGURIDAD

MOTOR DE LA COLABORACIÓN PÚBLICO-PRIVADA

La Estrategia Nacional de Ciberseguridad, aprobada por el Consejo de Seguridad Nacional en abril de 2019, considera la colaboración público-privada como un elemento clave para impulsar la seguridad y confiabilidad del ciberespacio.

La propia Estrategia establece específicamente que dicha colaboración se articule a través del Foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la comunidad académica, asociaciones, organismos sin ánimo de lucro, entre otros, con el fin de para potenciar y crear sinergias público-privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

El Foro Nacional de Ciberseguridad se constituye oficialmente en julio del año 2020, siguiendo el mandato de su creación acordado en el Consejo Nacional de Ciberseguridad.

La composición del Foro responde a la pretensión de contar con la mayor representatividad posible de organismos públicos y de la sociedad civil en el ámbito de la ciberseguridad.

Bajo la presidencia del Departamento de Seguridad Nacional y las vicepresidencias del Instituto Nacional de Ciberseguridad (INCIBE) y del Centro Criptológico Nacional (CCN), el Foro está constituido por 18 organizaciones representantes de la sociedad civil, además de otros organismos con competencia en ciberseguridad.

El documento "España, Hub de Ciberseguridad Europeo" elaborado por el Foro Nacional de Ciberseguridad, responde a la línea de acción 7 de la Estrategia Nacional de Ciberseguridad: desarrollar una cultura de ciberseguridad.

AGRADECIMIENTOS

Coordinador institucional:

Departamento de Seguridad Nacional

Coordinador sociedad civil:

Gianluca D´Antonio. ISMS Forum

Autores y colaboradores:

Instituto Nacional de Ciberseguridad (INCIBE)
Centro Criptológico Nacional (CCN)
Adolfo Albaladejo
Luis Miguel Aldeguer Bolarín
Juan Ramón Aramendia Muneta
Mariano J. Benito Gómez
Miguel de la Cal Bravo
Juan Francisco Cornago Baratech *
Juan García Galera
Javier A. Gil-Ruiz Gil-Esparza
Tomás Gómez Pérez
Mabel González Centenera
Gustavo Herva Iglesias
Daniel Largacha Lamela
Diego Martínez
José Manuel Navarro Meseguer
Julia Perea Velasco *
José Manuel Pérez Pérez
Enrique Rando González
Lola Rebollo Revesado
Carlos Alberto Sáiz Peña
Jesús Sánchez López
Tomás Serna Navarro
Guillermo Unamuno Enciondo

*Coordinadores de los subgrupos de trabajo

ÍNDICE

RESUMEN EJECUTIVO

1. RESUMEN EJECUTIVO

Como ha indicado recientemente McKinsey&Company, España contaría con múltiples elementos para convertirse en un *hub* de ciberseguridad en Europa. Además de las conexiones económicas, culturales e históricas con América Latina, sus ventajas pueden transformar a España en una potencia líder en ciberseguridad, no solo para controlar los ciberataques que se producen en la región, sino también para ser un centro preeminente donde el talento cualificado prospere, la tecnología avance y las empresas sean más productivas y rentables.

El objetivo principal de "España, *hub* de ciberseguridad europeo" es generar conciencia sobre las posibles oportunidades existentes para impulsar nuestras fortalezas como país y favorecer las condiciones para colocar a España en una mejor posición, respecto al resto de Europa, en la provisión de servicios de ciberseguridad. Cabe señalar que en este trabajo se han tenido en cuenta distintas iniciativas ya existentes[1], con el objeto de no duplicar trabajos sino de proponer algunas medidas de carácter complementario a las que ya están en marcha en este ámbito.

Como punto de partida, se ha realizado un **análisis DAFO** donde se incluyen algunas de las principales fortalezas y debilidades nacionales, así como las oportunidades y amenazas existentes para situar a España como *hub* de ciberseguridad en Europa.

En cuanto a las **debilidades**, además del grave problema de la falta de profesionales, se añadiría el dominio insuficiente del idioma inglés, los retos estructurales señalados por el Banco de España, como la baja productividad o el reducido peso de la innovación en comparación con otros paises del entorno, la falta de incentivos fiscales o la carencia de una agencia o centro a nivel nacional que dirija y coordine la ciberseguridad nacional.

Las **amenazas** incluirían la fuga de talento nacional, la dependencia tecnológica, las cargas administrativas, las injerencias y conflictos internacionales, así como la percepción estereotipada asociada frecuentemente a aspectos como los gastronómicos o el atractivo turístico de España.

Por otro lado, las **fortalezas** abarcarían el posicionamiento en los índices y organizaciones internacionales de ciberseguridad, la existencia de un ecosistema tecnológico en expansión, los índices de bienestar general de la sociedad, las infraestructuras existentes, el patrimonio

[1] Entre otras, las incluidas en el Plan Nacional de Ciberseguridad https://www.mpr.gob.es/prencom/notas/Paginas/2022/290322-ciberseguridad.aspx y en España Digital 2026. Eje 03. Ciberseguridad https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf

cultural, los indicadores de percepción de la calidad de la gobernanza, y la conexión con América Latina y el mundo hispanohablante.

Finalmente, las **oportunidades** se centrarían en el gran potencial de mercado existente, la nueva regulación en ciberseguridad, la disponibilidad de fondos europeos, el impulso del teletrabajo y los nómadas digitales.

Una de las conclusiones principales de este análisis apunta a que, para la posible constitución de España como un *hub* de ciberseguridad europeo, son necesarias, en primer lugar, las personas. Existe **una carencia preocupante de profesionales de la ciberseguridad**, no solo en España, sino a nivel europeo y mundial. Además, la gran disparidad entre oferta y demanda genera graves problemas para la contratación de personal, tanto por parte del sector privado como del público. Por ello, es fundamental fomentar en España la atracción del talento, nacional e internacional, y crear un entorno favorable para el desarrollo del talento existente y su retención.

En cuanto a las **posibles propuestas** planteadas para corregir debilidades, afrontar amenazas, mantener fortalezas y explotar oportunidades, se recomienda, entre otras, actualizar el Catálogo de Ocupaciones de Difícil Cobertura del SEPE, revisar las deducciones fiscales en el capítulo IV de la *Ley 27/2014 24 diciembre 2024 del Impuesto sobre Sociedades* para incentivar la realización de actividades relacionadas con la ciberseguridad, impulsar la creación del futuro Centro Nacional de Ciberseguridad y un nuevo Plan Nacional de Ciberseguridad con el apoyo de los Fondos europeos, reconocer el papel cada vez más importante en las organizaciones de los directores de seguridad de la información (CISOs), favorecer la implantación de nuevos centros de proceso de datos que proporcionen una capacidad de procesado local suficiente para el soporte a la inteligencia artificial y futuras tecnologías.

Adicionalmente, en el Anexo, se incluyen algunos posibles criterios para la selección de la localización de un territorio donde se pudiera favorecer la concentración física de empresas y profesionales de la ciberseguridad, teniendo en cuenta aspectos socioeconómicos, empresariales, institucionales, de calidad de vida, así como infraestructuras y sostenibilidad.

UNA OPORTUNIDAD PARA ESPAÑA

2. UNA OPORTUNIDAD PARA ESPAÑA

Contexto de la situación en el ciberespacio

Al ritmo actual de crecimiento, los daños causados por los ataques cibernéticos a nivel mundial se prevé que asciendan a unos 10,5 billones de dólares en 2025, un aumento del 300 % con respecto a los niveles de 2015. Si se midiera como país, el cibercrimen sería la tercera economía más grande del mundo después de Estados Unidos y China, superando la riqueza de naciones enteras.[2]

En el último informe sobre el panorama de las ciberamenazas de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)[3] se constata como, a lo largo de la última parte de 2023 y la primera mitad de 2024, se ha producido una notable escalada de los ciberataques, tanto en la variedad y el número de incidentes, como en sus consecuencias. Asimismo, se destaca cómo los Estados miembros de la UE se siguen viendo afectados por las crisis geopolíticas en curso, con un número cada vez mayor de agentes de amenazas que dirigen sus esfuerzos contra organizaciones públicas y privadas. En este sentido, la guerra en Ucrania ha marcado un antes y un después en el entendimiento del ciberespacio como campo de batalla.[4]

En cuanto a la cibercriminalidad, 1 de cada 5 delitos que se denuncian en España ya se producen en el ciberespacio, y los ciberdelitos no paran de crecer. En 2023, los 472.125 ciberdelitos cometidos conocidos representaron un crecimiento de un 26% respecto a 2022.[5]

Dos datos para tener en cuenta: la estimación del coste medio de un ciberataque a una pyme, que se cifraría en unos 35.000 euros, y el 60% de las pymes cierra seis meses después de haber sufrido un ciberataque.[6]

---

[2] Steve Morgan, *2024 Cybersecurity Almanac: 100 facts, figures, predictions, and statistics* https://cybersecurityventures.com/cybersecurity-almanac-2024/

[3] ENISA,*ENISA threat landscape 2024 July 2023 to June 2024* https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

[4] CCN-CERT, *Ciberamenazas y tendencias 2024* https://www.ccn-cert.cni.es/ca/informes-ca/publics/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html

[5] Ministerio del Interior, *Informe sobre la cibercriminalidad en España*, 2023 https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf

[6] Google, *Panorama actual de la Ciberseguridad en España* https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

Sector en crecimiento exponencial

Según un reciente informe[7], ante el aumento y sofisticación de los ciberataques, las organizaciones gastaron aproximadamente 200.000 millones de dólares en productos y servicios de ciberseguridad en 2024, frente a los 140.000 millones de dólares de 2020.

Asimismo, este informe indica que se espera que el mercado de ciberseguridad de proveedores independientes crezca un 12,4 por ciento anual entre 2024 y 2027, superando los niveles históricos de crecimiento, y que la demanda potencial ascienda a un asombroso mercado de 2 billones de dólares a nivel mundial.

En cuanto a la Unión Europea, se espera que el cumplimiento de la Directiva NIS2[8] aumente los presupuestos en ciberseguridad hasta en un 22 por ciento en los primeros años posteriores a su implementación y que el mercado supere los 45 mil millones de euros en 2025.[9]

Por su parte, INCIBE[10] cifra en unas 1.800 el número de empresas dedicadas a la ciberseguridad en España, existiendo una gran cuota de mercado disponible. El 95% del tejido empresarial son pymes y, de ellas, sólo el 36% utiliza protocolos básicos de ciberseguridad, lo cual supone un nicho importante de crecimiento.[11]

Además, un dato importante para tener en cuenta es que la inversión en ciberseguridad constituiría únicamente un 2% del coste de los ciberataques.[12]

> Como indica la agenda *España Digital 2026*[13] la industria de ciberseguridad en España es "***una palanca clave para la generación de riqueza, empleo y empresas en un sector de crecimiento exponencial***".

---

[7] McKinsey, *The cybersecurity provider´s next opportunity: making IA safer*, 2024 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer

[8] https://www.boe.es/doue/2022/333/L00080-00152.pdf

[9] https://tech.eu/2022/10/28/3-great-eu-locations-for-cyber-security-jobs/

[10] https://www.incibe.es/emprendimiento/publicaciones/blog/pilares-del-emprendimiento-en-ciberseguridad-en-espana

[11] https://www.investinspain.org/es/sectores/tic

[12] https://ecs-org.eu/ecso-uploads/2024/12/ECSO-Cybersecurity-Market-Analysis-and-Recommendations-v1.1.pdf

[13] *España digital 2026* https://espanadigital.gob.es/sites/espanadigital/files/2022-10/Espa%C3%B1a_Digital_2026.pdf

ANÁLISIS DAFO

3. ANÁLISIS DAFO

Mediante un análisis DAFO se muestran a continuación algunas de las características internas de España (Debilidades y Fortalezas) y de la situación externa (Amenazas y Oportunidades) que podrían afectar a la posible constitución de España como un *hub* de ciberseguridad europeo y que servirá de base para plantear una posible estrategia y proponer algunas iniciativas.

	Análisis interno	Análisis externo
Debilidades	• Escasez de profesionales de ciberseguridad. • Insuficiente dominio del idioma inglés. • Falta de incentivos fiscales. • Retos estructurales y falta de I+D+i. • Modelo de gobernanza de la ciberseguridad nacional.	
Amenazas		• Fuga de talento nacional. • Dependencia tecnológica. • Cargas administrativas. • Injerencias y conflictos internacionales. • Percepción estereotipada de España.
Fortalezas	• Posicionamiento en índices y organizaciones internacionales de ciberseguridad. • Ecosistema tecnológico en expansión. • Bienestar general, infraestructuras y patrimonio cultural. • Indicadores de percepción de la calidad de la gobernanza. • Conexión con América Latina y mundo hispanohablante.	
Oportunidades		• Gran potencial de mercado. • Nueva regulación en ciberseguridad. • Fondos europeos. • Teletrabajo y nómadas digitales.

3.1. Debilidades

A continuación, se detallan aquellas áreas, factores internos, en las que España podría mejorar.

3.1.1. Escasez de profesionales en ciberseguridad

Todos los estudios conocidos coinciden en que existe una preocupante falta de profesionales en ciberseguridad en España, al igual que en Europa y a nivel mundial[14]. En 2021, los datos del estudio *Análisis y diagnóstico del talento de ciberseguridad en España*[15] señalan que España **habría alcanzado una fuerza laboral en ciberseguridad cercana a los 149.774 trabajadores con una brecha de talento estimada en 26.024. En consecuencia,** el estudio destacaba como ***"una de las mayores prioridades de la administración el hacer frente al reto de identificar, atraer, desarrollar, y retener el talento en los diversos campos de la ciberseguridad".***

Datos más recientes de 2023 de ISC2[16] indicaban que la fuerza laboral en este ámbito en España sería de 182.144 trabajadores y la brecha de talento se cifraría en unos 74.498, con un aumento del 23% en relación con el año anterior.

Por su parte el Foro Económico Mundial[17], ha señalado que desde 2024 la brecha de habilidades cibernéticas ha aumentado en un 8%. Además, solo el 14 % de las organizaciones dispondría de las personas y habilidades que necesitan hoy en día.

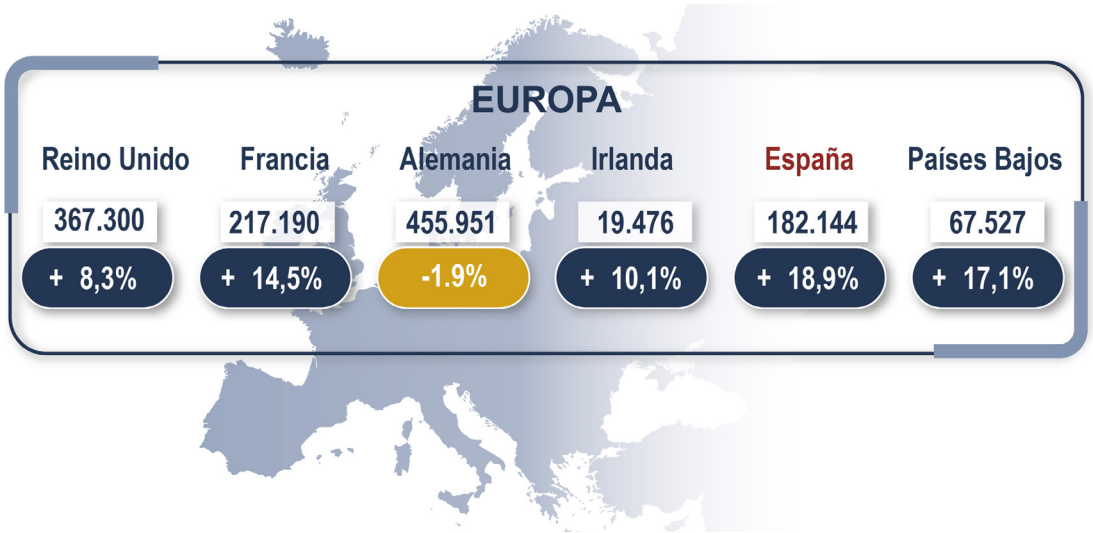


Figura 1: ISC2. Estimación de la fuerza laboral en ciberseguridad, 2023

[14] https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

[15] Análisis y diagnóstico del talento de ciberseguridad en España https://www.observaciber.es/sites/observaciber/files/media/documents/EstudioDiagnosticoTalento2022.pdf

[16] ISC2. *Estudio de la fuerza laboral en ciberseguridad, 2023* ISC2_Cybersecurity_Workforce_Study_2023.pdf

[17] Foro Económico Mundial. *Global Cybersecurity Otulook, 2025.* https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

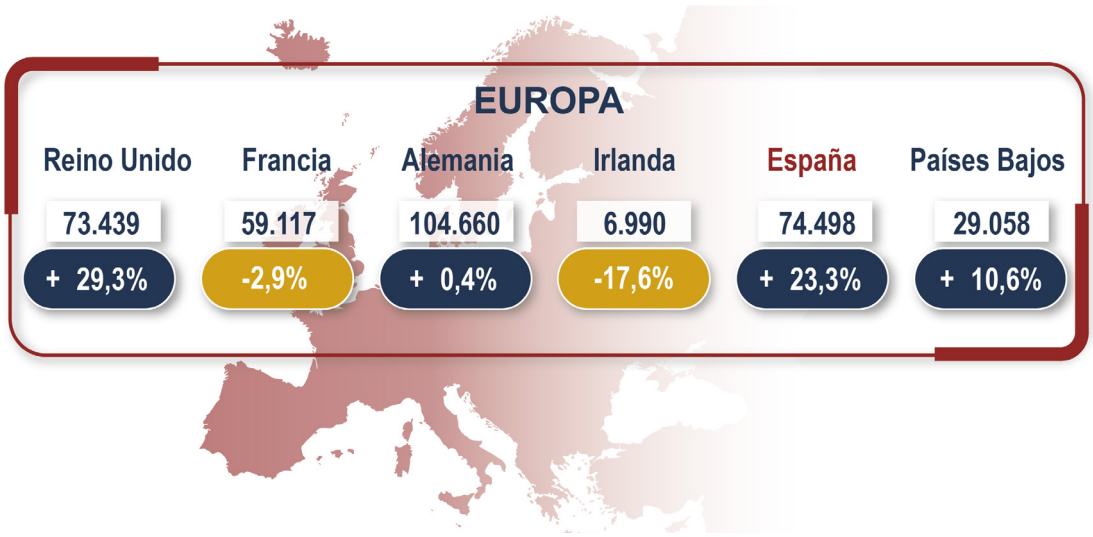


Figura 2: 21 ISC2. Estimación de la brecha de talento en ciberseguridad, 2023

Algunas de las causas posibles de la carencia de profesionales serían las siguientes:

Desajuste entre las competencias disponibles y las requeridas por el mercado laboral

El informe sobre la productividad en España de la OCDE [18] indica que, en comparación con otros países miembros, en España la escasez de cualificaciones es especialmente acusada en una serie de ámbitos importantes para la innovación y el uso de la tecnología, como la ingeniería, la informática y la electrónica, y este hecho puede haber contribuido a la subcualificación existente en estos campos.

Aunque quizá y más importante, continúa el informe, sería el no disponer de las competencias adecuadas para los puestos de trabajo disponibles, incluyendo, además de la subcualificación, el exceso de cualificación, ya que la educación superior en España no estaría bien alineada con las necesidades de las empresas. En este sentido, se señala que la Formación Profesional podría ser un instrumento eficaz para proporcionar competencias técnicas específicas de las que se carece. No obstante, la proporción de estudiantes españoles matriculados en Formación Profesional es muy inferior a la media de los países de la OCDE.

[18] Ministerio de Trabajo y Economía Social (2024), Reactivar el crecimiento ampliamente compartido de la productividad en España. 2024 Informe productividad OCDE español

Además, según un estudio de Eurobarómetro[19], en España el porcentaje de empleados relacionados con la ciberseguridad que se preparan para obtener cualificaciones oficiales o certificaciones sería mucho menor en comparación con la media europea, en concreto, de un 7% frente a un 21%.

En definitiva, como ha indicado la Comisión Europea en su Comunicación al Parlamento y al Consejo en 2023[20] existe un desajuste entre las competencias disponibles y las requeridas por el mercado laboral.

Además, es importante señalar que en esta Comunicación se pone de manifiesto que la mano de obra en el ámbito de la ciberseguridad sigue viéndose afectada por ideas equivocadas en relación con su imagen técnica. En este sentido, se constata que existe un amplio abanico de funciones relacionadas con la ciberseguridad, en ámbitos tan diversos como el regulatorio, el cumplimiento normativo, la auditoría, la sociología o la psicología, entre otros.

Salarios bajos en comparación con países del entorno

En el mencionado estudio *Análisis y diagnóstico del talento de ciberseguridad en España*[21] se indica que uno de los principales obstáculos para la atracción y retención de talento de ciberseguridad está asociado al salario, que hace que la rotación de personal sea muy elevada y que el acceso a talento capacitado sea complicado.

En concreto, se señala que en otros países el sueldo se puede llegar a duplicar o triplicar, incorporando, además, *bonus* o pagos en acciones. La diferencia salarial unida a la posibilidad de teletrabajar complica aún más la retención del talento.

Además, los proyectos para el territorio nacional no serían todo lo rentables que cabría esperar. En un contexto globalizado con tensiones en cuanto demanda y oferta, los costes ajustados no permitirían adaptar los salarios a cantidades competitivas.

Reticencia a contratar personas sin experiencia

En general las empresas son reticentes a la contratación de perfiles sin experiencia ("*entry level*"). La inversión en aprendizaje, formación y adaptación es elevada. A menudo, cuando el profesional empieza a ser productivo y rentable, se plantea el cambio de empresa para crecer en salario o mejorar las condiciones laborales.

---

[19] Eurobarómetro. Cibercompetencias, Trabajo de campo: 24 de abril –17 de mayo de 2024 https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=93344

[20] Colmar la brecha de talento en materia de ciberseguridad para impulsar la competitividad, el crecimiento y la resiliencia de la UE https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:-52023DC0207

[21] Análisis y diagnóstico del talento de ciberseguridad en España https://www.observaciber.es/sites/observaciber/files/media/documents/EstudioDiagnosticoTalento2022.pdf

Las empresas son conscientes de la elevada tasa de rotación en el sector de los profesionales de la ciberseguridad. La escasez de talento nacional, unida a los bajos salarios que se ofrecen en el mercado español, comparado con otros países del entorno, son componentes que incrementan el riesgo de rotación y fuga de talento.

Este es un problema que afecta en general a toda la Unión Europea, como indica la Comisión[22]: "*la reticencia de los empleadores a invertir en capital humano, buscando mano de obra ya formada y experimentada, [...]contribuye aún más a limitar el mercado laboral*".

En este sentido, el estudio del Eurobarómetro mencionado con anterioridad[23] muestra que la mayoría de los encuestados contestaron que los empleados que desempeñaban funciones de ciberseguridad, asumieron el puesto junto al que ya tenían. Sin embargo, en mucha menor medida, los empleados comenzaron directamente en ese puesto su carrera profesional.

Envejecimiento de la población

Como señala la OCDE[24], en la última década, los puestos de trabajo sin cubrir casi se han duplicado, especialmente en sectores como la sanidad y las TIC. El envejecimiento de la población está agravando estas carencias y se espera que se acelere en las próximas décadas. La persistente escasez de mano de obra puede impedir el crecimiento económico y sacar el máximo partido de la transición digital.

España está por debajo de la media europea en tasa de fertilidad y por encima en cuanto a la media de edad de la población.

---

[22] Colmar la brecha de talento en materia de ciberseguridad para impulsar la competitividad, el crecimiento y la resiliencia de la UE https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:-52023DC0207

[23] Eurobarómetro. Cibercompetencias, Trabajo de campo: 24 de abril –17 de mayo de 2024 https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=93344

[24] OECD (2024), OECD Economic Outlook, Volume 2024 Issue 2, OECD Publishing, Paris, https://doi.org/10.1787/d8814e8b-en

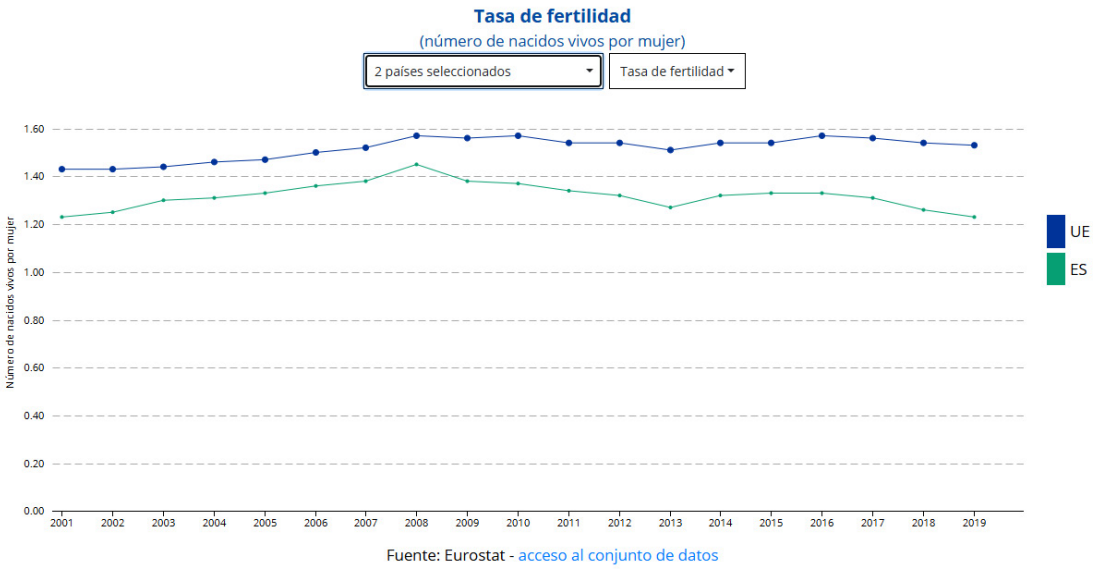


Figura 3: Tasa de fertilidad (número de nacidos vivos por mujer) en España y UE 2002-2019

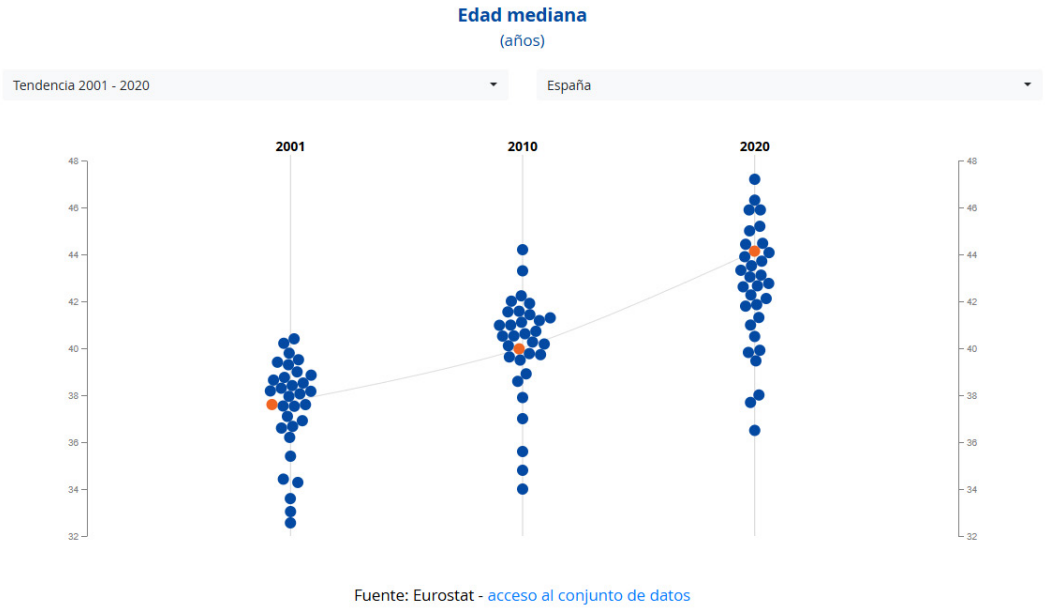


Figura 4: Edad mediana (años) tendencia 2001-2020 en España

Fuente: INE[25]

Por otro lado, el sector de la ciberseguridad y tecnología en general, en auge, podría ser aprovechado como palanca para el incremento de niveles de contratación que, consolidados en un futuro, puedan contribuir a frenar los efectos del envejecimiento poblacional generalizado.

[25] https://www.ine.es/prodyser/demografia_UE/bloc-1c.html?lang=es

3.1.2. Insuficiente dominio de idioma inglés

Según el informe del Índice de Dominio del Inglés 2024 de EF – EPI (*English Proficiency Index*)[26] España ocuparía el puesto número 36 de un total de 116 países, con un nivel de aptitud considerado como "medio". En Europa se encuentra en el puesto 26 de un total de 35 países europeos analizados. Los 10 países que encabezan este ranking son: Países Bajos, Noruega, Singapur, Suecia, Croacia, Portugal, Dinamarca, Grecia, Austria y Alemania.

La falta de dominio del inglés obstaculiza la colaboración y la provisión de servicios en el ámbito europeo e internacional.

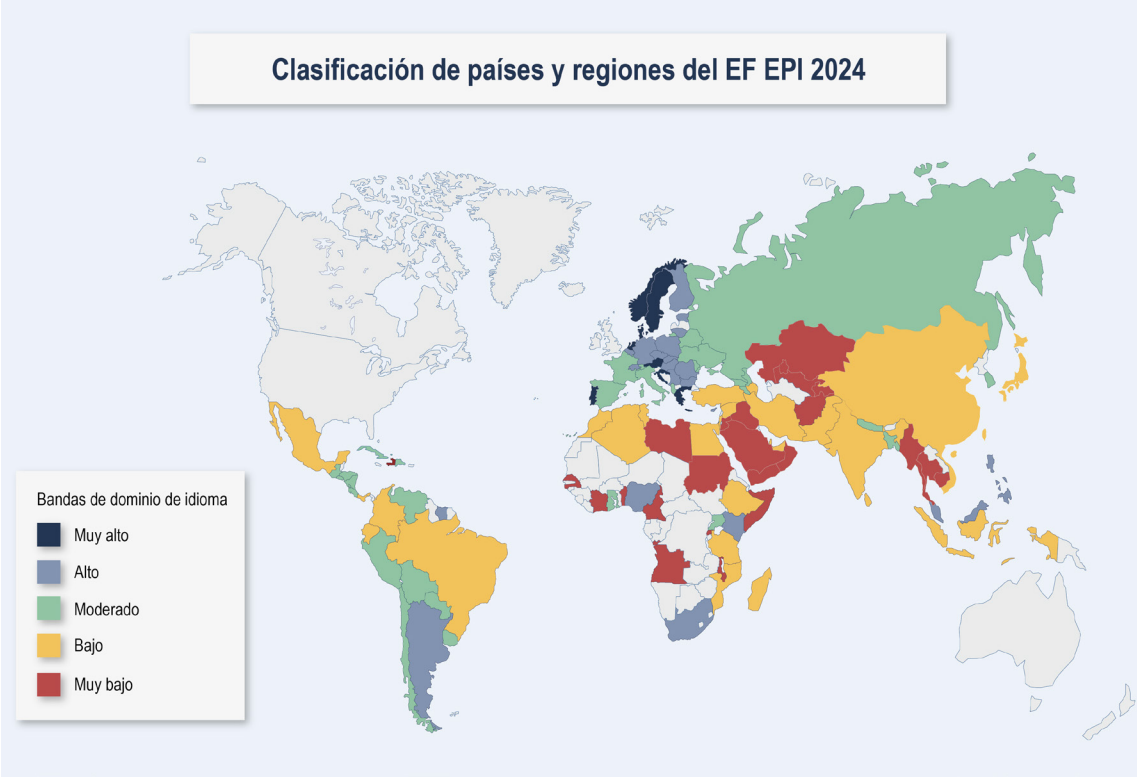


Figura 5: Clasificación de países y regiones del EF EPI 2024

[26] **Índice de Dominio del** Inglés 2024 de EF – EPI https://www.ef.com.es/epi/regions/europe/spain/

3.1.3. Falta de incentivos fiscales

Las deducciones fiscales para incentivar la realización de determinadas actividades incluidas en el capítulo IV de la ***Ley 27/2014 24 diciembre 2024 del Impuesto sobre Sociedades***[27], no recogen específicamente ninguna relacionada con la ciberseguridad.

Ya en 2020, **la Cámara de Comercio de España**[28] proponía el perfeccionamiento del modelo de incentivos para las actividades empresariales vinculadas a la I+D+i y **la sociedad de la información**, con especial atención a las necesidades y naturaleza de las pymes, mediante la revisión de las deducciones fiscales del Impuesto de Sociedades y la simplificación del proceso de emisión de los Informes.

Como ejemplo, la **deducción por actividades de investigación y desarrollo e innovación tecnológica** actualmente incluye la obtención del certificado de cumplimiento de las normas de aseguramiento de la calidad de la serie ISO 9000, GMP o similares, pero no las de gestión de sistemas de seguridad de la información, como **el Esquema Nacional de Seguridad**[29]**,** la **ISO 27001**[30] u otras relacionadas con la ciberseguridad. En este sentido, cabe señalar que, según la directiva europea NIS2 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, la seguridad de los sistemas de redes y de información de los organismos que realizan actividades de investigación es parte integrante de la ciberseguridad global del mercado interior y, por tanto, **el sector de la investigación es uno de los sectores considerados crítico**s según esta directiva.

Asimismo, hay que tener en cuenta que la directiva NIS2 y su transposición al ordenamiento jurídico español, prevista durante el año 2025, supondrá nuevas obligaciones de ciberseguridad en los próximos años para un número muy elevado de entidades de un total de 18 sectores considerados críticos, que en algunos casos incluirían la realización de auditorías periódicas según normas nacionales o internacionales. No obstante, estas obligaciones no se materializarán hasta que el marco de cumplimento esté establecido, previsiblemente en un desarrollo reglamentario posterior, que se demorará en el tiempo.

Por otro lado, las pequeñas y medianas empresas que no pertenecen a sectores críticos y no están bajo el paraguas de la directiva también sufren de un elevado número de ciberataques, que pueden impactar fuertemente en la continuidad del negocio. Estas empresas están, en términos generales, mucho menos preparadas para hacer frente a la creciente ciberamenaza.

En general, la ciberseguridad continúa siendo una asignatura pendiente para la mayoría de las empresas españolas[31] **y los incentivos fiscales para implantar sistemas de gestión y medidas de ciberseguridad no existen.**

---

[27] BOE-A-2014-12328 Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades.

[28] Propuestas para la recuperación y reconstrucción económica y social de España https://www.camara.es/sites/default/files/publicaciones/propuestas_recuperacion_y_reconstruccion_cce-abril_2020.pdf

[29] https://ens.ccn.cni.es/es/

[30] ISO/IEC 27001:2022 - Information security management systems

[31] https://www.incibe.es/empresas/blog/las-principales-vulnerabilidades-de-una-pyme-en-materia-de-ciberseguridad

3.1.4. Retos estructurales y falta de I+D+i

Según el último informe anual del Banco de España[32], en las últimas décadas la economía española ha experimentado una ralentización en el dinamismo de la productividad, superior a la de otros países desarrollados, que constituye uno los principales retos estructurales de la economía española. Entre las causas de la baja productividad se encontrarían: el reducido peso de la innovación en comparación con otros países de nuestro entorno; el nivel educativo de la población española, que seguiría siendo inferior a la media europea; el elevado peso de las empresas de menor tamaño en España en comparación con otros países de nuestro entorno; o la caída en la confianza en las instituciones y en la percepción de su calidad.

Según el citado informe, otro reto estructural es la elevada tasa de paro, en un contexto de desafíos asociados al envejecimiento de la población y a la transición digital, así como a las dificultades crecientes de acceso a la vivienda.

Existen distintas iniciativas a nivel local, autonómico y estatal tendentes a equilibrar los mercados inmobiliarios de zonas tensionadas de ciertas ciudades. En tanto en cuanto estas iniciativas no fructifiquen, la contratación laboral en dichas zonas se dificulta, por cuanto la escasez de vivienda disponible y sus altos precios disuaden a los profesionales. Esto afecta directamente al ámbito de la ciberseguridad en el que a menudo los profesionales que las empresas logran captar proceden de zonas de España distintas del lugar de radicación de la empresa (a menudo una gran ciudad afectada por el problema de la vivienda) o del extranjero.

En cuanto al déficit público en Europa, Grecia, Italia, Francia, España y Bélgica son los países con la deuda más elevada, todos ellos con ratios de deuda en relación con el PIB superiores al 100 %. Luxemburgo, Bulgaria y Estonia registran las ratios más bajas[33].

En relación con la innovación, España se encuentra entre los países de la OCDE que menos gastan en este ámbito y con menor proporción de empresas innovadoras[34]. Solo el 1,4% del PIB se destina a I+D, dos tercios de la media de la OCDE. En 2020, el 11% de las empresas tenían actividades de innovación en curso, la mitad de la media de la OCDE.

---

[32] https://www.bde.es/f/webbe/SES/Secciones/Publicaciones/PublicacionesAnuales/InformesAnuales/23/Fich/InfAnual_2023.pdf

[33] https://european-union.europa.eu/principles-countries-history/facts-and-figures-european-union_es

[34] Ministerio de Trabajo y Economía Social (2024), Reactivar el crecimiento ampliamente compartido de la productividad en España. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/trabajo14/Documents/2024/050624-informe-productividad-ocde.pdf.pdf

Figura 2.13. El gasto en I+D es bajo y en España hay pocas empresas innovadoras

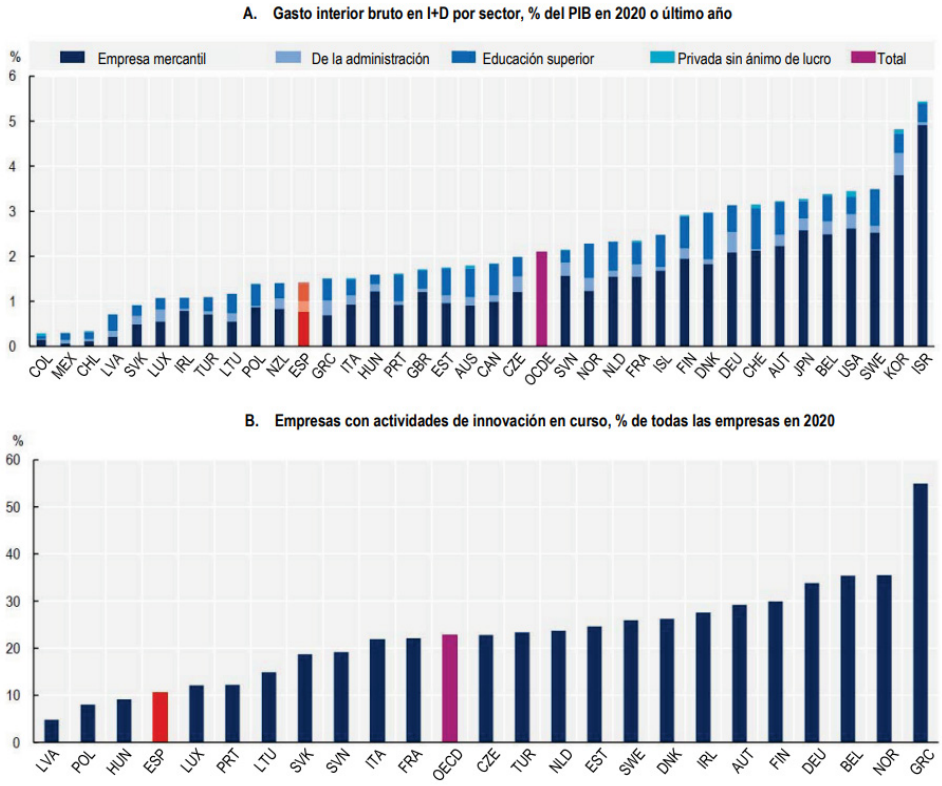


Figura 6: El gasto en I+D es bajo y en España hay pocas empresas innovadoras

3.1.5. Modelo de gobernanza de la ciberseguridad nacional

En España, el Real Decreto-ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información[35] y la Estrategia Nacional de Ciberseguridad[36] han definido la actual estructura de la gobernanza de la ciberseguridad y su integración en el marco del Sistema de Seguridad Nacional. En este modelo **no existe una agencia, centro nacional o autoridad única que impulse, dirija, coordine y asigne recursos en materia de ciberseguridad**. El modelo español contrasta con el modelo más centralizado que en la actualidad tienen la mayoría de países europeos.

En este sentido, es destacable que España es un país descentralizado en el que comunidades autónomas y entidades locales cuentan con importantes competencias transferidas: sanidad, educación, servicios sociales etc. recayendo en el ámbito autonómico la competencia relativa a

[35] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

[36] https://foronacionalciberseguridad.es/estrategia-nacional-de-ciberseguridad

la digitalización de los servicios y su consiguiente ciberseguridad, que tiene repercusiones tanto para el sector público como para el privado. A menudo las comunidades autónomas colaboran de forma voluntaria en el ámbito de la ciberseguridad, siendo recomendable un incremento y consolidación de procesos trasversales que permitan el intercambio y colaboración para el aprendizaje colectivo.

Como indicaba en 2020 el Comité de Contacto de las Entidades Fiscalizadoras Superiores de la Unión Europea[37]: "*Los modelos de gobernanza de la ciberseguridad difieren entre los Estados miembros, y dentro de estos, las competencias en materia de ciberseguridad a menudo se reparten entre numerosas entidades. Estas diferencias podrían obstruir la cooperación necesaria para responder a incidentes transfronterizos de gran envergadura e intercambiar información sobre amenazas en el ámbito nacional, e incluso más a escala de la UE*". Es más que una mera cuestión técnica, por lo que exige un liderazgo eficaz.

Con el fin de reordenar competencias públicas dispersas y aportar coherencia y efectividad a las políticas públicas en esta materia, se han propuesto nuevos modelos de gobernanza pública de ciberseguridad[38,39] o de políticas públicas que podrían contribuir a una mayor unidad, coordinación y claridad del sistema de gobernanza de la ciberseguridad.

El anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad[40] publicado el 14 de enero de 2025, que transpondrá al ordenamiento jurídico español de la directiva NIS2, constituye una oportunidad para reforzar el actual modelo de gobernanza de la ciberseguridad nacional con la previsión de la creación de un Centro Nacional de Ciberseguridad, que pueda superar la actual dispersión competencial en materia de ciberseguridad.

---

[37] La ciberseguridad en la UE y sus Estados miembros https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_ES.pdf

[38] https://www.fundacionesys.com/es/la-fundacion-empresa-seguridad-y-sociedad-digital-esys-propone-un-nuevo-modelo-de-gobernanza-publica-de-la-ciberseguridad-en-espana/

[39] https://revistas.uca.es/index.php/rejucrim/article/view/9046/10401

[40] https://www.interior.gob.es/opencms/ca/detalle/articulo/El-Consejo-de-Ministros-aprueba-el-anteproyecto-de-Ley-de-Coordinacion-y-Gobernanza-de-la-Ciberseguridad/

3.2. Amenazas

A continuación, se detallan aquellas áreas, factores externos, a las que España se enfrenta que, en caso de materializarse, pueden afectar negativamente a la constitución de España como *hub* de ciberseguridad europeo.

3.2.1. Fuga de talento nacional

Todas las empresas tecnológicas, muchas de las cuales tienen un origen extranjero, se encuentran a la búsqueda de talento. España presenta debilidades en la formación y generación de talento propio a lo que se suman los bajos salarios en comparación con el resto de países del entorno.

Estas variables propician que una parte del talento nacional sea contratado por empresas extranjeras capaces de ofrecer mayores salarios, inversiones en formación y capacitación y mejores condiciones labores incluyendo la posibilidad de trabajar en remoto buena parte del tiempo en España.

Esta opción de fuga de talento sin desplazamiento no es tan gravosa como la fuga de talento tradicional, si bien es igual de negativa en lo que se refiere al crecimiento de la empresa e industria nacional en ciberseguridad, que se enfrenta a serias dificultades para la contratación de perfiles nacionales adecuados.

En términos generales, como indica un estudio[41] basado en datos del INE, el ritmo actual de emigración supone un lastre para la economía española, si no es compensado por el valor del capital humano de los inmigrantes o el retorno futuro de parte de los emigrantes actuales.

3.2.2. Dependencia tecnológica

En la actualidad, buena parte de las tensiones geoestratégicas de relevancia están vinculadas al desarrollo y dominancia tecnológica. Países líderes en tecnología como China o Estados Unidos libran una batalla por mantener posiciones de preponderancia. La UE se ha quedado rezagada de Estados Unidos en tecnologías avanzadas, mientras que China se ha puesto al día en muchos sectores y está ganando la carrera por el liderazgo en algunas nuevas áreas de crecimiento.[42]

La UE pretende evitar situaciones claras de dependencia tecnológica avanzando en mayor soberanía en este ámbito que permita obtener a los 27 Estados Miembros el peso específico suficiente como para tomar sus propias decisiones, basándose en sus propios valores y respetando sus propias reglas frente a otros Estados preponderantes y gigantes tecnológicos como las Plataformas actuales. En este sentido la Brújula de la Competitividad de la UE incluye como uno de sus pilares la reducción de las dependencias excesivas de determinados países o proveedores incrementando la resiliencia y la seguridad.

---

[41] https://www.fbbva.es/noticias/emigraciones-valor-capital-humano/

[42] *A Competitiveness Compass for the EU*, 2025
https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en

Como indica la Estrategia de Seguridad Nacional[43], el impulso hacia una soberanía tecnológica forman parte, entre otros, del amplio espectro de políticas tendentes al fortalecimiento de la seguridad europea y del papel de la Unión como actor global. En este sentido, es clave la reducción de las dependencias estratégicas de materias primas y componentes esenciales de las cadenas de valor industriales, a través de la diversificación de la producción y el suministro, el mantenimiento de reservas y el impulso a la producción e inversión en Europa.

Las materias primas fundamentales, vitales para la economía y tecnologías estratégicas cuyo suministro presenta un elevado riesgo de sufrir interrupciones, proceden principalmente de fuera de la Unión Europea. Actualmente, para determinadas materias primas fundamentales se depende sólo de un país, en concreto de China, que proporciona el 100 % del suministro de tierras raras. Por su parte Turquía proporciona el 98 % del suministro de boro y Sudáfrica el 71 % de platino.[44]

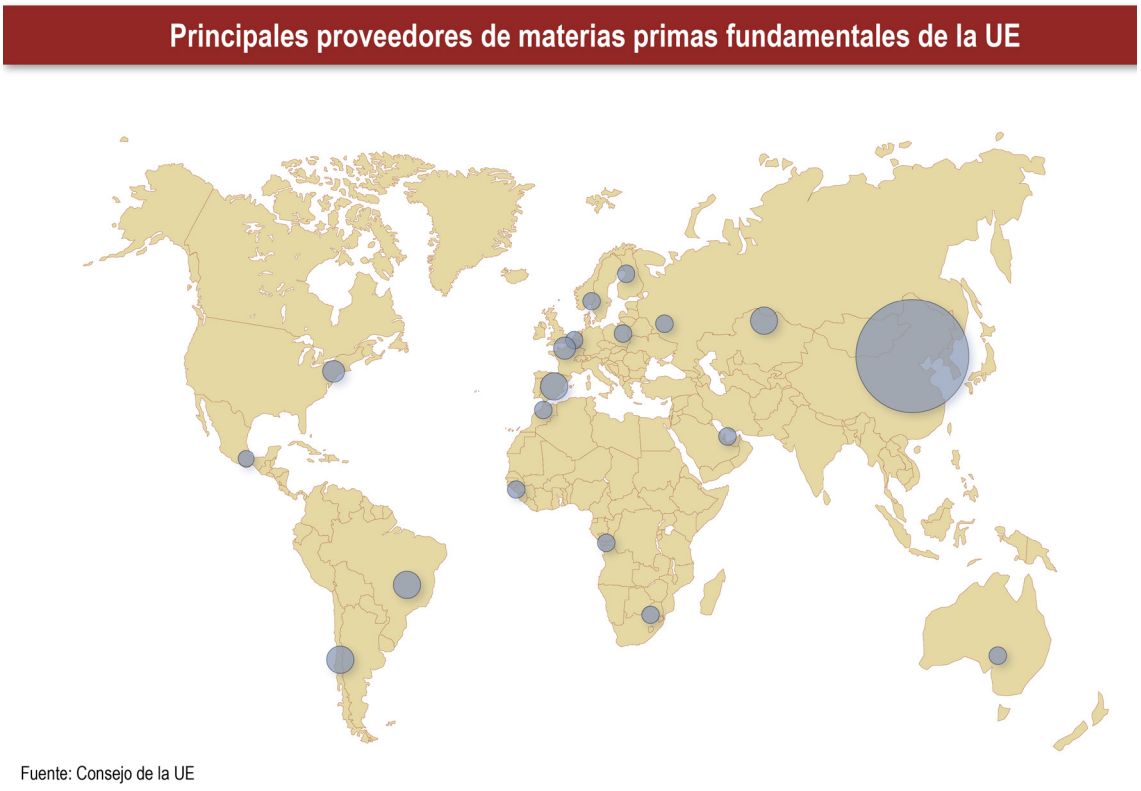


Figura 7: Principales proveedores de materias primas fundamentales de la UE

[43] https://www.dsn.gob.es/es/publicaciones/estrategia-de-seguridad-nacional-2021

[44] https://www.consilium.europa.eu/es/infographics/critical-raw-materials/

Para promover la independencia tecnológica cabe destacar iniciativas legislativas como el Reglamento europeo de Materias Primas Fundamentales, el Reglamento UE de Mercados digitales, la Ley Europea de Chips o de Identidad Digital Europea, así como económicas: los Fondos procedentes de NextGeneration UE o financiación de competencias digitales para ciudadanos de la UE.

3.2.3. Cargas administrativas

En el plano de las ayudas económicas, si bien hay un amplio abanico dentro de los planes europeos y nacionales, los mecanismos administrativos para todo el ciclo de vida de presentación, aprobación, implementación y seguimiento de cualquier iniciativa sobre ciberseguridad ralentizan su materialización. Se requieren procesos más efectivos que reduzcan el coste de gestión y aceleren la creación de valor.

Según el proyecto *Doing Business*[45] del Grupo Banco Mundial, España en 2020 ocupaba el puesto 30 de 190 países en cuanto a facilidad para hacer negocios. Este *ranking* tiene en cuenta un total de 10 ámbitos diferentes. No obstante, el primer paso, que se refiere al establecimiento de un nuevo negocio, el puesto bajaba hasta el 97, en especial debido al apartado relativo a los trámites y número de procedimientos.

La Brújula de la competitividad de la UE reconoce la necesidad de simplificar el marco regulador, reducir las cargas y favorecer la rapidez y la flexibilidad, a la vez que insta a todos a hacer un gran esfuerzo para producir normas más sencillas y acelerar los procedimientos administrativos. Señala específicamente que acceder a fondos u obtener decisiones administrativas debe ser más rápido y barato para empresas y ciudadanos.

3.2.4. Injerencias y conflictos internacionales

Tal y como establece la Estrategia de Seguridad Nacional[46] española, el espionaje e injerencias extranjeras es un grave riesgo para la seguridad de España, pudiendo extrapolarse el mismo al resto de países europeos y occidentales. El contexto internacional actual se caracteriza por una cierta tendencia al retroceso del multilaterialismo, y un incremento de la competición estratégica entre Estados ha supuesto un aumento de estas amenazas, incluyendo el despliegue de campañas de desinformación, que figuran entre las herramientas más eficaces con las que algunos países aspiran a expandir su influencia internacional.

---

[45] https://archive.doingbusiness.org/content/dam/doingBusiness/country/s/spain/ESP.pdf

[46] https://www.dsn.gob.es/es/publicaciones/estrategia-de-seguridad-nacional-2021

La guerra de agresión de Rusia sobre Ucrania, que dio comienzo en febrero del año 2022, ha generado efectos negativos en todos los países, europeos y occidentales, primeramente. Dichos efectos fueron económicos, energéticos y directamente relacionados con la ciberseguridad, en tanto en cuanto España, al igual que el resto de países que han apoyado a Ucrania han sido blanco de ciberataques en forma de *hackivismo* o grupos patrocinados por estados.

En el ámbito tecnológico y de la ciberseguridad, China y EEUU mantienen un pulso por la soberanía cuyas consecuencias se trasladan al resto de países, entre ellos España.

3.2.5. Percepción estereotipada de España

Según un reciente estudio[47] los europeos occidentales perciben sus propios países como superiores a España en lo que respecta al desarrollo científico y tecnológico, el sistema económico, la democracia y el respeto al medio ambiente. Pero la mayoría considera que la calidad de la vida en España es mayor que en su país y que España tiene una mejor producción artística y cultural. La característica mejor valorada de España sería como destino turístico, tanto por parte de los europeos como por parte de los propios españoles. Es destacable que los españoles sistemáticamente expresen opiniones sobre España más negativas que los demás europeos.

La percepción de España en Hispanoamérica sería en general positiva, y alineada con la que se tendría de otros países europeos, aunque asociada también frecuentemente a aspectos como los gastronómicos o el atractivo turístico.[48]

Además, nuestro país podría enfrentar prejuicios y estereotipos por parte de otros países o empresas en el entorno internacional. A menudo esta visión negativa o sesgada en lo que respecta a España no es sino parte de una posible estrategia de descrédito desplegada a menudo con éxito por otro país competidor, en ciertos momentos puntuales, por ejemplo, aquellos en los que se pueda estar dilucidando una importante inversión o compra de empresa nacional por otra extranjera de mayor tamaño.

La percepción internacional de país con nivel de desarrollo inferior al de muchos de sus competidores es una amenaza a tener en cuenta, ya que, de ser explotada convenientemente, puede generar desconfianza en posibles inversores o percepción errónea en cuanto a la calidad de los productos o servicios de ciberseguridad.

---

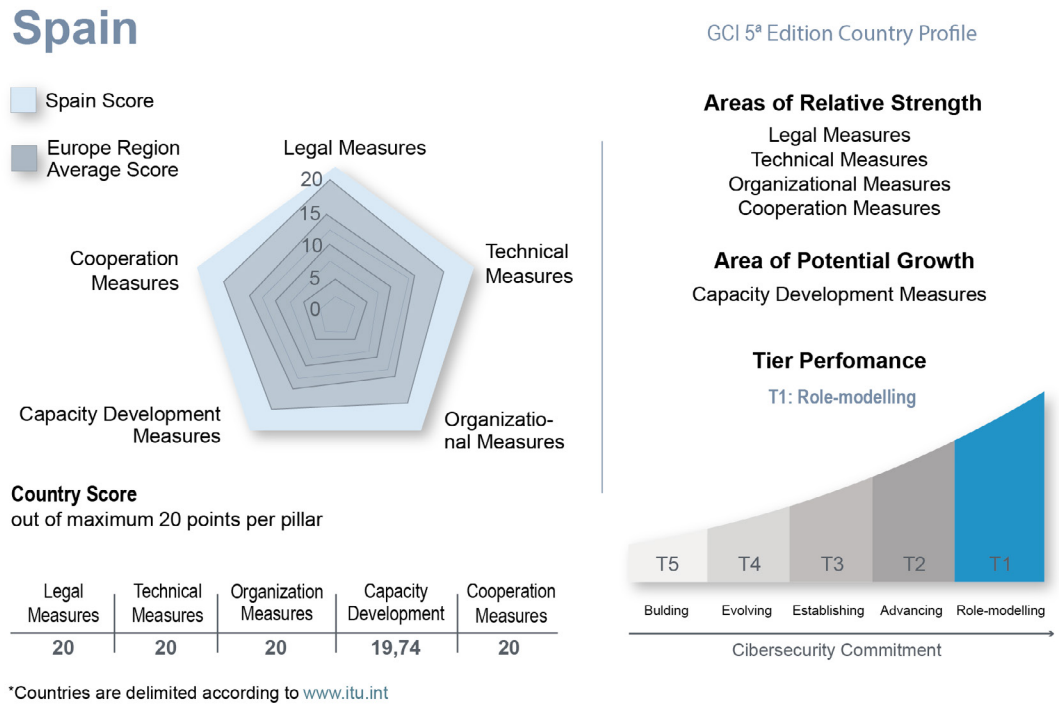
[47] Barómetro de la Imagen de España

[48] 11ª Oleada Barómetro Imagen de España. Estudio monográfico sobre América Latina - Real Instituto Elcano

3.3. Fortalezas

3.3.1. Posicionamiento en índices y foros internacionales de ciberseguridad

España se encuentra entre los países que muestran un compromiso mayor con la ciberseguridad a nivel mundial, según se recoge en el Índice de Ciberseguridad Global[49] de la Unión Internacional de Telecomunicaciones (UIT), el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación (TIC).



Fuente: Unión Internacional de Telecomunicaciones (UIT)

Figura 8: Índice de Ciberseguridad Global 2024 (UIT)

España, con 62 Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), es el segundo país del mundo tras los Estados Unidos con mayor número de equipos en el foro de referencia mundial FIRST.[50]

[49] https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

[50] https://www.first.org/members/map

Figura 9: Equipos de respuesta a incidentes en el foro de referencia mundial FIRST

3.3.2. Ecosistema tecnológico en expansión

El desarrollo actual de clústeres de ciberseguridad sectoriales y territoriales, así como aceleradores verticales y la importante presencia de las grandes multinacionales de consultoría en España fomentan el desarrollo de nuevos negocios y establecimientos empresariales. Ejemplos como CyberMadrid[51], el Clúster de Ciberseguridad de Andalucía[52], Cybasque[53], o la reciente iniciativa CyberLur[54], cuyo objetivo es la integración de empresas, asociaciones regionales y clústeres, muestran la potencialidad de un sector en expansión.

Además, la iniciativa RETECH[55] (Redes Territoriales de Especialización Tecnológica) tiene el objetivo de desarrollar el ecosistema de ciberseguridad (capacidades, industria, I+D+i, talento, etc.) constituyendo una política pública de inversión territorial asegurando la coordinación, la colaboración y la complementariedad.

---

[51] https://www.cybermadrid.org/

[52] https://www.juntadeandalucia.es/presidencia/portavoz/economiayempleo/190658/ConsejeriadelaPresidencia/AntonioSanz/ClusterdeCiberseguridad/entidades/CIAN/Malaga

[53] https://www.cybasque.eus/

[54] https://www.aeiciberseguridad.es/index.php/AEI_Ciberseguridad_se_transforma_en_CyberLur_con_el_objetivo_de_dimensionarse_y_posicionar_la_ciberseguridad_espanola_como_una_industria_referente

[55] https://www.incibe.es/retech

Por su parte, el ICEX ha venido elaborando estudios de mercado de la ciberseguridad a nivel internacional para facilitar el proceso de internacionalización de la industria española de ciberseguridad[56]. Asimismo, desarrolla conjuntamente con INCIBE misiones comerciales para la apertura o consolidación de la presencia española en mercados internacionales.[57]

España cuenta con múltiples parques tecnológicos y centros de innovación, como el Málaga TechPark, que alberga unas 630 empresas tecnológicas. Estos polos actúan como catalizadores para atraer empresas extranjeras, ofreciendo la infraestructura de apoyo necesaria. Los centros de datos existentes posicionan al país como un nodo de interconexión en el sur de Europa.[58]

Otra de las fortalezas con las sólidas redes de telecomunicaciones, incluyendo las infraestructuras terrestres y submarinas, como los 45.000 km de cable que conectan África, la península ibérica, Reino Unido y Asia Occidental. Es el primer país en despliegue de fibra óptica dentro de la Unión Europea, lo que proporciona unas buenas condiciones de conectividad, incluso en zonas rurales. En este sentido, el último informe de la Comisión europea sobre la Década Digital se indica que España obtiene unos resultados excepcionales en conectividad: el despliegue de fibra óptica hasta las instalaciones se sitúa en el 95,2% y la cobertura 5G en el 92,3%, muy por encima de la media de la Unión Europea[59]. Además, una infraestructura digital bien desarrollada puede atraer inversiones extranjeras, promover la creación de empleo en el sector tecnológico y estimular la creación de nuevas empresas y *startups* innovadoras, lo que en última instancia impulsa el crecimiento económico y mejora la calidad de vida de los ciudadanos.

En cuanto formación especializada, según datos recopilados por INCIBE[60], España cuenta con un total de 87 programas de máster, 9 especializaciones universitarias, 11 grados y 113 especializaciones de formación profesional en ciberseguridad.

En el ámbito regulatorio, la *Ley 28/2022[61], de 21 de diciembre, de fomento del ecosistema de las empresas emergentes*, establece un conjunto de medidas específicas en el ámbito fiscal, mercantil, civil y laboral.

Por su parte, la iniciativa de "Nómadas Digitales"[62] no solo contribuye a posicionar a España como un destino preferido para profesionales globales, sino que también impulsa la economía local, promueve la diversidad y el intercambio cultural, y fomenta la innovación y el crecimiento en sectores clave.

---

[56] https://www.incibe.es/internacionalizacion/nuevos-mercados/estudios-de-mercado-de-la-ciberseguridad-internacionales

[57] https://www.incibe.es/index.php/incibe/sala-de-prensa/incibe-e-icex-se-unen-promover-internacionalizacion-industria-espanola

[58] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/europes-next-cybersecurity-hub-what-makes-spain-a-leading-contender#/

[59] https://digital-strategy.ec.europa.eu/en/factpages/spain-2024-digital-decade-country-report

[60] https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad

[61] https://www.boe.es/buscar/pdf/2022/BOE-A-2022-21739-consolidado.pdf

[62] https://prie.comercio.gob.es/es-es/paginas/teletrabajadores-caracter-internacional.aspx

Respecto a los costes de establecimiento de empresas, existen una serie de beneficios y ahorros estructurales propios del país: eficiencia energética gracias al clima y las horas de luz solar frente a países más septentrionales, menores costes de conectividad y mayor rendimiento debido al nivel de despliegue de conectividad de altas prestaciones en el territorio nacional frente al resto de Europa. Menores costes de seguridad física y mayor potencial de desarrollo local vinculado a la seguridad territorial.

En relación con los salarios, un trabajador medio en España ganaría 4.526€ menos al año de la media europea[63]. Si bien es cierto que este dato podría representar un problema, es un claro ejemplo de la facilidad para grandes empresas de situar sus centros de trabajo en el país y aprovechar esta ventaja.

En cuanto a la imprescindible colaboración público-privada, en España existen numerosas iniciativas en este ámbito, entre las que se encuentra el Foro Nacional de Ciberseguridad.[64]

En relación con las materias primas utilizadas en el ámbito tecnológico **es muy relevante que España sea el único productor de estroncio en la Unión Europea y el principal productor mundial**. El estroncio es un material utilizado en electrónica, telecomunicación e informática[65] y está considerado como materia prima fundamental para el futuro de las cadenas de suministro de la UE.

3.3.3. Bienestar general, infraestructuras, patrimonio cultural

Según el Índice para una Vida Mejor elaborado por la OCDE[66], España obtiene buenos resultados en muchas dimensiones de bienestar general. En concreto destaca en el equilibrio vida-trabajo, salud, relaciones sociales y seguridad. Entre las fortalezas destaca un fuerte sentido de comunidad y un alto nivel de compromiso cívico.[67]

---

63 https://ec.europa.eu/eurostat/databrowser/bookmark/fafb4e3b-f3aa-4907-9102-16be8df6f775?lang=en

64 https://foronacionalciberseguridad.es/

65 https://web.igme.es/PanoramaMinero/actual/ESTRONCIO%202021.pdf

66 https://www.oecdbetterlifeindex.org/es/countries/spain-es/

67 En promedio, los resultados serían menores en empleo, educación y satisfacción ante la vida.

Por su parte, el Índice de Desarrollo Humano de Naciones Unidas[68], sitúa a España en el puesto 27 del total de 193 países, en el grupo de desarrollo humano muy alto.

En cuanto al Índice Global de Paz 2024[69] elaborado por el Instituto para la Economía y la Paz, España ocupa la posición 23 de los 163 países analizados, con un nivel de seguridad alto.

Cuando las personas se sienten seguras en su entorno, están más dispuestas a establecerse y participar activamente en la vida de la comunidad. Un entorno seguro promueve la confianza y la tranquilidad, lo que contribuye a mejorar la calidad de vida de los habitantes. Las ciudades con altos niveles de seguridad suelen ser más atractivas para vivir, especialmente para familias y personas que buscan un lugar donde criar a sus hijos o establecerse a largo plazo. Un entorno seguro también promueve la inversión empresarial, el desarrollo comercial y el turismo, lo que a su vez genera empleo y aumenta la actividad económica en la comunidad. La seguridad ciudadana promueve la cohesión social y el sentido de pertenencia a la comunidad. España es un país con una tasa de criminalidad más baja[70] en comparación con otros países europeos.

Una buena sanidad garantiza que los residentes tengan acceso a atención médica de calidad cuando la necesiten. El acceso a una atención médica confiable y efectiva es fundamental para mantener la salud y el bienestar de la población, promueve la calidad de vida, brinda seguridad y tranquilidad para la atracción de talento. España se sitúa entre los primeros puestos[71] del "Ranking mundial" que evalúa los sistemas de salud de todo el mundo.

España ocupa el segundo lugar a nivel mundial en extensión de su red ferroviaria de alta velocidad[72], siendo únicamente superada por China. Tiene, además, la mayor red de autopistas y autovías de la UE (más de 17.000 km) una plataforma marítima inmejorable en el sur de Europa y es centro neurálgico de conexiones aéreas.[73]

Por otra parte, la climatología y las horas de luz mejora la calidad de vida, posibilita atraer turismo, promover el bienestar psicológico, atraer talento y estimular el desarrollo económico. España se distingue por sus abundantes horas de luz solar, que rondan las 3.000 horas de sol anuales, en comparación con otros países europeos.

España ocupa asimismo las primeras posiciones del mundo por número de sitios declarados patrimonio de la humanidad por la UNESCO[74], con 50 bienes inscritos en Lista del Patrimonio Mundial, que poseen un valor universal excepcional, es decir, que tienen una importancia cultural o natural extraordinaria, que trascienden fronteras y tienen un significado especial dentro de la historia de la humanidad.[75]

---

68 https://hdr.undp.org/system/files/documents/global-report-document/hdr2023-24overviewsp.pdf

69 https://www.economicsandpeace.org/wp-content/uploads/2024/06/GPI-2024-web.pdf

70 https://www.interior.gob.es/opencms/eu/detalle/articulo/La-tasa-de-criminalidad-se-situa-en-el-488-al-cierre-de-2022/

71 https://www.jstor.org/stable/j.ctv17hm85z?turn_away=true

72 https://uic.org/passenger/highspeed/article/high-speed-data-and-atlas

73 https://www.autopista.es/noticias-motor/paises-con-mas-kilometros-de-autovias-espana-tercera_138079_102.html

74 https://whc.unesco.org/es/list/

75 https://www.exteriores.gob.es/RepresentacionesPermanentes/unesco/es/UNESCO%20en%20Espana/Paginas/Inscripciones%20UNESCO/Patrimonio-Mundial.aspx

El rico patrimonio cultural de España permite forjar una identidad única, generando un sentido de pertenencia entre los residentes locales, además de ingresos y empleo, lo que contribuye al desarrollo económico y la vitalidad de la comunidad.

España es el segundo país del mundo que más turistas atrae, solo por detrás Francia.[76]

Además, España es el cuarto país de la OCDE tras Estados Unidos, Alemania y Reino Unido en atracción de población extranjera. Según un estudio del Fondo Monetario Internacional (FMI)[77], tanto los trabajadores cualificados como los no cualificados que se trasladan a otro país aportan ventajas a las naciones receptoras a largo plazo. En este sentido, el estudio sobre inmigración internacional de la OCDE[78] indica que, en todos los países miembros, los inmigrantes aportarían más en impuestos y cotizaciones de lo que los gobiernos gastan en su protección social, sanidad y educación.

3.3.4. Indicadores de percepción de la calidad de la gobernanza

La estabilidad política y la gobernanza democrática fomentan la confianza de los inversores y las empresas, lo que promueve la inversión extranjera y nacional, y estimula el desarrollo económico. De esta manera se crea un entorno propicio para la innovación, el emprendimiento y la protección de los derechos civiles y las libertades individuales. Asimismo, facilita la cooperación internacional, el comercio y la integración regional, lo que contribuye al fortalecimiento de la posición del país en la comunidad internacional y a su desarrollo socioeconómico a largo plazo.

De acuerdo con el Índice de Democracia 2023[79] elaborado por *The Economist Intelligence Unit* (EIU), España se encuentra en la posición 23 a nivel global, con 8,07 puntos, en el grupo de cabeza catalogado como "*full democracy*," aunque por un estrecho margen.[80]

Los Indicadores Mundiales de Gobernanza[81] elaborados por el Banco Mundial describen patrones generales de percepción de la calidad de la gobernanza en los distintos países y a lo largo del tiempo. La gobernanza incluye el proceso por el que se seleccionan, controlan y sustituyen los gobiernos; la capacidad del gobierno para formular y aplicar eficazmente políticas sólidas; y el respeto de los ciudadanos y del Estado por las instituciones que rigen las interacciones económicas y sociales entre ellos. Los indicadores de España se muestran, en general, superiores a los del grupo de Europa y Asia Central, aunque inferiores a los del grupo de países de altos ingresos de la OCDE en el que se encuentra España.

---

[76] https://www.unwto.org/es/news/en-2023-con-la-reapertura-de-asia-y-el-pacifico-al-turismo-china-recupero-su-primera-posicion-en-la-clasificacion-de-paises-que-mas-gastan

[77] http://www.imf.org/~/media/files/publications/spillovernotes/spillovernote8

[78] https://www.oecd.org/en/publications/international-migration-outlook-2021_29f23e9d-en/full-report.html

[79] https://pages.eiu.com/rs/753-RIQ-438/images/Democracy-Index-2023-Final-report.pdf

[80] Entre los años 2006 y 2023 la media de la puntuación de los países europeos y del entorno se ha mantenido superior a la de España. En el índice de 2021, con 7,94 puntos descendió al grupo "*flawed democracies*".

[81] https://www.worldbank.org/en/publication/worldwide-governance-indicators/interactive-data-access

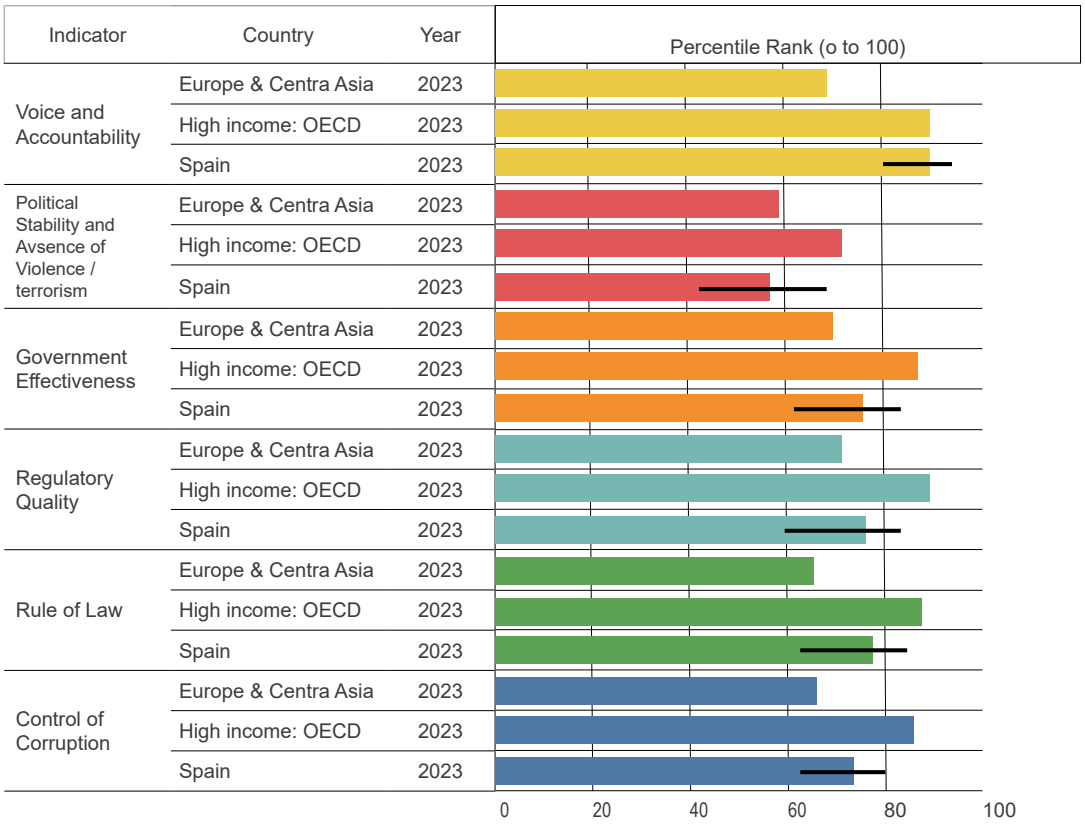


Figura 10: Indicadores Mundiales de Gobernanza del grupo Banco Mundial

En España se ha promulgado la *Ley 15/2017 de Defensa de la Competencia*[82], que forma parte de la normativa nacional sobre soborno, corrupción, antimonopolio y ayudas estatales Las leyes antimonopolio tienen como objetivo principal promover la competencia en los mercados, evitando la formación de monopolios que puedan restringir la libre competencia y perjudicar a los consumidores. Al fomentar la competencia, se contribuye a mejorar la eficiencia económica, estimular la innovación y reducir los precios para los consumidores finales. Estas leyes garantizan un entorno empresarial más equitativo y transparente, donde las empresas compiten en igualdad de condiciones y se promueve un mercado más dinámico y justo.

Asimismo, España ha impulsado medidas para proteger a los consumidores vulnerables[83] frente a los nuevos retos del entorno digital y social, destacando la importancia de reforzar las relaciones internacionales y la cooperación para abordar conjuntamente estos desafíos. Además, ha priorizado la protección de los consumidores en áreas como las comunicaciones comerciales online, el comercio electrónico y la defensa del medio ambiente, reconociendo la importancia de garantizar un nivel elevado de protección para todos los consumidores dentro y fuera de la Unión Europea.

---

[82] https://www.fnmt.es/transparencia/organizacion-gobierno-y-personal/normativa-sobre-soborno-corrupcion-antimonopolio-y-ayudas-estatales

[83] https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/consumo/Paginas/2023/140923-proteccion-consumidores-vulnerables.aspx

3.3.5. Conexión con América Latina y mundo hispanohablante

Además de las relaciones institucionales existentes, culturales e históricas, España es, junto con Estados Unidos, el inversor de referencia en la región. Asimismo, España es el segundo destino mundial de las inversiones de las empresas latinoamericanas. Veinte países de la región cuentan con inversiones en España. América Latina sería el cuarto mayor inversor en España, precedido de Estados Unidos, Reino Unido y Francia, y por delante de Alemania o Italia. Es destacable que el sector tecnológico es el principal generador de iniciativas de inversión.[84]

Para favorecer la inversión existe una extensa red de convenios que evitan la Doble Imposición, así como Acuerdos para la Promoción y Protección Recíproca de Inversiones.[85]

Cabe señalar que el español es el 4º idioma más hablado del mundo, detrás del inglés, el chino mandarín y el hindi. El volumen de hablantes de español como lengua nativa se sitúa en segundo lugar, solo por debajo del chino mandarín. Los hablantes potenciales de español sobrepasaron en 2024 por primera vez la cifra de los 600 millones en todo el mundo, lo que facilita el acceso a un mercado global en constante expansión. Esto elimina las trabas relacionadas con el idioma a la hora de relacionarse con un amplio conjunto de profesionales y empresas y configura a nuestro país como un nodo desde el que ofrecer servicios a un elevado número de mercados internacionales.

Asimismo, la proporción de sitios web relevantes cuyo contenido se expresa en español se sitúa por encima de los porcentajes de los sitios con contenido en alemán o en francés.[86]

---

[84] https://www.investinspain.org/content/icex-invest/es/noticias-main/2024/global-latam.html

[85] Secretaría de Estado de Comercio. *Relaciones bilaterales España-Latinoamérica y el Caribe,* 2024 Relaciones bilaterales

[86] https://cvc.cervantes.es/lengua/anuario/anuario_24/elm/p02.htm

3.4. Oportunidades

3.4.1. Gran potencial de mercado

A nivel mundial el mercado de la ciberseguridad tiene el potencial para crecer hasta superar los 2 billones de dólares en los próximos años según un estudio de McKinsey[87]. Se trata de un aumento significativo con respecto al tamaño actual del mercado. Estiman que ese crecimiento vendrá no sólo de las grandes organizaciones, sino también de un desarrollo más rápido del segmento de las pequeñas y medianas empresas.

En España, según datos referenciados por INCIBE[88] hay más de 1800 empresas dedicadas a la ciberseguridad. En cuanto a la posible demanda de productos y servicios de ciberseguridad, que son básicos para la supervivencia de las empresas, a 1 de enero de 2024 había 3.255.276 empresas económicamente activas en España[89], por lo que existiría una gran cuota de mercado disponible.

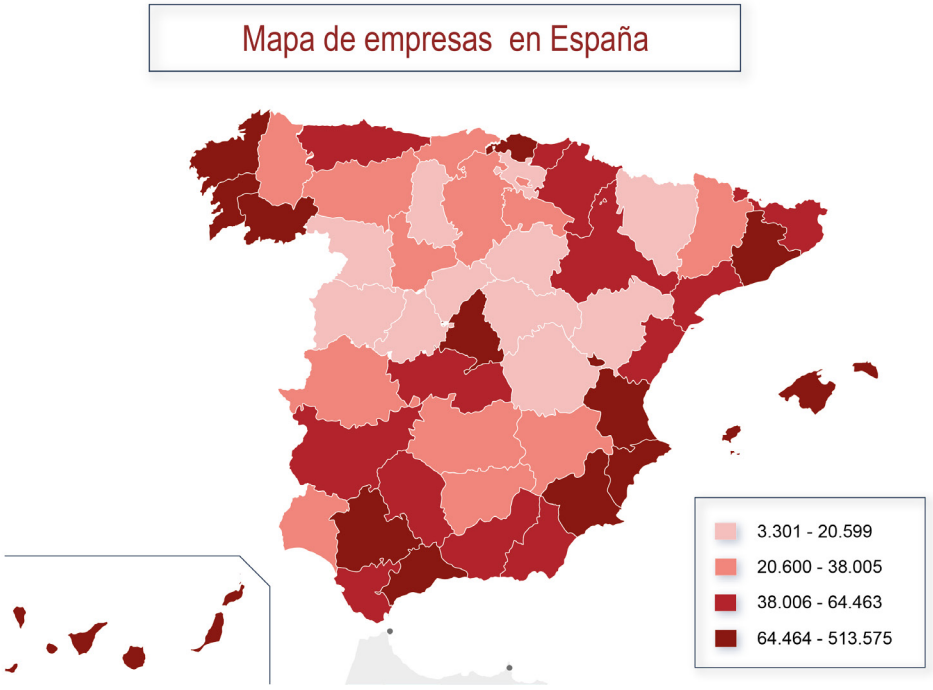


Figura 11: Mapa de empresas en España

Fuente: INE.[90]

[87] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer

[88] https://www.incibe.es/emprendimiento/publicaciones/blog/pilares-del-emprendimiento-en-ciberseguridad-en-espana

[89] https://www.ine.es/dyngs/Prensa/es/DIRCE2024.htm

[90] https://www.ine.es/jaxiT3/Datos.htm?t=4721#_tabs-mapa

Cabe destacar que América Latina y el Caribe es la región del mundo que presenta el aumento más rápido de ciberincidentes divulgados, con una tasa de crecimiento anual del 25 % de 2014 a 2023. Además, sería la región menos protegida, con una puntuación promedio de ciberseguridad de 10.2 sobre 20[91]. España podría beneficiarse de las relaciones institucionales existentes, culturales e históricas para impulsar los servicios de la ciberseguridad en la región. En términos generales, Hispanoamérica ofrece un vasto mercado emergente, con una población joven y en crecimiento, y bien formada.[92] Establecer relaciones comerciales y económicas con países hispanohablantes puede impulsar el crecimiento económico a través de nuevas oportunidades de exportación e importación, colaboración en proyectos de infraestructuras tecnológicas y nuevos desarrollos. Además, las conexiones con Hispanoamérica pueden promover la diversificación de la economía nacional y fortalecer la competitividad global del país al abrir puertas a nuevos mercados y oportunidades de inversión desde Hispanoamérica hacia el resto de Europa.

3.4.2. Nueva regulación en ciberseguridad

El contexto regulatorio demanda la adquisición de nuevos productos o servicios de ciberseguridad, lo que permite nuevas fuentes de generación de negocio con la creación de nuevos startups, líneas de negocio o productos.

En este sentido, cabe señalar que la Directiva NIS2[93] impone a todas las medianas y grandes empresas de 18 sectores críticos la adopción de medidas de gestión de riesgos, incrementando de manera drástica el alcance de los sujetos obligado por la directiva anterior NIS1.[94]

Por su parte, y en vista del aumento de los riesgos y del número de incidentes que afectan a los Estados miembros, el Reglamento de Cibersolidaridad[95] prevé un Mecanismo de Emergencia en materia de Ciberseguridad para ayudar a los Estados miembros a prepararse y responder a incidentes de ciberseguridad significativos y a gran escala. Como parte de este Mecanismo está prevista la creación gradual de una Reserva de Ciberseguridad de la UE, integrada por servicios de proveedores de servicios de seguridad gestionados de confianza. Como se indica en el Reglamento, la Reserva de Ciberseguridad de la UE también podría contribuir a reforzar la posición competitiva de la industria y los servicios en la Unión en toda la economía digital, incluidas las microempresas y las pequeñas y medianas empresas, así como las empresas emergentes incentivando la inversión en investigación e innovación.

Además, el Reglamento de Ciberresiliencia[96] tiene como objetivo el desarrollo de productos con elementos digitales seguros, de manera que se introduzcan en el mercado con menos vulnerabilidades y que los fabricantes se tomen en serio la seguridad a lo largo de todo el ciclo de vida de un producto.

---

[91] https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

[92] "La comunidad idiomática hispanohablante muestra un nivel de desarrollo humano superior al promedio de las comunidades anglófona y francófona". Instituto Cervantes. *El español en el mundo, Anuario 2024*

[93] https://www.boe.es/doue/2022/333/L00080-00152.pdf

[94] https://www.boe.es/doue/2016/194/L00001-00030.pdf

[95] https://www.boe.es/doue/2025/038/L00001-00034.pdf

[96] https://www.boe.es/doue/2024/2847/L00001-00081.pdf

3.4.3. Fondos europeos

En cuanto a fondos, además de Next Generation UE, el Centro Europeo de Competencia en Ciberseguridad[97] junto con la Red Nacional de Centros de Coordinación tienen como objetivo el refuerzo de la soberanía tecnológica mediante inversiones conjuntas en proyectos estratégicos de ciberseguridad, a través de instrumentos financieros, como el Programa Europa Digital[98] y Horizonte Europa.[99] Por su parte, el CDTI[100], Entidad Pública Empresarial dependiente del Ministerio de Ciencia, Innovación y Universidades, canaliza las solicitudes de ayuda y apoyo a los proyectos de I+D+I de empresas españolas.

3.4.4. Teletrabajo y nómadas digitales

La generalización del teletrabajo durante la pandemia de COVID-19 hizo posible una deslocalización del puesto de trabajo, eliminando o relajando los vínculos geográficos entre las empresas y su personal. En España en 2024 el alrededor del 14% de las personas podían trabajar de manera telemática desde su domicilio.[101]

Además, según el *Digital Nomad Visa Index*[102], España sería el país mejor posicionado para acoger a nómadas digitales. Los factores que se tendrían en consideración para este sistema de clasificación incluirían: velocidad de Internet, políticas fiscales, requisitos de ingresos para la solicitud de visados, coste de la vida, puntuación de la sanidad y popularidad turística.

---

97 https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-cybersecurity-competence-centre-eccc_es

98 https://digital-strategy.ec.europa.eu/en/activities/digital-programme

99 https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

100 https://www.cdti.es/

101 https://www.ontsi.es/sites/ontsi/files/2024-08/Flash%20Teletrabajo%202024.pdf

102 https://visaguide.world/digital-nomad-visa/digital-nomad-index/

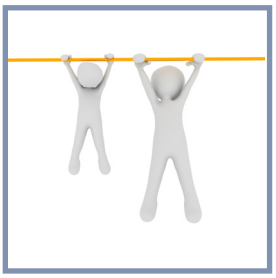
CONCLUSIÓN Y PROPUESTA DE INICIATIVAS

4. CONCLUSIÓN Y PROPUESTA DE INICIATIVAS

Para finalizar, se incluyen algunas propuestas de acciones para corregir las debilidades, afrontar las amenazas, mantener las fortalezas y explotar las oportunidades. No se trata de un análisis exhaustivo, sino de mostrar algunas posibles iniciativas nuevas, o ya en curso, que puedan sumarse a las existentes, para reforzar la posición de España como *hub* de ciberseguridad europeo.

Corregir las debilidades

Afrontar las amenazas



Mantener las fortalezas

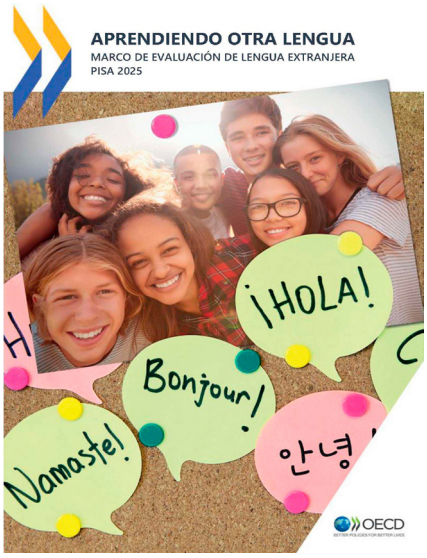
Explotar las oportunidades

- FNCS2025-HUB-01: Para facilitar la contratación de profesionales de la ciberseguridad, se recomienda actualizar el **Catálogo de Ocupaciones de Difícil Cobertura**[103]**, para que refleje de manera adecuada las necesidades reales de las empresas** y se pueda generar un mecanismo ágil y eficaz de contratación.
- FNCS2025-HUB-02: Para mitigar el desajuste entre las competencias disponibles y las requeridas por el mercado laboral, se recomienda impulsar el **Marco Europeo de Capacidades en Ciberseguridad**[104] como enfoque común sobre los perfiles de funciones de ciberseguridad y las capacidades asociadas, apoyando la identificación y articulación de tareas, competencias, capacidades y conocimientos asociados a las funciones de los profesionales europeos de la ciberseguridad .

[103] https://www.sepe.es/HomeSepe/es/empresas/informacion-para-empresas/profesiones-de-dificil-cobertura/profesiones-mas-demandadas.html

[104] https://www.enisa.europa.eu/topics/skills-and-competences/skills-development

- FNCS2025-HUB-03: Asimismo, se recomienda seguir las indicaciones de la **Comunicación de la Comisión al Parlamento Europeo y al Consejo de 2023** (*Colmar la brecha de talento en materia de ciberseguridad para impulsar la competitividad, el crecimiento y la resiliencia de la UE*), entre otras:
  - Ofrecer oportunidades de aprendizaje en el lugar de trabajo a través de la formación de aprendices.
  - Garantizar el apoyo al desarrollo y el reconocimiento de las microcredenciales del aprendizaje en materia de ciberseguridad, en consonancia con la Recomendación del Consejo relativa a un enfoque europeo de las microcredenciales.
  - Incluir las cualificaciones en materia de ciberseguridad, incluidas las microcredenciales en los marcos nacionales de cualificaciones.
  - Aplicar la Declaración sobre las mujeres en el ámbito digital y lograr la convergencia en los puestos de ciberseguridad.
- FNCS2025-HUB-04: Se propone la revisión de las **deducciones fiscales en el capítulo IV de la *Ley 27/2014 24 diciembre 2024 del Impuesto sobre Sociedades*** para incentivar la realización actividades relacionadas con la ciberseguridad, como la obtención de certificados de gestión de sistemas de seguridad de la información, tales como el Esquema Nacional de Seguridad, la ISO 27001 u otras, de modo análogo a las deducciones existentes por la obtención del certificado de cumplimiento de las normas de aseguramiento de la calidad de la serie ISO 9000, GMP o similares.
- FNCS2025-HUB-05: La previsión de **creación del futuro Centro Nacional de Ciberseguridad** contemplado en el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, constituye una oportunidad para reforzar el modelo actual, superar la dispersión competencial en la materia e integrar capacidades. Es fundamental el **impulso político y la dotación recursos** para que se haga una realidad.
- FNCS2025-HUB-06: Con el fin de disponer de un diagnóstico más preciso de la situación en cuanto al **dominio del idioma inglés** y poder proponer medidas para el medio plazo, cabe señalar que el Programa para la Evaluación Internacional de Estudiantes (PISA) 2025[105] incluirá por primera vez la evaluación internacional de lengua extranjera, que en este primer ciclo será el inglés. Como indica la OCDE[106], en el mundo global e interconectado en el que vivimos, el dominio de más de una lengua extranjera es una herramienta esencial para comunicarse e interactuar con los demás y un factor clave para la empleabilidad.



[105] https://www.educacionfpydeportes.gob.es/inee/evaluaciones-internacionales/pisa/pisa-2025.html

[106] https://www.libreria.educacion.gob.es/libro/aprendiendo-otra-lengua-marco-de-evaluacion-de-lengua-extranjera-pisa-2025_175125/

- FNCS2025-HUB-07: En cuanto al **reto estructural de la falta de productividad**, cabe señalar que a finales de 2024 se puso en marcha el Consejo de la Productividad de España[107] con el objetivo de fijar las líneas de trabajo que permitan tener análisis y propuestas para mejorar la productividad y competitividad de la economía española. El Consejo elaborará un informe anual para recopilar los análisis y trabajos realizados sobre la evolución de la productividad en España. El primer informe anual se publicará antes del fin de 2025. Asimismo, podrá publicar análisis económicos y estadísticos independientes y opiniones públicas en materia de política económica orientadas a la mejora de la productividad y la competitividad.
- FNCS2025-HUB-08: Para ayudar a **mitigar la dependencia exterior**, y aprovechar las excelentes capacidades de conectividad de España y el uso de energías renovables que ofrecen las condiciones climáticas, se propone favorecer la implantación de nuevos centros de proceso de datos, ampliando su huella también en nuevas localizaciones geográficas con potencial climático y energético que se sumen a las capacidades hiperescalares actuales, y que proporcionen una capacidad de procesado local suficiente para el soporte a la inteligencia artificial y futuras tecnologías. Así, estas instalaciones de procesado masivo de datos serían el centro de polos locales de innovación y tecnología que permitan una mayor extensión de las capacidades del hub, una mayor resiliencia ante eventos locales y un mejor aprovechamiento del potencial humano en toda la geografía, tanto local como de nómadas digitales.
- FNCS2025-HUB-09: Para **reducir las cargas administrativas**, está en marcha la iniciativa denominada "Régimen 20"[108], que pretende eliminar la disparidad de requisitos administrativos entre comunidades autónomas y entidades locales y, al mismo tiempo, reducir trámites. El primer paso será la realización de un diagnóstico común por sectores para antes de final de año poner sobre la mesa sector a sector, en aquellos que se consideren más prioritarios, medidas concretas para empezar a implantarlas el próximo año.
- FNCS2025-HUB-10: Para afrontar **la amenaza que supone la percepción estereotipada de España**, como alejada de la tecnología, y aprovechar la oportunidad que ofrece el gran potencial de mercado, se propone reforzar el papel del ICEX incrementando la dotación de medios y recursos para intensificar las actividades de difusión de las capacidades técnicas existentes, sus productos, servicios y propuestas de valor, incrementando el conocimiento en otras geografías de estas capacidades y la atracción de nuevos inversores al *hub*, creando nuevas y mayores capacidades de llegada al mercado y de la marca España como sinónimo de éxito y excelencia tecnológica.
- FNCS2025-HUB-11: Con el fin de **reforzar el ecosistema tecnológico en expansión**, se requiere fomentar una mayor colaboración entre los sectores público y privado, evitando discrepancias entre ambos, con el objetivo de aumentar la confianza en el cibermercado español y atraer más inversiones.[109]

---

[107] https://portal.mineco.gob.es/ca-es/economiayempresa/ConsejoProductividad/Pagines/consejo_productividad_espana.aspx#publicaciones

[108] https://portal.mineco.gob.es/es-es/comunicacion/Paginas/Conferencia-Sectorial-de-Mejora-Regulatoria-y-Clima-de-Negocios.aspx

[109] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/europes-next-cybersecurity-hub-what-makes-spain-a-leading-contender#/

- FNCS2025-HUB-12: Para **reforzar los lazos con América Latina y el mundo hispanohablante**, las próximas tres citas regionales en 2025 y 2026: la Cumbre UE-CELAC, en Colombia; la X Cumbre de las Américas, en República Dominicana; y la gestión de la secretaría pro tempore (SPT) de la XXX Cumbre Iberoamericana, serán una oportunidad para confirmar que España sigue siendo el socio estratégico que la región necesita como puente indispensable con Europa.[110]
- FNCS2025-HUB-13: Para aprovechar el **gran potencial de mercado** existente, y afrontar los retos cada vez más complejos de los ciberataques, los directores de seguridad de la información (CISO) tienen que asumir un papel cada vez más importante en las organizaciones, y contribuir a la mejora del proceso de toma de decisiones en este ámbito por parte de los órganos de gobierno de las organizaciones y, en especial, por el órgano de administración, así como potenciar la incorporación de tecnologías avanzadas y herramientas basadas en Inteligencia Artificial. Para ello, se recomienda impulsar la adopción de programas de formación y cualificación específica, como el "Esquema nacional de certificación de responsables de ciberseguridad" desarrollado en 2023 por este Foro Nacional de Ciberseguridad[111], y así además constituirse en un referente en los proyectos europeos que se desarrollen en este ámbito.
- FNCS2025-HUB-14: Para aprovechar las oportunidades que trae la **nueva regulación europea de ciberseguridad** se recomienda que las Administraciones públicas participen de manera activa en los proyectos que se desarrollen para impulsar los servicios de ciberseguridad en Europa, con el objetivo de reforzar la posición de las empresas y los profesionales de la ciberseguridad españoles. Como ejemplo, se puede mencionar el proyecto *Support Action* de ENISA[112], o los que se pongan en marcha en relación con la creación de la Reserva de Ciberseguridad de la UE incluida en la Ley europea de cibersolidaridad[113]. Además, **es imprescindible que los servicios ofrecidos generen confianza en el mercado europeo y mundial**. Así, el 18 de abril de 2023, la Comisión europea propuso una modificación específica de la *Ley de Ciberseguridad de la UE* , que culminó con la publicación el 15 de enero de 2025 del Reglamento (UE) 2025/37, que permitirá la certificación europea de los servicios de ciberseguridad gestionados, incluyendo la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría. Esta certificación constituiría un indicador de calidad fundamental para las entidades públicas y privadas que tengan intención de contratar esos servicios.

---

110 https://www.realinstitutoelcano.org/analisis/espanya-y-america-latina-en-2025/

111 https://foronacionalciberseguridad.es/documentacion/publico/110-trabajos-foro-nacional-ciberseguridad-paginas/file

112 https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/support-action-programme

113 https://www.boe.es/buscar/doc.php?id=DOUE-L-2025-80049

- FNCS2025-HUB-15: En cuanto a los **Fondos Europeos**, pueden ser una oportunidad para financiar un nuevo Plan Nacional de Ciberseguridad[114], con medidas actualizadas, y para apoyar la creación del Centro Nacional de Ciberseguridad. Además, sería preciso disponer de un marco de financiación nacional predecible y competitivo e incentivos públicos, con un fondo nacional específico para la ciberseguridad a largo plazo.[115]

Conclusión

España cuenta con muchos factores a su favor para convertirse en un hub de ciberseguridad en Europa. Si se impulsan las medidas adecuadas para reforzar sus puntos débiles y aprovechar las nuevas oportunidades que se ofrecen ante un panorama creciente de ciberamenazas, sus ventajas podrían convertir al país en una potencia líder en ciberseguridad a nivel europeo y global.

---

[114] https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2022/refc20220329_corregidav02.aspx#ciberseguridad

[115] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/europes-next-cybersecurity-hub-what-makes-spain-a-leading-contender#/

ANEXO

5. ANEXO: PROPUESTA DE FACTORES HABILITADORES PARA EL TERRITORIO DE ESTABLECIMIENTO DE UN HUB DE CIBERSEGURIDAD

A continuación se muestra una selección de posibles criterios para la localización de un territorio donde se pudiera favorecer la concentración física de empresas y profesionales de la ciberseguridad, teniendo en cuenta aspectos socioeconómicos, de calidad de vida, de infraestructuras y de sostenibilidad.

5.1. Aspectos socioeconómicos

Ámbito empresarial	Propuesta de servicios comerciales
	Estudio económico/diversificación de servicios
	Incubadoras de empresas
Foros sectoriales	Ciberseguridad
	Digitalización
	Emprendimiento
Respaldo institucional	Ubicaciones. Suelo público
	Soporte administrativo
	Facilidades económicas
	Relaciones con instituciones académicas
	Fomento institucional

Incentivos fiscales	Impuesto sobre Sociedades - Tasa reducida para nuevas empresas - Deducciones por inversión en I+D+i y ciberseguridad
	Impuesto sobre la Renta de las Personas Físicas - Régimen especial para empleados altamente cualificados y empresas emergentes que preste servicios a empresas emergentes o que lleve a cabo actividades de formación, investigación, desarrollo e innovación - Deducciones y exenciones fiscales para expatriados
	Impuesto sobre la Renta de No Residentes - Tasas competitivas para inversores extranjeros - Beneficios fiscales para no residentes que invierten en la región
	Impuesto sobre el Patrimonio - Exenciones para inversiones empresariales - Tasas reducidas para grandes patrimonios que invierten localmente
	Impuesto Temporal de Solidaridad sobre las Grandes Fortunas - Exenciones parciales para nuevos inversores con altos patrimonios
	Impuesto sobre Sucesiones y Donaciones - Reducciones significativas para la transmisión de empresas familiares - Beneficios fiscales para la transmisión de activos empresariales
	Beneficios fiscales específicos para sociedades holding establecidas en la región
	Tratamiento fiscal de los royalties - Deducciones y exenciones para fomentar la inversión en propiedad intelectual

5.2. Calidad de vida

Protección de la salud	Cobertura sanitaria universal
	Aportación farmacéutica
	Oferta/demanda asistencial equilibrada
Ocio	Cultura, gastronomía, deporte
Factores climáticos	Niveles de humedad
	Estacionalidad
	Riesgos naturales
	Variabilidad climática
	Niveles de radiación solar
Programas de apoyo para la reagrupación familiar	Visas y permisos de residencia
	Asistencia legal y educativa
	Beneficios de reubicación
	Asistencia en la búsqueda de vivienda
	Apoyo logístico, comunitario, legal y psicosocial
	Becas y ayudas
	Visas de estudiante dependiente

5.3. Educación e investigación

Entorno de investigación	Iniciativas de colaboración público-privada
	Programas de financiación y subvenciones
	Centros o *hubs* de innovación digital regionales
	Incubadoras de alta tecnología y pymes, para el análisis, estudio y desarrollo de casos de uso
	Plataformas y laboratorios virtuales aplicados a la ciberseguridad
Formación especializada	Convenios de colaboración con empresas, prácticas y tutorías
	Incentivos: premios, reconocimiento mejores trabajos, becas
Mantenimiento de las capacidades y desarrollo e innovación constantes	Certificación de conocimientos
	Conferencias y eventos
	Retos y *hackatones*
	Espacio para la innovación durante jornada laboral

5.4. Infraestructuras

Oferta hotelera	Variada y competitiva en coste y disponibilidad
	Combinación de actividad profesional y confort
Instalaciones laborales	Oficinas
	Salas de reuniones y congresos
	Coworking
	Laboratorios de tecnología
	Áreas de descanso
Telecomunicaciones	Cobertura de red: -Proveedores de Servicios de Internet - 5G - Fibra óptica - Satelital
	Velocidad de internet - Velocidad de descarga y subida - Latencia
	Estabilidad y Fiabilidad - Tasa de disponibilidad - Historial de interrupciones
	Costes - Costos de instalación. - Tarifas mensuales - Costos de mantenimiento
	Capacidad de ancho de banda - Ancho de banda disponible - Escalabilidad

	Infraestructura - Presencia de centros de datos - Redes de comunicación (*backbone*)
	Seguridad - Medidas de seguridad - Protección frente a los ciberataques
	Soporte técnico y servicio al cliente - Disponibilidad - Tiempo de respuesta
	Compatibilidad con tecnología emergente - Preparación para IoT - Adopción de tecnologías avanzadas
	Feedback de usuarios actuales - Opiniones y reseñas - Estudios de satisfacción del cliente

5.5. Sostenibilidad

Aspectos medioambientales y planificación urbanística	Eficiencia y consumo energético
	Emisiones de CO_2
	Ruido ambiental
	Tratamiento de residuos
	Espacios verdes
	Calidad del aire
	Drenaje y gestión del agua
	Accesibilidad
	Uso eficiente del suelo
	Red de transporte público
	Edificios sostenibles

FORO
NACIONAL DE
CIBERSEGURIDAD